



# **TippingPoint Security Management System User's Guide**

**Version 2.5.1**

Part Number: TECHD - 0000000083

Publication Control Number: 22707:741

Digital Vaccine is a registered trademark and TippingPoint and the TippingPoint logo are trademarks of 3Com Corporation or one of its subsidiaries.

This document contains confidential information or trade secrets or both, which are the property of 3Com Corporation. This document may not be copied, reproduced, or transmitted to others in any manner, nor may any use of the information in this document be made, except for the specific purposes for which it is transmitted to the recipient without the prior consent of 3Com Corporation.

Copyright © 2002 - 2007 3Com Corporation. All rights reserved.

This product includes code licensed from RSA Data Security.

This product includes the Sun® Microsystems, Inc. Java™ Runtime Environment (J2RE), Version 1.3.x

This product includes the IBM® Runtime Environment for Linux®, Java™ 2 Technology Edition, Version 1.3.1, 32-bit version

#### Runtime Modules

Copyright © IBM Corporation 1997-2002 All Rights Reserved

Copyright © 2001 Brett McLaughlin & Jason Hunter. All rights reserved. This product includes software developed by the JDOM Project, <http://www.jdom.org/>

Copyright © 1999 The Apache Software Foundation. All rights reserved. This product includes software developed by the Apache Software Foundation, <http://www.apache.org/>

Copyright © 1999 - 2001, AdventNet Inc. All rights reserved. This product includes copyright material licensed from AdventNet, Inc., <http://www.adventnet.com/>

Copyright © 1996, Marc A. Mnich, All rights reserved. This product includes software developed by the Java Exchange project, <http://www.javaexchange.com/>

Copyright © 1997-2000, Sitraka Inc. All rights reserved. This product includes software developed by Sitraka, <http://www.sitraka.com/>

# Table of Contents

<b>About This Documentation</b>	<b>xxix</b>
Overview	xxix
Target Audience	xxix
Conventions	xxx
Headings	xxx
Typeface	xxx
Cross References	xxx
Messages	xxx
Product Documentation	xxxii
Customer Support	xxxii
Contact Information	xxxii
<b>Chapter 1 - System Overview</b>	<b>1</b>
Overview	1
TippingPoint Architecture	1
Security Management System	2
SMS Server	3
SMS Client	3
Intrusion Prevention System Devices	4
High Availability	5
IPS Local Clients	6
X-Series Devices	6
Threat Suppression Engine	7
Threat Management Center	7
<b>Chapter 2 - Product Overview</b>	<b>9</b>
Overview	9
Product Overview: What's New	10
Virtual Segments	10
Digital Vaccine Alert Window	10
How To Tasks	10
SMS Overview	11
Features	11
SMS Components	11
Segments and Security Zones	12
Security Levels	14

SMS Server Web Site	15
Reports	16
SMS Client Interface	16
Notifications Window	17
Digital Vaccine Alert Window	17
Main User Interface	18
Interface Screens	21
Navigating Screens	22
Whols Utility	23
SMS Dashboard	24
Dashboard Configuration	25
System Preferences	27
Security Preferences	27
Device Preferences	28
Dashboard Preferences	29
Events Preferences	30

## **Chapter 3 - Getting Started** **31**

Overview	31
Getting Started: What's New	32
How To Tasks	32
Updating Existing Systems	33
Software Updates	33
Migration	34
Installing the SMS Client	34
Logging On to the SMS Client	35
Performing Initial Management Tasks	37
My Account	37
Date and Time Controls	37

## **Chapter 4 - Events** **39**

Overview	39
Events: What's New	40
Virtual Segments	40
Category Settings	41
Save Exported Queries to the SMS Server	41
How To Tasks	41
Navigation and Menu Options	42
Main Screen	42
Navigation Pane	44
Query Pane	44
List Pane	47
Menu Bar Options	53

Event Monitoring	54
Searching Events	54
Viewing Events	57
Viewing the Packet Trace	58
Exporting Query Results	59
Using the Whols Utility	60
Managing Queries	60
Tuning the System	61
Editing Attack Filters	61
Creating Attack Filter Exceptions	62
Threshold State	64
Firewall Events (X-Family Devices)	66
Firewall Block Events	67
Firewall Traffic Events	69

## Chapter 5 - Reports 71

Overview	71
Reports: What's New	73
Virtual Segments	73
Reports	73
Category Settings	74
How To Tasks	74
Navigation and Menu Options	75
Main Screen	76
Navigation Pane	76
Reports Query Pane	77
Reports Graph Pane	78
Reports List Pane	78
Menu Bar Options	79
Severity Level	79
General Instructions for Reports	80
Setting Up Reports	80
Process Time for Reports	81
Viewing Reports	81
Report Permissions	81
Attacks: All Reports	82
All Attacks Report	83
All Destination Report	85
All Sources Report	87
Attacks: Specific Reports	89
Specific Attack Report	89
Specific Destination Report	92
Specific Source Report	94

Attacks: Top Reports	96
Top Attacks	97
Top Destinations	99
Top Sources	101
Performance Protection: All Reports	103
All Filters	104
All Peers	105
Performance Protection: Specific Reports	107
Specific Filter	107
Specific Peer	109
Performance Protection: Top Reports	111
Top Filters	111
Top Peers	114
Rate Limit Reports	116
Device Rate Limit Report	116
Rate Limit Report	118
X-Family Reports	120
All Traffic by Protocol Reports	120
Web Traffic Reports	122
Device Traffic Reports	124
IPS Physical Port Report	125
X-Family Physical Port Report	127
Traffic Threshold Reports	128
E-Series Advanced DDoS Reports	131
Saved Reports	133
Edit or Delete Saved Reports	135
View/Export Report Results	136
All Schedules	140
Scheduling Reports	140
Managing Scheduled Reports	143

## **Chapter 6 - Profiles** **147**

Profiles: What's New	149
Virtual Segments	149
Profile Snapshots	149
X-Family Devices	149
IPS Profiles	150
IPS Profile Filters	150
How To Tasks	152
Navigation and Menu Options	154
Profiles Screen	154
Menu Bar Options	156

IPS Profiles (All Devices)	157
IPS Profile Management	157
IPS Profiles Shared Settings	166
Profile Overview	183
Profile Settings	183
IPS Profile Filters	189
Application Protection	196
Application Protection Filters	204
Infrastructure Protection Filters	208
Performance Protection Filters	226
Traffic Management Filters	230
DDoS Filters (E-Series Devices)	235
Firewall Profiles (X-Family Devices)	237
Managing Firewall Profiles	237
Managing Firewall Profile Rules	239
Firewall Shared Settings	241
VPN Profiles (X-Family Devices)	244
Managing VPN Profiles	244
VPN Shared Settings	245
Digital Vaccine Management	246
Digital Vaccine Screen	247
Digital Vaccine Tasks	249
Custom Shield Package Management	254
Custom Shield Packages Screen	255
Creating and Activating Packages	256
Managing Packages	257
Distributing Packages	259

## Chapter 7 - Quarantine 261

Overview	261
Quarantine: What's New	262
How To Tasks	262
Navigation and Menu Options	263
Main Screen	263
Navigational Pane	264
Menu Bar Options	265
Configuring Quarantine	265
Quarantined Hosts	266
Monitoring Quarantined Hosts	268
Quarantine Events	269
Actions	269
Types of Actions	269
Editing Default Actions	270
Defining Actions	272

Policies	278
Policy Setup Options	278
Default Quarantine Policy	280
Manual Quarantine	281
Creating a Quarantine Policy	282
Network Devices	283
Adding a Switch	283
Radius	285
Configuring RADIUS	285
IP Correlation	286
Configuring IP Correlation	287
IP Correlation Web Services	289
Testing IP Correlation	290
Managing Manual Quarantine Policy	291
Managing Quarantine Through an External/3rd-Party Interface	291

## Chapter 8 - Devices 293

Devices: What's New	294
Virtual Segments	294
Bridge Mode for X-Family Devices	294
Adding Offline X-Family Devices	295
Viewing TOS Information For X-Family Devices	295
Remote Syslog	295
IPSec Security Association Setup	296
DDoS Preferences	296
Management Port Settings	296
Interface Changes	297
How To Tasks	298
Navigation and Menu Options	302
Devices Screen	302
Graphics Pane	303
Menu Bar Options	303
Device Information	304
All Devices	305
Member Summary	305
Device Details	306
Device Monitoring	309
Events	309
System Health	314
Device Management	318
Adding a Device	319
Adding Offline X-Family Devices	320
Creating a Segment Group	324
Changing Management Port Settings	325
Unmanaging a Device	326



Managing a Device	327
Deleting a Device	327
Rebooting a Device	328
System Update	328
TippingPoint OS	332
Importing and Downloading the TOS	334
High Encryption for X-Family Devices	336
Managing TOS Distribution	336
Segment Groups	337
Managing Segment Groups	339
Importing Device Profiles	341
IPS Devices: Device Configuration	341
IPS Device Configuration Wizard	342
IPS Devices: Network Configuration	366
Link-Down Synchronization	367
IPS Devices: Event Monitoring	371
IPS Device Events: System Log	372
IPS Device Events: Audit Log	373
X-Family Devices: Device Configuration	375
X-Family Device Configuration Wizard	375
X-Family Devices: Network Configuration	393
Network Configuration: Segments/Zones Tab	395
Network Configuration: IP Interfaces Tab	400
Network Configuration: IP Address Groups Tab	401
Network Configuration: DHCP	402
Network Configuration: Routing Multicast	403
X-Family Devices: Security Configurations	406
Firewall	406
Web Filtering	411
VPN Configuration	413
Authentication	419
X-Family Devices: Event Monitoring	423
X-Family Device Events: System Log	425
X-Family Device Events: Audit Log	425
X-Family Device Events: VPN Log	426
E-Series: Advanced DDoS	427
DDoS Preferences	428

## Chapter 9 - Administration

431

Overview	431
Administration: What's New	432
High Availability	432
Remote Syslog	433
Named Resources	433

How To Tasks	433
Navigation and Menu Options	434
Main Screen	434
Navigational Pane	435
Menu Bar Options	436
General Administration	437
Log Administration	437
SMS Status	441
Usernames	447
Passwords	447
User Roles	448
Security Level Capabilities	449
Managing User Accounts	449
Password Expired	452
Active Sessions	452
Database Administration	454
Database Maintenance	456
Database Backup and Restore	457
SMS Server Properties	460
Management Information	460
Remote Syslog Record Formats and Examples	462
Network Information	470
Authentication Information	473
High Availability	475
HA Overview	476
Configuring HA	477
HA Configuration Option Examples	479
Synchronization Process	480
Using HA	485
Synchronization Timing	486
Named Resources	487
Named IP Addresses	488
Named VLAN IDs	489
Named Email Addresses	489

## **Appendix A - CLI Reference** **491**

Overview	491
Usage	492
Command Types	492
Remote Paths	493
The help Command	495
Command Reference	496
Attribs and Objects	512
Attrib Types	512
Object Reference	513

<b>Appendix B - Open Source Licenses</b>	<b>531</b>
Open Source Software in SMS	531
Apache License	532
JDOM License	533
Gnu Public License (GPL)	534
<b>Appendix C - Troubleshooting</b>	<b>541</b>
Overview	541
Log On Error Messages	541
Password Recovery	541
Network Changes	542
IPS Port Out-of-Service	543
SMS Error Messages	543
Modifying Filters	543
Modifying Filter Action Settings	544
Adding Exceptions	544
Distributing Profiles	545
<b>Appendix D - X-Family Remote Deployment</b>	<b>547</b>
Example Deployment	548
How It Works	549
Setup	550
SMS Setup	550
VPN Terminator Setup	553
X-Family Device Setup	553
Device Management	554
Device Recovery	554
Network Outage	555
X-Family Reboot	555
<b>Appendix E - Port Information</b>	<b>557</b>
Required Ports	558
TMC Ports	559
Quarantine Ports	559
HA Ports	560
Optional Ports	561
<b>Glossary</b>	<b>563</b>



# List of Procedures

## Chapter 1. System Overview

## Chapter 2. Product Overview

Access the Whols Utility	23
Configure the Dashboard	26
Configure Security Preferences	27
Configure Device Preferences	28
Configure Dashboard Preferences	29
Configure Event Preferences	30

## Chapter 3. Getting Started

Update Software	34
Install the SMS Client	35
Log On to the SMS Client	36

## Chapter 4. Events

Display the Events Screen	42
Customize the List Pane	48
Sort Query Results	48
Update Displayed Results	49
Create a Query	56
Create a Query with the Taxonomy Tab	56
View an Attack Event	58
View the Packet Trace	58
Export Query Results	59
Edit a Saved Query	60
Delete a Saved Query	61
Edit the Attack Filter	62
Create a Filter Exception	63
Edit a Traffic Threshold Filter	65
Reset a Traffic Threshold Filter	66
Reset All Traffic Threshold Filters	66
Display the Firewall Block Events Screen	67
Customize Displayed Results	68
Display the Firewall Traffic Events screen	69

## Chapter 5. Reports

Generate an All Attacks Report	84
Generate an All Destination Report	86
Generate an All Sources Report	88

Generate a Specific Attack Report	90
Generate a Specific Destination Report	93
Generate a Specific Source Report	95
Generate a Top Attacks Report	98
Generate a Top Destination Report	100
Generate a Top Sources Report	102
Generate an All Performance Protection Filters Report	104
Generate an All Performance Protection Peers Report	106
Generate a Specific Performance Protection Filter Report	108
Generate a Specific Performance Protection Peer Report	110
Generate a Top Performance Protection Filters Report	113
Generate a Top Performance Protection Peers Report	115
Generate a Device Rate Limit Report	117
Generate a Rate Limit Report	119
Generate an All Traffic by Protocol Report	121
Generate a Web Traffic by Category Report	123
Generate a Device Traffic Report (IPS Physical Port)	126
Generate a Device Traffic Report (X-Family)	127
Generate a Traffic Threshold Report	130
Generate a DDoS Report	132
Delete a Report	136
Export Report Results	137
Open Report Results	139
Schedule a Report	142
Edit Scheduled Report	144
Delete a Scheduled Report	146

## Chapter 6. Profiles

Create a Profile	161
Copy a Profile	161
Edit a Profile Details	162
Delete a Profile	162
Snapshot a Profile Version	162
Activate a Profile Version	163
View Profile Version Details	163
Distribute a Profile	165
Cancel a Distribution In-Progress	166
Create/Edit an Action Set	172
Configure a Quarantine Action Set	174
Set Aggregation Settings	179
Create an Email Notification Contact	179
Edit an Email Notification Contact	179
Create a SNMP Notification Contact	180
Edit an SNMP Notification Contact	180
Set Aggregation Settings	181
Add a Non-Standard Port	183

Delete a Non-Standard Port	183
Create an Attack Filter Profile Restriction	185
Edit an Attack Filter Profile Restriction	185
Delete an Attack Filter Profile Restriction	186
Create an Attack Filter Profile Exception	186
Edit an Attack Filter Profile Exception	186
Delete an Attack Filter Exception	187
Create a Profile Performance Protection Restrictions	188
Edit Global Performance Protection Restrictions	188
Delete Global Performance Protection Restriction	188
Search/View a Filter	191
Perform an Advanced Search	192
Edit Multiple Filters	194
Edit Application Protection Category Settings	200
Edit an Application Protection Filter	200
Create Filter Exception	203
Delete Filter Exception	204
Edit Infrastructure Protection Category Settings	210
Create Filter Exception	211
Delete Filter Exception	211
Create/Edit an Advanced DDoS Filter for 100E/200E/210E Models	213
Create/Edit an Advanced DDoS Filter for 1200E/2400E/5000E Models	216
Create an Advanced DDoS Exception for 100E/200E/210E Models	217
Edit an Advanced DDoS Exception for 100E/200E/210E Models	218
Delete an Advanced DDoS Exception for 100E/200E/210E Models	219
Create/Edit an Advanced DDoS Exception for 1200E/2400E/5000E Models	219
Edit a Network Equipment Filter	220
Edit a Traffic Normalization Filter	222
Create/Edit a Traffic Threshold Filter	224
Delete a Traffic Threshold Filter	225
Edit Performance Protection Category Settings	228
Edit a Performance Protection Filter	229
Create/Edit a Traffic Management Filter	232
Delete a Traffic Management Filter	234
Save the Traffic Management Filter Order	234
Edit a DDoS Filter	236
Add a Firewall Profile	238
Distribute a Firewall Profile	238
Add a Firewall Rule	239
Manage Firewall Rules	240
Edit a Firewall Rule	240
Add a Custom Service	241
Edit a Custom Service	242
Add a Service Group	242
Edit a Custom Service	242
Add a Schedule	243

Edit a Schedule	243
Set up a common definition for common parameters	243
Associate a common name with a firewall profile	244
Set up a VPN Profile	245
Deploy a VPN Profile	245
Set up IPSec Security Association	246
Auto-Download New Digital Vaccine Packages	250
Download a Digital Vaccine Package	250
Import a Digital Vaccine Package	250
Delete a Digital Vaccine Package	251
Activate a Digital Vaccine Package	251
View Details of a Digital Vaccine Package	252
Auto-Distribute New Packages	253
Distribute New Packages	253
Cancel a Distribution Process	254
New Scheduled Distribution	254
Edit Scheduled Distribution	254
Import and Activate a Custom Package	256
Import a Custom Shield Package	257
Delete a Custom Shield Package	258
Activate/Deactivate a Custom Shield Package	258
View Details of a Custom Shield Package	258
Uninstall a CSW Package	259
Distribute New Packages	259

## Chapter 7. Quarantine

Search Quarantined Hosts	268
Unquarantine a Host	268
View Quarantine Events by Hosts	269
Edit the Switch Disconnect Action	270
Implement the Switch Disconnect Action	271
Edit the IPS Default Quarantine Action	271
Create/Edit a Syslog Action	272
Implement a Syslog Action	273
Create/Edit an Email Action	273
Implement an Email Action	273
Create/Edit a NMS Trap Action	274
Create/Edit a Web Action	275
Implement a Web Action	276
Create/Edit a SNMP Trap Action	276
Create/Edit a Move Quarantined Host onto a VLAN action	277
Implement a Move Quarantined Host onto a VLAN Action	277
Edit Default Quarantine Policy	280
Manually Quarantine a Host	281
Create/Edit a new Policy	282
Add/Edit a Switch	284



Configure RADIUS	286
Add/Edit Network Mapping	288
Add/Edit Web Services	289
Control Web Service Precedence	289
Perform a Test	290

## Chapter 8. Devices

View configuration settings for All Devices	306
Edit configuration settings for an individual device	306
View Events for All Devices	313
View Events for a Specific Devices	313
Search Events Lists	313
Reset Events Lists	313
Flush Events Lists	314
Set Health Thresholds	317
Reset Logs	318
Configure Logging Mode Settings	318
Add an IPS Device	319
Add an Offline X-Family Device	323
Create a Device Group	324
Edit Device Group Membership	324
Create a Device Group	325
Edit Device Group Membership	325
Unmanage a Device	326
Manage a device	327
Delete a Device	328
Rebooting a Device	328
Rollback to a Previous Version	330
Delete a Previous Version	330
Create a New System Snapshot	330
Import Snapshot From File	331
Export Snapshot to File	331
Copy Snapshot to the Device	331
Copy Snapshot to the SMS	331
Rollback to Snapshot	331
Delete Snapshot	332
Download the TOS Software	335
Import TOS Software from a File	335
Obtain a High Encryption Package	336
View TOS Details	336
Distribute the TOS	337
Delete a TOS Entry	337
Create/Edit a Segment Group	340
Edit a Segment Group Member	341
Import a Device Profile	341
Configure the Management Port	346

Reset Filters	346
Configure Management Routes	347
Configure Services	349
Configure the AFC Settings	351
Configure Network HA	353
Configure Logging Mode Settings	354
Configure NMS Settings	355
Create/Edit Remote Syslog Servers	357
Configure Servers	358
Configure the Time Options	362
Configure TSE Settings	364
Edit IPS Segment Details	368
Create/Edit a Virtual Segment	369
Edit Port Details	369
Import IPS Profile	370
View Log	371
Reset Logs	371
Configure the Management Port	377
Reset Filters	378
Configure Services	379
Configure the AFC Settings	380
Configure Logging Mode Settings	382
Configure NMS	383
Create/Edit Remote Syslog Servers	385
Configure Servers	386
Configure the Time Options	390
Configure TSE Settings	392
Create/Edit Security Zone	397
Edit IPS Segment Details	398
Edit Port Details	398
Import a Profile	399
Create/Edit a Named IP Addresses	401
Create/Edit a Named Group of IP Addresses	401
Edit DHCP Server Settings	402
Create New DHCP Static Mapping	403
View/Refresh Routing Table	405
Edit Unicast/Multicast Routing Settings	405
Create a New Static Route	405
Add a Firewall Rule	407
Manage Firewall Rules	407
Edit a Firewall Rule	408
Add a Custom Service	409
Edit a Custom Service	409
Add a Service Group	409
Edit a Custom Service	410
Add a Schedule	410

Edit a Schedule	410
Add a Virtual Server	411
Edit a Virtual Server	411
Edit Web Filtering Global Settings	412
Edit 3Com Content Filter Settings	412
Enable/Disable Manual Web Filtering	413
Enable/Disable IPSec Global Setting	414
Add/Edit IPSec Global Association	414
Set Up IPSec Security Association (IKE)	415
Enable/Edit L2TP Configuration Settings	416
Enable/Edit PPTP Configuration Settings	417
Edit Radius Configuration	419
Add/Edit Local Users	420
Edit Local User Preferences	420
Create/Edit Privilege Groups	421
Import a Local Certificate	421
Import CA Certificate	422
Export CA Certificate	422
Import Local Signed Certificate	422
Create Certificate Request	423
View Log	423
Reset Logs	424
Configure Advanced DDoS Filter Options	428
Set DDoS Preferences	429

## Chapter 9. Administration

View the SMS System Log	438
View an SMS System Log Entry	438
View the SMS Audit Log	440
View an SMS Audit Log Entry	441
Download and Install the SMS Software	443
Import and Install SMS Software	444
Upgrade the SMS License	445
Create/Edit a User Account	451
Delete a User Account	452
Terminate a User Session	453
Refresh Database Maintenance	456
Edit Database Maintenance	456
Cleanup Database Maintenance	456
Backup the SMS Database	457
Restore the SMS Database	458
Schedule a Database Backup	459
Configure the Management Settings	469
Create a new Remote Syslog for Events	469
Edit a Remote Syslog for Events	470
Configure the Network Settings	471

## List of Procedures

Configure the Authentication Settings	474
Configure High Availability - Primary Only Option	481
Configure High Availability - Primary + Secondary Option	482
Manually Synchronize HA Systems	484
Disable High Availability	484
Create/Edit a Named IP Address	488
Create/Edit a Named Group of IP Addresses	488
Create/Edit a Named VLAN ID	489
Create/Edit a Named Group of VLAN IDs	489
Create/Edit a Named Email Address	489
Create/Edit a Named Group of Email Addresses	490
Set All System Information Using Interactive Mode	493
Configure SMS for Remote X-Family Device Acquisition and Management	552

# List of Figures

## Chapter 1. System Overview

TippingPoint Architecture	2
---------------------------	---

## Chapter 2. Product Overview

SMS Server Web site	15
SMS Digital Vaccine Alert Window	18
SMS Main User Interface	19
Navigation Pane Sample	21
SMS Dashboard	24
Dashboard Configuration Dialog Box	26
System Preferences - Security Screen	27
System Preferences - Devices Screen	28
System Preferences - Dashboard Screen	29

## Chapter 3. Getting Started

SMS Client Icon	35
-----------------	----

## Chapter 4. Events

Events Screen	43
Events - Export Query Results	59
Sample Filter Edits/Details Dialog Box	62
Filters - Application Protection Filters - Create/Edit Exception Dialog Box	63
Events - Traffic Threshold State Screen	64
Filters - Traffic Threshold - Edit Dialog Box	65
Firewall Block Events Screen	67
Firewall Traffic Events Screen	70

## Chapter 5. Reports

Reports Window	76
Attacks - All Attacks Report - Query Pane	83
Attacks - All Destination Report - Query Pane	85
Attacks - All Sources Report Screen	87
Attacks - Specific Attack Report Screen	89
Attacks - Specific Destination Report Screen	92
Attacks - Specific Source Report Screen	94
Attacks - Top Attacks Screen	97
Reports - Top Destinations Screen	99
Attacks - Top Sources Screen	101

Performance Protection - All Filters Screen	104
Performance Protection - All Peers Screen	105
Performance Protection - Specific Filter Screen	107
Performance Protection - Specific Peer Screen	109
Performance Protection - Top Filters Screen	111
Performance Protection - Top Peers Screen	114
Rate Limit - Device Rate Limit Screen	116
Rate Limit - Rate Limit Screen	118
Device Traffic Report Screen	120
Device Traffic Report Screen	122
Device Traffic Report Screen	125
Device Traffic Report Screen	127
Reports - Saved Reports Screen	134
Report Results Screen	136
Report - Export Results Window	138
Results - Export Result Window	139
All Schedules Screen	144

## Chapter 6. Profiles

Profiles Screen	155
Profiles - Details Screen	159
Profiles - Versions Screen	159
Profiles - Profile Distribution Dialog Box	165
Shared Settings - Action Sets Tab	168
Profiles - Action Set - Edit Dialog Box	172
Filters - Action Set - Configure Quarantine Response Dialog Box	174
Shared Settings - Notification Contacts Screen	178
Shared Settings - Services Screen	182
Profile Settings - Attack Filter Restrictions/Exceptions Tab	184
Profile Settings - Performance Protection Restrictions Tab	187
Filter Edits/Details Screen (Main tab)	191
Profiles - Advanced Search - Criteria Screen	192
Profiles - Advanced Search - Advanced Screen	193
Filter - Change Action Set Dialog Box (Multi-Edit)	195
IPS Profiles - Application Protection	198
Action Sets Box (Main tab)	201
Filter Edits/Details Dialog Box (Details tab)	202
Profiles - Infrastructure Protection Screen	209
Filter Controls Tab	214
100E/200E/210E Settings Tab	215
Filter Controls Tab	216
1200E/2400E/5000E Settings	217
Filters - Traffic Threshold - Edit Dialog Box	224
Profiles - Performance Protection	226
Filters - Edit Dialog Box	229
Up & Down Buttons	230

Traffic Management Filters - Create/Edit Filter Dialog Box	233
Filter - DDoS - Edit Filter Dialog Box (Main tab)	236
Digital Vaccine Screen	247
Profiles - Custom Shield Packages Screen	255

## Chapter 7. Quarantine

Quarantine Screen	264
Quarantined Hosts Screen	267
Quarantine - Create Manual Quarantine Dialog Box	281
Quarantine - RADIUS Screen	285
Quarantine - IP Correlation Screen	287
IP Correlation Test Dialog Box	290

## Chapter 8. Devices

Devices Screen	302
Member Summary Screen	306
Device Details Screen	307
Device Events (All Devices) Screen	310
Device System Health Screen	315
Device Configuration - Software Versions	329
Devices (TippingPoint OS) Screen	333
Devices - Segment Groups Screen	338
Devices (Segment Groups) Screen	339
Segment Group Edit Dialog Box	340
IPS Device Configuration Wizard	343
IPS Device Configuration (Management Information) Screen	344
IPS Device Configuration (Management Routes) Screen	347
IPS Device Configuration (Services) Screen	349
IPS Device Configuration (AFC Settings) Screen	350
IPS Device Config (HA (High Availability)) Screen	352
IPS Device Configuration (Logging Mode) Screen	354
IPS Device Configuration (Servers) Screen	358
IPS Device Configuration (Time Settings) Screen	360
IPS Device Configuration (TSE Settings) Screen	364
Devices - Network Configuration Screen for IPS Devices (V 2.5 and above)	366
Devices - Network Configuration Screen for IPS Devices (prior to V 2.5)	367
Devices - System Log Screen	372
Devices - Audit Log Screen	374
Device Configuration (Management Information) Screen for X-Family Devices	376
Device Configuration (Services) Screen for X-Family Devices	379
Device Configuration (AFC Settings) Screen for X-Family Devices	380
Device Configuration (Virtual Firewall HA) Screen for X-Family Devices	381
Device Configuration (Logging Mode) Screen for X-Family Devices	382
Device Configuration (NMS) Screen for X-Family Devices	383
Device Configuration (Servers) Screen for X-Family Devices	386
Device Configuration (Time Settings) Screen for X-Family Devices	388

Device Configuration (TSE Settings) Screen for X-Family Devices	392
Devices - Adv. DDoS Configuration Screen for E-Series Devices	427
Devices - Configuration (TSE Settings) Screen for E-Series Devices	429

## Chapter 9. Administration

Admin (General) Screen	435
Admin (General - SMS System Log) Screen	437
SMS - System Log Record Details Dialog	439
Admin (General - SMS Audit Log) Screen	439
Audit Log Record Details	441
Admin (General) Screen	442
Admin - Users Screen	446
Admin - Create/Edit User Dialog Box	450
Active Sessions	453
Admin - Database Screen	455
Server Properties - Management Screen	460
Server Properties - Network Screen	470
Server Properties - Authentication Screen	473
High Availability	477
HA Example - Primary Only Option (same subnet)	479
HA Example - Primary + Secondary Option (same subnet)	480

## Appendix. X-Family Remote Deployment

Device - New Device: Remote Acquisition Configuration	549
Device - New Device: Remote Acquisition Configuration	552

## Appendix. Port Information



# List of Tables

## Chapter 1. System Overview

## Chapter 2. Product Overview

Table 2 - 1: Events Screen - Interface Description	19
Table 2 - 2: Toolbar Buttons	20

## Chapter 3. Getting Started

Table 3 - 1: SMS Logon screen	36
-------------------------------	----

## Chapter 4. Events

Table 4 - 1: Events Screen - Options	43
--------------------------------------	----

## Chapter 5. Reports

Table 5 - 1: Attacks - All Attacks Report - Graph Details	83
Table 5 - 2: Attacks - All Attacks Report - Details	83
Table 5 - 3: Attacks - All Destination Report - Graph Details	85
Table 5 - 4: Attacks - All Destination Report - Details	85
Table 5 - 5: Attacks - All Sources Report - Graph Details	87
Table 5 - 6: Attacks - All Sources Report Details	87
Table 5 - 7: Attacks - Specific Attack Report - Graph Details	90
Table 5 - 8: Attacks - Specific Attack Report - Details	90
Table 5 - 9: Attacks - Specific Destination Report - Graph Details	92
Table 5 - 10: Attacks - Specific Destination Report - Details	92
Table 5 - 11: Attacks - Specific Source Report - Graph Details	94
Table 5 - 12: Attacks - Specific Source Report - Details	94
Table 5 - 13: Attacks - Top Attacks - Graph Details	97
Table 5 - 14: Attacks - Top Attacks - Details	97
Table 5 - 15: Attacks - Top Attacks - All Details	98
Table 5 - 16: Attacks - Top Destinations - Graph Details	99
Table 5 - 17: Attacks - Top Destinations - Summary	99
Table 5 - 18: Attacks - Top Destinations - All Details	100
Table 5 - 19: Attacks - Top Sources - Graph Details	101
Table 5 - 20: Attacks - Top Sources - Summary	101
Table 5 - 21: Attacks - Top Sources - All Details	102
Table 5 - 22: All Performance Protection Filters - Graph Details	104
Table 5 - 23: All Performance Protection Filters - Details	104
Table 5 - 24: All Peers - Graph Details	105
Table 5 - 25: Performance Protection - All Peers - Details	106
Table 5 - 26: Performance Protection - Specific Filter - Graph Details	108
Table 5 - 27: Performance Protection - Specific Filter - Details	108

Table 5 - 28: Performance Protection - Specific Peer - Graph Details	109
Table 5 - 29: Performance Protection - Specific Peer - Details	110
Table 5 - 30: Performance Protection - Top Filters Graph Details	112
Table 5 - 31: Performance Protection - Top Filters - Summary	112
Table 5 - 32: Performance Protection - Top Filters - All Details	112
Table 5 - 33: Performance Protection - Top Peers - Graph Details	114
Table 5 - 34: Performance Protection - Top Peers - Summary	114
Table 5 - 35: Performance Protection - Top Peers - All Details	115
Table 5 - 36: Rate Limit Report - Graph Details	117
Table 5 - 37: Rate Limit Report - Rate Limit Details	117
Table 5 - 38: Rate Limit - Rate Limit - Graph Details	118
Table 5 - 39: Rate Limit Report - Rate Limit Details	119
Table 5 - 40: Device Traffic Report - Graph Details	120
Table 5 - 41: Devices Traffic Details	121
Table 5 - 42: Web Traffic by Category Report - Graph Details	122
Table 5 - 43: Summary by Category Details	122
Table 5 - 44: Traffic Details by Category, Source IP Address	123
Table 5 - 45: Device Traffic Report - Graph Details	125
Table 5 - 46: Devices Traffic Details	125
Table 5 - 47: Device Traffic Report - Graph Details	127
Table 5 - 48: Devices Traffic Details	127
Table 5 - 49: Traffic Threshold Report - Graph Details	129
Table 5 - 50: Traffic Thresholds by Device: Segment Details	129
Table 5 - 51: Advanced DDoS Report - Graph Details	132
Table 5 - 52: Advanced DDoS Report - Details	132
Table 5 - 53: Report Types	135
Table 5 - 54: All Scheduled Screen	144

## Chapter 6. Profiles

Table 6 - 1: Profile Inventory Details	164
Table 6 - 2: Distribution Process Details	164
Table 6 - 3: Action Sets: Inventory Details	168
Table 6 - 4: Action Sets: Default Actions Sets and Options	169
Table 6 - 5: Action Sets: Available Actions Sets and Options	171
Table 6 - 6: Rate Limit Rates per Model	176
Table 6 - 7: Notification Contacts Details	178
Table 6 - 8: Services Details	182
Table 6 - 9: IPS Profiles - Application Protection Screen Information	199
Table 6 - 10: Profiles - Infrastructure Protection Screen Information	209
Table 6 - 11: Profiles - Performance Protection Screen Information	226
Table 6 - 12: Example Traffic Management Settings	231
Table 6 - 13: Profiles - Traffic Management Screen Information	231
Table 6 - 14: DV Inventory Details	248
Table 6 - 15: Permissions for Scheduled Distributions	253
Table 6 - 16: CSW Inventory Details	256

## Chapter 7. Devices

Table 8 - 1: All Devices Screen	305
Table 8 - 2: Device Details	307
Table 8 - 3: Chassis Component Legend	308
Table 8 - 4: Status Indicator Legend	308
Table 8 - 5: TSE Connection Table Details	311
Table 8 - 6: TSE Quarantine Table Details	312
Table 8 - 7: TSE Adaptive Filter Configuration Information	312
Table 8 - 8: Events Search Criteria	312
Table 8 - 9: Packet Statistics Details	316
Table 8 - 10: Health Details	316
Table 8 - 11: Traffic Details	317
Table 8 - 12: Software Versions Table Information	329
Table 8 - 13: TOS Inventory Details	333
Table 8 - 14: Distribution Process Details	333
Table 8 - 15: Segment Group Information	338
Table 8 - 16: Segment Group Details	339
Table 8 - 17: Management Port Information	345
Table 8 - 18: Services Information	349
Table 8 - 19: Network HA Information	352
Table 8 - 20: Remote Syslog Field Descriptions	356
Table 8 - 21: Time Option Information	360
Table 8 - 22: Time Zone Definitions	361
Table 8 - 23: System Log Details	373
Table 8 - 24: Audit Log Details	374
Table 8 - 25: Management Port Information	377
Table 8 - 26: Remote Syslog Field Descriptions	384
Table 8 - 27: Time Option Information	388
Table 8 - 28: Time Zone Definitions	389
Table 8 - 29: Devices - Network Configuration for X-Family Devices	394
Table 8 - 30: Devices - Segment Zones Tab for X-Family Devices	396
Table 8 - 31: Security Zones Summary Information	396
Table 8 - 32: Devices - IP Interfaces Tab for X-Family Devices	401
Table 8 - 33: Devices - Routing/Multicast Screen for X-Family Devices	404
Table 8 - 34: System Log Details	425
Table 8 - 35: Audit Log Details	426
Table 8 - 36: Audit Log Details	426

## Chapter 8. Administration

Table 9 - 1: SMS System Log Information	438
Table 9 - 2: SMS Audit Log	440
Table 9 - 3: SMS Software Information	442
Table 9 - 4: Health Information	445
Table 9 - 5: Security Levels and Account Names	447
Table 9 - 6: Username Examples	447

Table 9 - 7: Security Levels and Passwords	448
Table 9 - 8: Password Examples	448
Table 9 - 9: User Role Capabilities	449
Table 9 - 10: User Information	450
Table 9 - 11: Active Sessions Details	453
Table 9 - 12: Database Maintenance Details	455
Table 9 - 13: Management Settings	461
Table 9 - 14: Remote Syslog Events Record Format (SMS V2.0/2.1)	462
Table 9 - 15: Remote Syslog Events Record Format (SMS V2.5)	464
Table 9 - 16: Remote Syslog Events Record Format (Firewall Session)	466
Table 9 - 17: Remote Syslog Events Record Format (Firewall Block)	467
Table 9 - 18: Remote Syslog Events Record Format (SMS Audit)	468
Table 9 - 19: Remote Syslog Events Record Format (SMS System)	468
Table 9 - 20: Network Settings	471
Table 9 - 21: Authentication Settings	474
Table 9 - 22: High Availability Settings	477
Table 9 - 23: Synchronization Timing Results	486
Table 9 - 24: Lock Resources	487

## Appendix. CLI Reference

Table A - 1: Help Commands	495
Table A - 2: SMS Commands	496
Table A - 3: Security Levels	503
Table A - 4: CLI Attrib Types	512
Table A - 5: cli Attribs	513
Table A - 6: ctl Attribs	514
Table A - 7: db Attribs	515
Table A - 8: dns Attribs	515
Table A - 9: ha Attribs	516
Table A - 10: health Attribs	517
Table A - 11: key Attrib	518
Table A - 12: license Attribs	519
Table A - 13: net and net2 Attribs	520
Table A - 14: ntp Attribs	521
Table A - 15: license Attribs	523
Table A - 16: pwd Attribs	524
Table A - 17: route Attribs	525
Table A - 18: smtp Attribs	526
Table A - 19: snmp Attribs	526
Table A - 20: svc Attribs	527
Table A - 21: sw Attribs	528
Table A - 22: sys Attribs	529
Table A - 23: time Attribs	530

## Appendix. X-Family Remote Deployment

Table E - 1: VPN Configuration Files - Definitions	551
--	-----

Table E - 2: X-Family Remote-Deploy Commands	554
--	-----

## **Appendix. Port Information**

Table F - 1: Required Port Availability	558
Table F - 2: TMC Port Availability	559
Table F - 3: Quarantine (Triggers) Port Availability	560
Table F - 4: HA Port Availability	560
Table F - 5: Optional Port Availability	561



# About This Documentation

*Explains intended audience, where related information is located, and how to obtain customer support.*

## Overview

Welcome to the TippingPoint Security System documentation.

This section includes the following items:

- [“Target Audience” on page xxix](#)
- [“Conventions” on page xxx](#)
- [“Product Documentation” on page xxxii](#)
- [“Customer Support” on page xxxii](#)

## Target Audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices. Users should be familiar with networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SNMP)
- simple Network management Protocol (SNMP)

# Conventions

The TippingPoint documentation uses the following conventions for structuring information.

## Headings

Each main section starts with a brief description of the information you can find in that section, which correlates with the major headings in that section. Each major heading corresponds to a task or concept that is important for you to understand. Headings are of a different size and type to make them easy to skim, whether you are viewing an online or print copy of this document.

## Typeface

This document uses the following typeface conventions:

<b>Bold</b>	Used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the <b>OK</b> button.
Code	Used for text a user must type to use the product.
<i>Italic</i>	Used for book titles, variables, and important terms.
<a href="#">Hyperlink</a>	Used for Web site and cross reference links.

## Cross References

When a topic is covered in depth elsewhere in this document, or in another document in this series, a cross reference to the other information is provided as follows:

## Messages

Messages are emphasized by font, format, and icons. There are four types of messages in this document:

- **Warnings** — indicate how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury includes anything requiring repair. Warnings indicate what you should or should not do and the consequences of not heeding the warning.
- **Cautions** — indicate how to avoid a serious loss that stops short of physical damage, such as the loss of data, time, or security. Cautions indicate what you should or should not do to avoid such losses and the consequences of not heeding the caution.
- **Notes** — Notes indicate information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior.
- **Tips** — Tips are suggestions about how to perform a task more easily or more efficiently.



## Warning

Warnings are represented by a red octagon with a white lightning bolt drawn inside. Warnings also start with the word “WARNING” and are presented in bold face type.



**WARNING** Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

## Caution

Cautions are represented by a yellow triangle icon with a black exclamation point drawn inside. Cautions also start with the word “CAUTION”.



**CAUTION** Do not type del \*.\* from the root (C:\) directory. Typing del \*.\* from the root directory will destroy all the program and configuration data that your computer needs to run, and will render your system inoperable.

## Note

A note has an icon represented by a piece of note paper and starts with the word “Note”.



**Note** To view information about attacks, you must have Operator authority. To create or edit attack filters and related objects, you must have Super User or Administrator authority.

## Tip

A tip is represented by a circle icon with a light bulb drawn inside and starts with the word “Tip”.



**TIP** Setting the **logging** parameter to “off” or “minimal” will improve your system’s processing performance, but it will make debugging very difficult in the event of a system crash. During system integration, you can set logging to “full” to ease debugging. After you have finished testing, set logging to “minimal” to improve performance.

# Product Documentation

TippingPoint Systems have a full set of documentation. These publications are available in electronic format on your installation CDs. For the most recent documentation updates, check the Threat Management Center (TMC) Web site at <https://tmc.tippingpoint.com>.

## Customer Support

TippingPoint is committed to providing quality customer support to all of its customers. Each customer is provided with a customized support agreement that provides detailed customer and support contact information.

For the most efficient resolution of your problem, take a moment to gather some basic information from your records and from your system before contacting customer support, including your customer number.

Have the following information available:

Information	Location
Your customer number	You can find this number on your Customer Support Agreement and on the shipping invoice that came with your TippingPoint system.
Your SMS server serial number	You can find this number on the bottom of the server chassis. Also, from the SMS CLI, you can run the <code>key</code> command.
Your SMS version number	You can find this information on the Dashboard in the <b>Updates</b> area. The <b>Admin</b> —> <b>General</b> screen also displays the version number.

## Contact Information

Use the following information to contact TippingPoint Customer Support:

### Telephone

**North America:** +1 866 681 8324

**International:** +1 512 681 8524

**Australia:** 800 783 933

**New Zealand:** 0800 852 300

### E-mail

[support@tippingpoint.com](mailto:support@tippingpoint.com)

# 1 System Overview

*The TippingPoint™ system is a high-speed, comprehensive security system that includes the Intrusion Prevention System™ (IPS),™ (LSM), Digital Vaccine™, and the Security Management System Appliance™. The SMS includes a secure server and management client for viewing, configuring, and reporting on multiple IPS devices in your network.*

## Overview

Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, TippingPoint's (TP) security system provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This section includes the following topics:

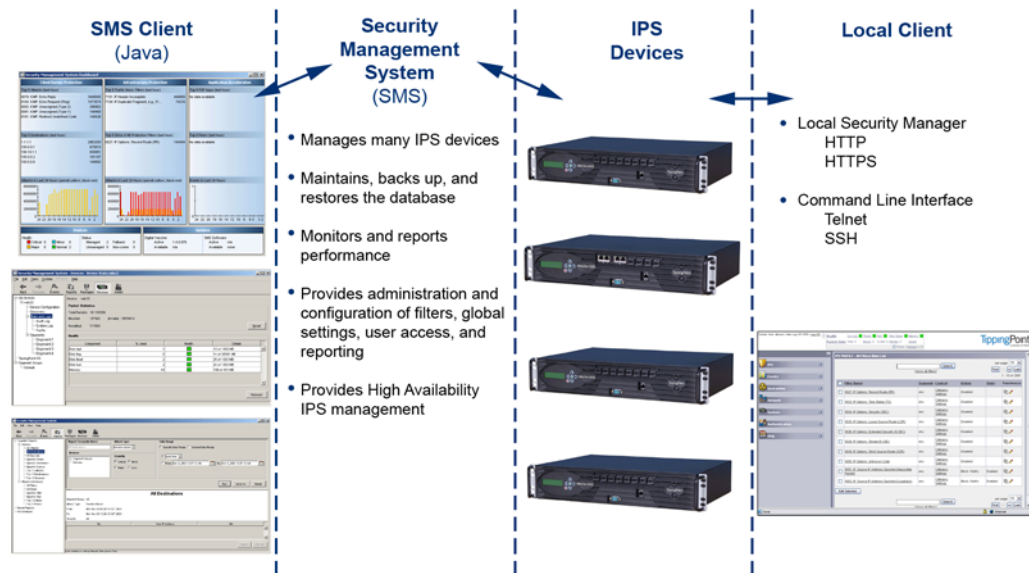
- [“TippingPoint Architecture” on page 1](#)
- [“Security Management System” on page 2](#)
- [“Intrusion Prevention System Devices” on page 4](#)
- [“Threat Suppression Engine” on page 7](#)
- [“Threat Management Center” on page 7](#)

## TippingPoint Architecture

The TippingPoint System uses a flexible architecture that consists of a Java-based SMS Client, SMS Management Server, IPS and/or X-Series device(s), and Local Clients including the Local Security

Manager (LSM) and Command Line Interface (CLI). The following diagram provides an overview of the architecture:

Figure 1 - 1: TippingPoint Architecture



## Security Management System

The SMS core components include:

- **SMS Secure Server** — hardware appliance for managing multiple devices
  - *SMS Home Page* — web-based interface with links to current Client software, documentation, and the Threat Management Center
- **SMS Management Client** — Java-based application for Windows or Linux workstations used to manage your TippingPoint system
  - *Graphical User Interface (GUI)*
  - *Dashboard*
  - *Command Line Interface (CLI)*

The SMS communicates with managed devices, the TippingPoint IPS or X-Series devices that are installed in your network.

The SMS architecture also includes the following 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.
- **Digital Vaccine (DV)** — Update service that includes up-to-date filter packages for protecting your network
- **Managed Devices** — TippingPoint IPS or X-Series devices that are installed in your network

## SMS Server

The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for up to 1,000 TippingPoint IPS or X-Series devices. The SMS provides the following functionality:

- **Enterprise-wide device status and behavior monitoring** — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status.
- **IPS networking and configuration** — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group.
- **Scheduled and pending network discovery scans** — Stores and enacts network discovery scans set and maintained by clients. Scan results save in the database for review and management by the SMS and local clients.
- **Filter customization** — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings.
- **Filter and software distribution** — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS Client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.

## SMS Client

The TippingPoint Security Management System (SMS) client provides services and functions to monitor, manage, and configure the entire TippingPoint system. This client is a Java-based application installed and accessed on a computer running the appropriate Windows operating system. Each user receives a specific user level with enhanced security measures to protect access and configuration of the system.

You can monitor the entire TippingPoint system through the SMS client on a computer with the following requirements:

- One of the following operating systems:
  - *Windows 98, 2nd edition*
  - *Windows NT, Service Pack 5 or later*
  - *Windows 2000, Service Pack 3 or later*
  - *Windows XP*
  - *Apple*
  - *Red Hat Linux*
- One of the following browsers:
  - *Microsoft Internet Explorer, version 6.0 or higher*
  - *Firefox*
  - *Safari*

The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs - including reports on all, specific, and top 10 attacks and their sources and destinations as well as all, specific, and top 10 peers and filters for misuse and abuse (peer-to-peer piracy) attacks. You can create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. You can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.

The SMS dashboard provides at-a-glance monitors, with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. It displays the entries for the top 5 filters triggered over the past hour in various categories, a graph of triggered filters over the past 24 hours, the health status of devices, and update versions for software of the system. Through the Dashboard, you gain an overview of the current performance of your system, including notifications of updates and possible issues with devices monitored by the SMS.

## Intrusion Prevention System Devices

Intrusion Prevention System (IPS) devices protect your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the amount 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.

TippingPoint IPS devices are active network defense systems using the Threat Suppression Engine (TSE) to detect and respond to attacks. TippingPoint Intrusion Prevention Systems are optimized to

provide high resiliency, high availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each TippingPoint can protect network segments from both external and internal attacks. TippingPoint Intrusion Prevention Systems are extremely low-latency network infrastructure ensuring switch-like network performance, even while under attack. TippingPoint also has built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

IPS devices provide the following segments and traffic performance:

- TippingPoint 50 — One 10/100 segment at an aggregate 50 megabits/second
- TippingPoint 100E — One 10/100/1000 segment at an aggregate 100 megabits/second
- TippingPoint 200/200E— Two 10/100 segments at an aggregate 200 megabits/second
- TippingPoint 400 — Four 10/100 segments at an aggregate 400 megabits/second
- TippingPoint 1200/1200E — Four 10/100/1000 segments at an aggregate 1.2 gigabits/second
- TippingPoint 2400/2400E — Four 10/100/1000 segments at an aggregate 2.0 gigabits/second
- TippingPoint 5000E — Four 10/100/1000 segments at an aggregate 5.0 gigabits/second

Multiple TippingPoint devices can be deployed to extend this unsurpassed protection to hundreds of enterprise zones. You can monitor and manage the devices by using the local client available on each device, or by using the SMS client to monitor and manage up to 1000 devices. E-Series systems provide Advanced DDoS protection.

You can also implement an optional device called the Zero Power High Availability (ZPHA). This device provides continued traffic in the event of a power loss in your IPS devices.

## High Availability

TippingPoint devices are designed to guarantee that your network traffic always flows at wire speeds in the event of internal device failure. In the case of any internal hardware or software failure, TippingPoint can automatically or manually fall back to be a simple Layer 2 switch, ensuring high-network availability. The TippingPoint System provides Network High Availability settings for Intrinsic Network HA (INHA) and Transparent Network HA (TNHA). These options enact manually or automatically, according to settings you enter using the clients (LSM and SMS) or LCD panel for IPS devices.

Intrinsic Network High Availability is the ability for two SMS systems to act as an active and passive solution for directing the flow of network traffic between SMS systems, devices, and their ports. When traffic flows through the SMS incur issues and interruptions, High Availability enables the passive SMS system to support traffic without a loss in connectivity or flow.

When traffic flows through the ports of a device, one port may 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 and state information by signalling one device, its port, and its client (LSM or SMS) of the IP address, connection table, and flow information. The target port, device, and client then builds the information from scratch, to handle network traffic for optimum usage. It transfers the TCP flow when fail-overs occur.

Transparent Network HA 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.

## IPS Local Clients

The TippingPoint System provides various points of interaction, management, and configuration of the intrusion prevention system. The clients include graphical user interfaces (GUI) and command line interfaces (CLI). These clients include the following:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires access from a supported web browser (Internet Explorer, Mozilla Firefox, and Netscape). Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides reports to monitor the device traffic, triggered filters, and packet statistics.
- **Command Line Interface (CLI)** — Command line interface for reviewing and modifying settings on the device. The CLI is accessible through Telnet and SSH (secure access).
- **LCD Panel** — IPS TippingPoint 50/200/400/1200/2400 devices provide an LCD panel to view, configure and modify some device settings.

## X-Series Devices

The TippingPoint X-Series devices integrate IPS functionality with stateful packet inspection firewall, virtual private network (VPN) management, bandwidth management, and web content filtering.

The X-Series firewall functionality provides service-level, stateful inspection of network traffic. It incorporates filtering functionality to protect mission-critical applications. An administrator can use firewalls and content filters to determine how the system handles traffic to and from a particular service. These filters are specified by the source, destination, and service or protocol of the traffic. The X-Series scans your network and maintains an inventory of the active hosts and services on those hosts. System administrators can use information collected by the X-Series to tune attack and IP filters.

VPN management provides the ability to apply all X-Series functionality across the enterprise, monitoring traffic at the enterprise level and also traffic between main office and branch locations. The X-Series supports IKE, IPSec, L2TP, and PPTP protocols.

Bandwidth management, or policy-based traffic shaping, enables the X-Series to control both inbound and outbound traffic streams, both inside and outside of IPSec VPN tunnels. Using these policies, the X-Series enables users to prioritize real-time business-critical applications, including video and conferencing, IP telephony, and interactive distance-learning over non-essential traffic, such as peer-to-peer file sharing.

Web content filtering provides the tools to enforce network policy by prohibiting the download of non-work-related web sites and offensive or illegal web content.



# Threat Suppression Engine

The Threat Suppression Engine (TSE) is a highly specialized, hardware-based intrusion prevention platform consisting of state-of-the-art network processor technology and TippingPoint's own set of custom ASICs. The TSE is a line-speed, hardware engine that contains all the functions needed for Intrusion Prevention, including IP defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of over 170 network protocols.

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The block of the traffic and packets ensures that the attack never reaches its destination.

The combination of high-speed network processors and custom ASIC chips provide the basis for IPS technology. These highly specialized traffic classification engines enable the IPS to filter with extreme accuracy at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance is affected by the number of filters installed, the highly-scalable capacity of the hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy.

# Threat Management Center

The Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.

The Threat Management Center (TMC) collects threat information and creates Digital Vaccine packages that are made available on the TMC web site. The packages include filters that block malicious traffic and attacks on your network. The filters provide the following protections:

- **Application Protection** — Defend against known and unknown exploits that target applications and operating systems:
  - *Attack Protection filters* — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include the following: Vulnerabilities and Exploits filters.
  - *Security Policy filters* — Detect and block traffic that may or may not be malicious. This traffic may be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to your company's security policies.
  - *Reconnaissance filters* — Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include the following: Probes and Sweeps/Scans filters.
  - *Informational filters* — Detect and block classic Intrusion Detection System (IDS) infiltration

- **Infrastructure Protection** — Protect network bandwidth and network infrastructure elements such as routers and firewalls from attack using a combination of filter types:

- *Advanced DDoS filters* — Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system.
- *Network Equipment Protection filters* — Protect networked equipment from attacks
- *Traffic Normalization filters* — Detect and block abnormal or malicious traffic



**Note** E-Series systems include the **Advanced DDoS Protection option** filters. For more information on upgrading your system with Advanced DDoS Protection, contact your TippingPoint Sales Representative,

- **Performance Protection** — Allow key applications to have prioritized bandwidth access setting that ensure mission critical applications have adequate performance during times of high congestion:

- *Misuse and Abuse filters* — Protect the resources and usage of file sharing across networks and personal computers. These filters protect peer-to-peer services.
- *Traffic Management filters* — Protect the network by shielding against IP addresses or permitting only a set of IP addresses

# 2 Product Overview

*Provides information about SMS components including the server Web site, dashboard and client interface.*

## Overview

The TippingPoint SMS offers centralized control of your TippingPoint system. The SMS is shipped as a management server and includes the SMS client that provides an easy interface for performing secure management tasks for multiple devices. The SMS provides functions similar to the Local Security Manager, but on a larger scale.

This section includes the following topics:

- [“Product Overview: What’s New” on page 10](#)
- [“How To Tasks” on page 10](#)
- [“Product Overview: What’s New” on page 10](#)
- [“SMS Overview” on page 11](#)
- [“SMS Client Interface” on page 16](#)
- [“SMS Dashboard” on page 24](#)
- [“System Preferences” on page 27](#)



**Note** See the Release Notes for specific limitations and known issues regarding the current release.

# Product Overview: What's New

This section outlines the following major changes for the current SMS release:

- [Virtual Segments](#)
- [Digital Vaccine Alert Window](#)

## Virtual Segments

Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events.

## Digital Vaccine Alert Window

When you log on to your SMS server and a new version of the Digital Vaccine is available, an alert window displays. The following options for downloading the package are now available directly from the alert window:

- Activate the new Digital Vaccine and make it the active DV in the SMS
- Distribute the new Digital Vaccine to all the available devices

# How To Tasks

### *SMS Client Interface*

- [“How To: Access the WhoIs Utility” on page 23](#)

### *SMS Dashboard*

- [“How To: Configure the Dashboard” on page 26](#)

### *System Preferences*

- [“How To: Configure Security Preferences” on page 27](#)
- [“How To: Configure Device Preferences” on page 28](#)
- [“How To: Configure Dashboard Preferences” on page 29](#)
- [“How To: Configure Event Preferences” on page 30](#)

# SMS Overview

This section contains the following topics:

- [“Features” on page 11](#)
- [“SMS Components” on page 11](#)
- [“Segments and Security Zones” on page 12](#)

The TippingPoint Security Management System is the control center where you can configure, monitor, and report on the TippingPoint devices in your network. The main components include a rack-mountable SMS Server appliance and a SMS Management Client application. Each SMS can manage hundreds of TippingPoint devices (based on environmental conditions).

## Features

You can use the SMS to create multiple profiles of filters with settings to distribute to specific devices. The devices can be organized in groups or security zones that make it easy to distribute and update security profiles. 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

### Core Components

- **SMS Secure Server** — hardware appliance for managing multiple devices
  - *SMS Home Page* — web-based interface with links to current Client software, documentation, and the Threat Management Center
- **SMS Management Client** — Java-based application for Windows or Linux workstations used to manage your TippingPoint system
  - *Graphical User Interface (GUI)*
  - *Dashboard*
  - *Command Line Interface (CLI)*

### Additional 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.
- **Digital Vaccine (DV)** — Update service that includes up-to-date filter packages for protecting your network
- **Managed Devices** — TippingPoint IPS or X-Family devices that are installed in your network

For descriptions and more information about the TippingPoint System, devices, Local Security Manager, Digital Vaccine, The Threat Management Center, and High Availability, see [“System Overview” on page 1](#).

## Segments and Security Zones

This section contains the following topics:

- [Physical Segments](#)
- [Virtual Segments \(IPS Devices\)](#)
- [Segment Groups \(IPS Devices\)](#)
- [Security Zones \(X-Family Devices\)](#)

### Physical Segments

Physical 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. Sets up a partition for traffic between two physical ports. 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 segment and segment groups.

#### *How It Works*

A segment is protected when its traffic passes through a pair of ports on the IPS that are configured with filters and global settings. The device scans and reacts to network traffic according to the filter instructions, or action set. To protect your network, each segment and device can use a different set of filters to manage and block traffic and malicious attacks. Action sets in these filters provide the instructions for the device to block, permit, and send alerts to the system.

#### *Implementation*

You distribute different profiles to the segments if you want different action sets.

For SMS 2.5 and above, you can rename default segments, but cannot make edits or create new segments.

### Virtual Segments (IPS Devices)

Two virtual ports make up a virtual segment. The SMS can create policies for a virtual segment in a similar manner as it does for a physical segment. Virtual segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events.

#### *How It Works*

Works exactly like physical segments with extra identifier, VLAN ID(s). If the traffic is VLAN tagged, the IPS checks for a virtual segment with the VLAN ID. If a virtual segment exists, the profile is used to determine the response. If there is not a virtual segment, the profile attached to the physical segment is used.

#### *Implementation*

If you want a different response or you want to run reports for a segment, you can create a virtual segment with a set of VLAN ID(s).

The SMS will not add a TippingPoint device that has virtual segments that are invalid for the SMS. Invalid virtual segments include cases where all VLAN IDs do not match each other on both the incoming and outgoing zones, or where the same port is used for both incoming and outgoing zones. These can be identified in the TippingPoint device by examining the System Log for a message similar to "Suspicious in/out combination: no traffic will ever match name1-name2. Please examine your virtual ports and profiles configuration."

## Segment Groups (IPS Devices)

A Segment Group is a grouping of device segments, physical or virtual, that are set up in a specific combination that allows users to maintain settings and files distribution. Users can then associate a particular profile of filters to the segment group. These groups can be used to provide greater management and distribution of profiles and updates for Digital Vaccine, package, TOS software, and SMS software.

### *How It Works*

Segment Groups enhance network security by providing a deep level of customization.

### *Implementation*

Depending upon network settings and architecture, users may need to have differing types and version of filters and action sets running on particular segment.

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, many profiles can point to the same segment. When distributing a profile, the segment replaced the currently used profile.

## Security Zones (X-Family Devices)

A Security Zone is a section of the network that is associated with a port or VLAN. If you need to control the traffic between devices, the devices must be in separate Security Zones. Security Zones enable you to logically segment your networks so that the SMS can apply firewall rules and IPS filters to control the traffic passing between the zones.

### *How It Works*

Any traffic originating from or destined to devices in a zone is directed through the device and policed by firewall policies, if the traffic passes through to another zone. However, traffic moving between devices within any zone that you have defined (intra-zone traffic) is not subject to firewall evaluation or IPS filtering (for example, a user on the LAN zone, accessing the local LAN printer) and does not pass through the device.

### *Implementation*

Although X-Family devices are pre-configured with default security zones, you can modify these or create your own security zones. After security zones are created, they can be associated in zone pairs. Depending the needs of your users and the topology of your network, you can then associate security policies and traffic shaping rules with a security zone.

Each Ethernet port and VPN tunnel is associated with one security zone, unless you use VLANs. If you configure VLANs, then a port can be in more than one security

## Security Levels

Every enterprise has specific needs for network security and protection. You can customize the TippingPoint system to meet the specific needs of your enterprise using the following:

- **Profiles and Filters** — Provide enterprise-wide centralized management for customizing and distributing filters to your devices. You can have multiple profiles with complete sets of filters assigned to actions sets. These profiles can be distributed to specified IPS segments or security zones, providing an enhanced level of customization and protection for your network.
- **Shared Settings** — Provide enterprise-wide settings for filters and their profiles. These settings include action sets, exceptions, IP limitations, and notification contacts.
- **Segment Groups** — Provide enterprise-wide management of device segments. It enables you to group segments of devices together for receiving distributions of profiles. You can also use these groups for generating reports and searching for events.
- **Security Zones** — Enable you to logically segment your networks so that the SMS can apply firewall rules and IPS filters to control the traffic passing between the zones.



**Note** Virtual segments are used with V2.5 and above device. For V2.5+ and above, physical segments can be used but cannot be not created. Security zones are used with X-Family devices. For more information, see [“IPS Devices: Network Configuration” on page 366](#) and [“Network Configuration: Segments/Zones Tab” on page 395](#).

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

- **Enterprise-wide** — These settings affect all device, segments, security zones on your network and take effect when you distribute a profile to that device. This level includes some of the settings for Profiles and the filters of these profiles, including action sets, shared exceptions, and notification contacts. These profile settings are called Shared Settings.
- **Device-wide** — These settings affect all of the segments or security zones on a particular device. Examples of these are Scans/Sweeps and Traffic Normalization filters. TOS updates, Digital Vaccine, and Custom Shield packages also fall under this type of protection. When you can distribute these packages to a particular device, they affect all segments on that device.
- **Segmental** — These settings affect only a particular segment or segment group; segmental setting do not affect an entire device. Examples of these include most Application Protection, Infrastructure Protection, and Performance Protection filters grouped as profiles.

Each filter, action set, notification contact, and Digital Vaccine package affects your devices and segments according to these levels of security. Enterprise-wide changes affect all devices and supersede device-wide and segmental settings. And Device-wide changes supersede Segmental settings.

This guide details how to modify and manage all of the components to creating enhanced intrusion prevention network security as generally discussed in this section.



# SMS Server Web Site

You can access the SMS Server Web site to download and install the SMS Client as well as access saved reports and database backups. To access the Web site, use Microsoft Internet Explorer. In the **Address** field, enter:

`https://<smsipaddr>`

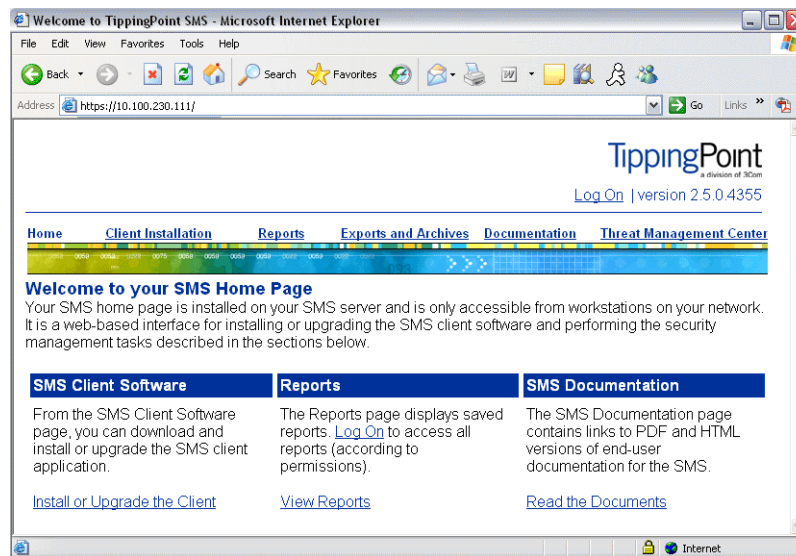
where **<smsipaddr>** is the IP address you configured for your SMS.

When you access the Web site, the Web page may prompt for a username and password. The login information is your SMS Client login.

If the Web site does not prompt for a login, you can always log into the web server using the Login link under the TippingPoint logo. Logging into the site may enable options such as displayed reports and archived files depending on your user account roles and security settings.

The following screen is the SMS Server Web site

Figure 2 - 1: SMS Server Web site



Through the Web site, you can access the following:

- **SMS Client Installation and Upgrade** — This page provides instructions and links to the SMS Client installation and upgrade files. Follow the documented instructions on the page for these options. For instructions, see [“Install the SMS Client” on page 35](#).
- **View Reports** — Through the **Reports** — **Scheduled Reports** option, you can send completed reports to the SMS Server. You can access this option to view and download reports sent to the SMS Server. See [“Reports” on page 16](#).
- **View Exports and Archives** — The page provides a link to display the exported and archived files sent to the SMS Server, such as database backups.
- **View Documentation** — The page provides access to the SMS documentation from the SMS Server.
- Open the **Threat Management Center** — The page provides a link to the TMC Web site

## Reports

When you review reports through the SMS Web Server Web site, the SMS displays reports according to the following:

- **Scheduled report generation settings** — Scheduled reports include settings to display for specific users. If you login to the Web site, you may display reports according to account settings.
- **User account security access** — The web page displays reports according to the security settings of your SMS Client account, such as accessible segment groups, devices, and profiles.

To view reports, click **Reports** from the menu items and select a report. The available results display on the page. You can select the file type for the report. The name “Adhoc” displays for reports run one time. For the latest generated report, click the **most recent result** options. The file types include:

- pdf — PDF generated file accessible using Adobe Reader
- csv — Comma delimited file
- xml — XML version of the data

# SMS Client Interface

The SMS client interface consists of two main windows: the Dashboard and main user interface. When accessing the SMS, these two windows display. The Dashboard gives you an overview of attacks detected and blocked, device performance, and system statistics. The main user interface provides the functions and windows to manage your system. Through the interface, you can do the following:

- Manage profiles of filters for the device(s)
- Update operating system and Digital Vaccine packages
- Manage user access and accounts
- Monitor devices, services, and logs
- Generate and review reports on performance

This section includes the following items:

- [“Notifications Window” on page 17](#)
- [“Digital Vaccine Alert Window” on page 17](#)
- [“Main User Interface” on page 18](#)
- [“Interface Screens” on page 21](#)
- [“Navigating Screens” on page 22](#)
- [“WhoIs Utility” on page 23](#)

## Notifications Window

When you log on to your SMS server, a **Notifications** window may be displayed in front of the SMS Dashboard. This window provides information regarding the current status of your SMS. After reading the message(s), click the **OK** button to close the window.

## Digital Vaccine Alert Window

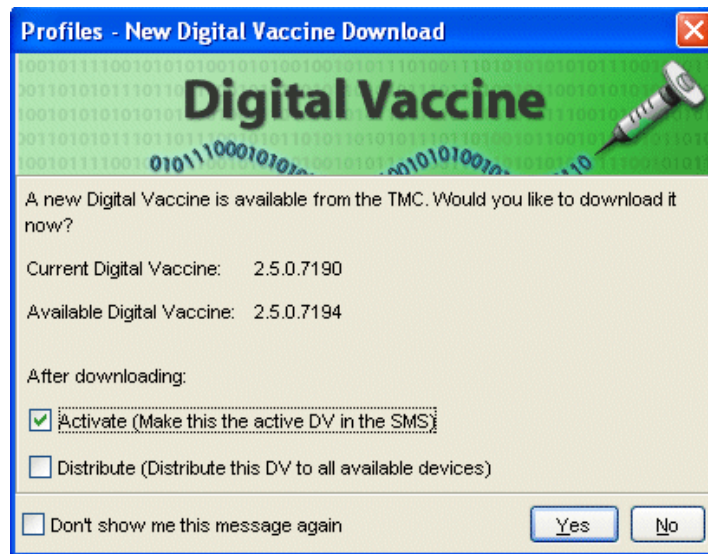
When you log on to your SMS server, a Digital Vaccine Alert Window may display and indicate that a new version of the Digital Vaccine is available. The SMS provides information about the new version of the package and the following options for downloading the package:

- Activate the new Digital Vaccine and make it the active DV in the SMS
- Distribute the new Digital Vaccine to all the available devices



**Note** If you do not want to activate a Digital Vaccine when downloading it, deselect that option when prompted to download a new DV and also on the Digital Vaccine management screen in the Profiles area of the SMS. See [“Digital Vaccine Management” on page 246](#).

Figure 2 - 2: SMS Digital Vaccine Alert Window



## Main User Interface

The main user interface provides and displays all components you need to manage and maintain your TippingPoint system. The interface works much like a web browser, allowing you to make selection from a tool bar, menu bar, and navigation pane. The interface opens dialog boxes as appropriate for creating, editing, and validating changes in system data.

This section includes the following descriptions:

- [“Menu Bar” on page 19](#)
- [“Toolbar” on page 20](#)
- [“Navigation Pane” on page 20](#)
- [“Main/List Pane” on page 21](#)

The following is the SMS main user interface:

Figure 2 - 3: SMS Main User Interface

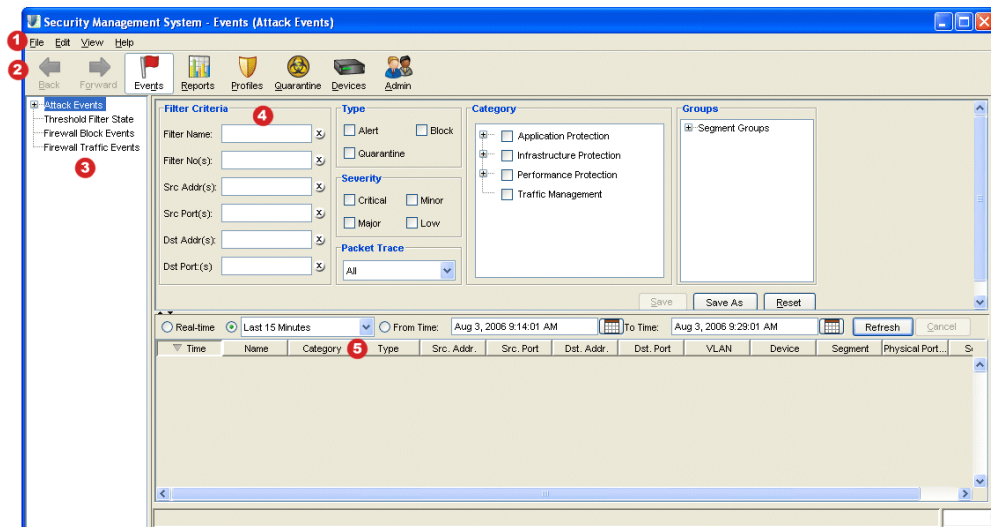


Table 2 - 1: Events Screen - Interface Description

Item No.	Item	Details
1	Menu Bar	Options may vary based on screen
2	Tool Bar	Navigate to other SMS areas
3	Navigation Pane	Click + to expand listings
4	Query Pane	Enter query criteria
5	Column Heading	Right-click for more options

## Menu Bar

The Menu Bar provides drop-down menus of options for using SMS features. The provided options differ according to the selected and displayed screen. The drop-down options include the following:









- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. You can **Logoff** and **Exit** the application from this menu.
- **Edit** — Provides edit options based on the currently selected and displayed screen.
- **View** — Displays the screens for the options listed in the Navigation Pane.
- **Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

For more information on the specific options per screen, see the related screen section in this guide.


## Toolbar

The Toolbar provides the key functions of the SMS. As you click on each button on the Toolbar, the Navigation and Main/List panes display functions appropriately. The Toolbar includes the following options:

Table 2 - 2: Toolbar Buttons

Button Image	Name	Description
	Back	Moves back a level as you select options in the SMS application. The <b>Back</b> button works much as the back button in a web browser.
	Forward	Moves forward a level as you select options in the SMS application. The <b>Forward</b> button works much as the forward button in a web browser.
	Events	Displays the default <b>Events</b> screen. Allows you to manage and view events such as attack and health events.
	Reports	Displays the default <b>Reports</b> screen. Allows you to use report related functions to generate, download, and view reports of performance, filters, and logs.
	Profiles	Displays the default <b>Profiles</b> screen. Allows you to use package related functions such as profiles and filters, global settings, Digital Vaccine packages, and custom shield packages.
	Quarantine+	Displays the default Quarantined Hosts screen. Allows you to create and maintain quarantine actions and policies for the SMS. You can also manually add and remove quarantined hosts from the queue.
	Devices	Displays the default <b>Devices</b> screen. Allows you to use device related functions such as monitoring and managing device features, update the operating system, and manage device groups.
	Admin	Displays the default <b>Admin</b> screen. Allows you to use administration related functions such as user access and accounts.

## Navigation Pane

The Navigation pane provides the functions for each screen of the application. When you select an option from the Toolbar, the Navigation pane displays the available options and functions. Functions may have multiple levels, shown with an expand icon, . The options listed in the Navigation pane

display on the View drop-down menu from the Menu Bar. The contents of the Navigation pane change with each selected and displayed screen.

The following is an example of a Navigation pane:

Figure 2 - 4: Navigation Pane Sample



## Main/List Pane

The Main/List pane of the application 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 change depending on the currently selected option from the Navigation pane, Toolbar, or Menu Bar.

This pane is called main and list because it may display items in a list format. It is the central area of the user interface, providing functions and features according to selections made in the application. In this pane you can do the following to navigate:

- **Sorting** — You can click on a column name to sort displayed content. Clicking the column header toggles between ascending and descending sort.
- **Right-Clicking** — You can right-click on a selected entry to perform actions on the entry.
- **Double-Clicking** — You can double-click on an entry to open the entry for viewing/editing.
- **Using Menu Bar Options** — You can select an entry and use options from the Menu Bar. Options differ on the screen displayed.

## Interface Screens

The SMS user interface includes a set of main screens that display according to your selections on the Toolbar. These screens provide the central options and functions of the SMS, changing the selections and data displayed in the Navigation and Main/List panes.

The SMS include the following screens:

- [“Events” on page 22](#)
- [“Reports” on page 22](#)
- [“Profiles” on page 22](#)
- [“Quarantine” on page 22](#)
- [“Devices” on page 22](#)
- [“Admin” on page 22](#)

### Events

The **Events** screen generates and displays information regarding the system's behavior in real time. The **Events** screen graphically depicts the IPS devices you are managing and the hosts on those devices. 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. See [Chapter 4. "Events"](#).

### Reports

While the Events window provides real-time information, the **Reports** screen accumulates the data collected by the devices and the SMS to create historical reports. These reports detail the threats encountered by the entire system and show processing trends. The **Reports** screen also provides real-time assessments of the IPS network statistics. See [Chapter 5. "Reports"](#).

### Profiles

The **Policy** screen provides a comprehensive, centralized interface for tuning your system's behavior by managing, editing, and applying profiles, filters, Digital Vaccine, action set, and notification contact updates across your TippingPoint system. See [Chapter 6. "Profiles"](#).

### Quarantine

The **Quarantine** screen provides a centralized interface for managing quarantine actions and policies for the SMS system. You can also manage quarantined hosts from this screen. See [Chapter 7. "Quarantine"](#).

### Devices

The SMS provides a mechanism for centrally managing the configuration of your TippingPoint system. On the **Devices** screen, you can add a new IPS to the SMS management view, adjust configuration parameters for existing devices, and review discovery information. See [Chapter 8. "Devices"](#).

### Admin

The **Admin** screen provides management options for user access, the system and audit logs, and system settings. Only users with the correct role and access can manage settings on the **Admin** screen. See ["Administration" on page 431](#).

## Navigating Screens

To access screens, select an option from the navigation pane. The screen displays in the main pane. In the main pane, screens may have buttons to click, lists of entries, column headers for these lists, and sections to enter or modify values and apply the changes.



## Lists of Entries

You can select listed entries in the main pane and perform functions on them in various ways. You can access these entries in the following ways:

- **Right-click** — You can right-click a selected entry to display a drop-down list of options. These options differ according to entry type and screen. You can use this option on the **Packages** screen.
- **Double-click** — You can double-click an entry to view/edit it.
- **Select and Use Menu Options** — You can select an entry by clicking it once. You can then access and select menu options from the Menu Bar. The available options differ depending on the type of selected entry, screen, function, and user access settings.
- **Select and Use Buttons** — You can select an entry by selecting it once and click a button for an action. These actions differ according to selected entry and screen, such as Edit, Delete, and Create Exception.

## Buttons

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.

## WhoIs Utility

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. You can have the utility running while you review events.

See also [“How To: Access the WhoIs Utility” on page 23](#).

### How To: Access the WhoIs Utility

1. Select the **View** —> **WhoIs Utility** menu item.
2. In an **Event Details** screen, click **WhoIs Utility**.

When an attack occurs, it displays in the **Events** screen. As you query and list events, you can select an event entry. If you have the WhoIs Utility open, you can auto-fill the utility with the event's destination and source IP addresses by right-clicking the event entry.

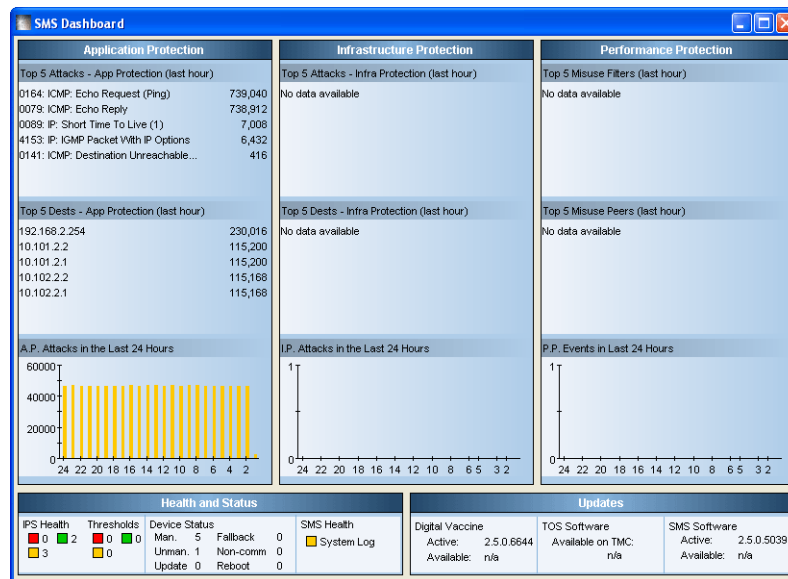
You can also enter a source or destination IP address in the **Domain** field. A list of administrative contacts displays for the domain. To clear the list, click **Clear**.

# SMS Dashboard

When you access the SMS application, the dashboard displays. The dashboard provides a centralized access to reviewing the status of the system. You gain a quick review of the system from this window according to the pillars, or types, of filters on the system. The information displays as graphs and text of attack reports and device health.

The following is the SMS Dashboard:

Figure 2 - 5: SMS Dashboard



The Dashboard displays attack data for the past hour and 24 hours according to the runtime. You can select an entry to display the event in the **Events** screen. The displayed information includes the IP address and total count of hits detected by the system. It also displays device health and available updates. You can click the entries in the **Health and Status** section to display the **Devices - All Devices** screen. You can select the entries in the **Updates** section to download and install the latest SMS software and Digital Vaccine updates.

The Dashboard displays the data in the following sections:

- **Three Customizable Tiers** — Displays three customizable report queries. You can customize the displayed report or chart results through the **View** → **Dashboard** → **Customize** menu option. See [“Dashboard Configuration” on page 25](#). You can select the displayed report or chart to open the

report in the **Reports** screen. The following three tiers are the default tiers that display when the client is first installed:

- **Application Protection** — Displays the top 5 triggered attack and destination filters (in the past hour) and a graph of all attacks triggering Application Protection filters triggered in the past 24 hours.
  - **Infrastructure Protection** — Displays the top 5 triggered Traffic Normalization filters and top 5 DDoS/Network Equipment Protection filters (in the past hour) and a protocol graph of all attacks and protection initiatives triggered within the past 24 hours.
  - **Performance Protection** — Displays the top 5 triggered peer-to-peer application filters and peers (in the past hour) and all Performance Protection events within the past 24 hours.
- **Health and Status** — Displays the number of devices in the health state (not the number of health events or device health items). The health reflects the logged health of the device. When you click the device health, it displays the **Devices - All Devices** screen, providing a view of all devices with details on health, status, and alerts.
  - **Updates** — Displays the current updates available or installed and the health of the updates. The number is the build number for the type of software or package file.

Through this screen, you can review the status and health of the SMS. It provides a graphical review of attacks, blocks, performance, health status, and running software versions. For more information, see the sections that detail and provide more information in [“Interface Screens” on page 21](#).

To enhance the quick view statistics, you can configure the Dashboard to display specific reports in the three report tiers. See [“Dashboard Configuration” on page 25](#).

## Dashboard Configuration

You can configure the displayed information on the SMS Dashboard. The Dashboard consists of three tiers of reports, each tier containing three report result displays. You can rename and select the reports for each tier in the section.

You can review report selections through the configuration screen. The saved reports display according to the filter pillar: Application Protection, Infrastructure Protection, and Performance Protection. To aid in selecting reports, you can navigate the report tree in the **Available Reports** section. The section allows you to view the details of a report, providing a preview of available reports by name and type (such as report or chart).

When selecting reports to display, the Dashboard may refresh at different rates. The SMS Dashboard refreshes every five minutes for reports and two minutes for charts. The **Available Reports** section details the type of report output as report or chart when selecting entries for the Dashboard.

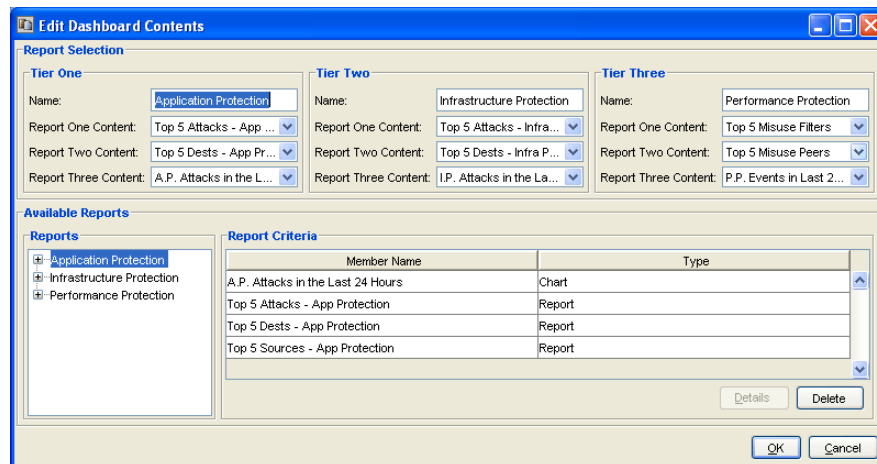
To configure the display preferences for the Dashboard, see [“Dashboard Preferences” on page 29](#).

See also [“How To: Configure the Dashboard” on page 26](#).

## How To: Configure the Dashboard

1. On any screen in the SMS Client, select **View** —> **Dashboard** —> **Customize** from the Menu Bar. The Dashboard Configuration dialog box displays.

Figure 2 - 6: Dashboard Configuration Dialog Box



2. In the **Report Selection** section, configure the three tiers of displayed information. For each tier, do the following:
  - Enter a **Name** for the section of the Dashboard. For example, Application Protection.
  - For the **Report One Content**, select a report from the drop-down menu.
  - For the **Report Two Content**, select a report from the drop-down menu.
  - For the **Report Three Content**, select a report from the drop-down menu.



**Note** To determine which reports you would like to display, use the **Available Reports** section to browse and preview the reports. You can view their details or delete reports by selecting and clicking **Details** or **Delete**.

3. After configuring the display sections for the Dashboard, click **OK**.

# System Preferences

To provide better performance and enhanced control, the **System Preferences** dialog box provides configuration setting for devices, the dashboard, and views. These controls include the following:

- [“Security Preferences” on page 27](#)
- [“Device Preferences” on page 28](#)
- [“Dashboard Preferences” on page 29](#)
- [“Events Preferences” on page 30](#)

## Security Preferences

The SMS provides a preference option for enabling a password for the SMS Server web interface. You can set the password requirement and security level for the login. SMS users can then use their account to log into the SMS Server web interface. For more information on the web options, see [“SMS Overview” on page 11](#).

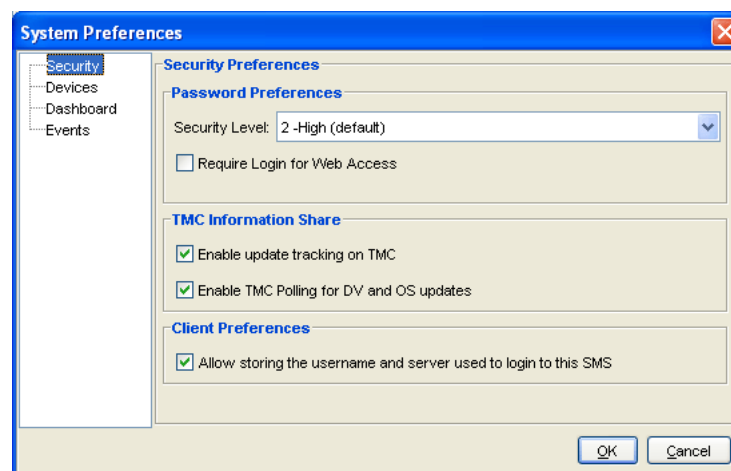
On this screen, you can also enable information sharing with the TMC. Enabling this feature allows you to track the TippingPoint OS(TOS), SMS, and Digital Vaccine image update history for the SMS and all devices under management. This information is securely uploaded to the Threat Management Center (TMC) and serves as a historical record that can be used by technical support personnel and you for trouble shooting and incident correlation.

See also [“How To: Configure Security Preferences” on page 27](#).

### How To: Configure Security Preferences

1. In any screen, select the **Edit** —> **Preferences** option from the Menu Bar. The **System Preferences** dialog box displays.
2. Select **Security**. The **Security Preferences** screen displays.

Figure 2 - 7: System Preferences - Security Screen



3. To enable security, select the **Require Login for Web Access** check box.
4. For the **Security Level**, choose a level: **0 - Low**, **1 - Medium**, or **2 - High**. For more information on levels, see [“Passwords” on page 447](#).
5. In the **TMC Information Share** section, select the **Upload device information to TMC** check box. This option exports configuration data to the TMC.
6. Click **OK**.

## Device Preferences

The SMS provides a preference option for enabling device communication checking. Once enabled, the option includes configuration settings for the following:

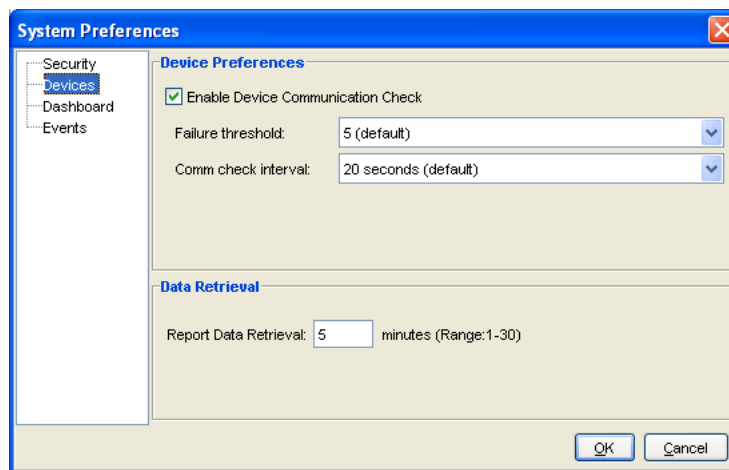
- Device timeout
- Maximum number of retries
- Device failure threshold
- Amount of device check intervals

See also [“How To: Configure Device Preferences” on page 28](#).

### How To: Configure Device Preferences

1. In any screen, select the **Edit** —> **Preferences** option from the Menu Bar. The **System Preferences** dialog box displays.
2. Select **Devices**. The **Devices Preferences** screen displays.

Figure 2 - 8: System Preferences - Devices Screen



3. Select the check box to **Enable Device Communication Check**. Once enabled, you can configure the check parameters.
4. For **Timeout**, select a value from the drop-down menu: 0, 1, 2, 3, 4, 5, 10, 20.

5. For **Retries**, select the number of retries allowed from the drop-down menu: 0, 1, 2, 3, 4, 5, 10, 20.
6. For **Failure Threshold**, select a threshold amount: 0, 1, 2, 3, 4, 5, 10, 20.
7. For **Comm check interval**, select an amount of time between checks: 20 seconds, 30 seconds, 1 minute, 5 minutes, 10 minutes.
8. Click **OK**.

## Dashboard Preferences

These controls determine if users can see or interact with charts and reports through the Dashboard. If these options are not enabled, Admin and Operator users may only see the Health and Update status sections of the Dashboard. If you disable the display of reports, the dashboard will not display any reports for all users. When enabled, the Dashboard periodically refreshes to display the latest information. By turning off this option, you can increase performance and restrict the access of some information. These options include the following:

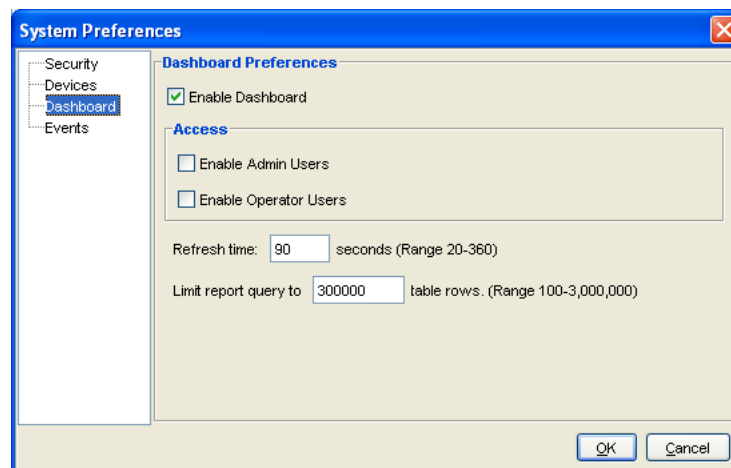
- Enables or disables the display of reports for all users from the Dashboard
- Access control for Admin and Operator users
- Amount of time in seconds for refreshing
- Limit query to an amount of rows

See also [“How To: Configure Dashboard Preferences” on page 29](#).

### How To: Configure Dashboard Preferences

1. In any screen, select the **Edit** —> **Preferences** option from the Menu Bar. The **System Preferences** dialog box displays.
2. Select **Dashboard**. The **Dashboard Preferences** screen displays.

Figure 2 - 9: System Preferences - Dashboard Screen



3. Click **Enable** to enable display of reports on the Dashboard. If you disable report display, the dashboard will not display the reports for any user.
4. For **Access**, click the check boxes for Dashboard access for **Admin** and **Operator** users.
5. Enter a value for the **Refresh time (seconds)**.
6. Enter a value to limit the report query to a number of rows for the **Limit report query to** option.
7. Click **OK**.

## Events Preferences

On this screen, you can enable or disable DNS Auto-lookup.

See also [“How To: Configure Event Preferences” on page 30](#).

### How To: Configure Event Preferences

1. In any screen, select the **Edit** —> **Preferences** option from the Menu Bar. The **System Preferences** dialog box displays.
2. Select **Events**. The **Events Preferences** screen displays.
3. To **Enable DNS Auto-lookup**, click the check box.
4. Click **OK**.



# 3

## Getting Started

*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.*

### Overview

This section includes the following topics::

- [Getting Started: What's New](#)
- [How To Tasks](#)
- [Updating Existing Systems](#)
- [Installing the SMS Client](#)
- [Logging On to the SMS Client](#)
- [Performing Initial Management Tasks](#)

Prior to using the SMS server, you need to install and perform configuration procedures on all the components of the SMS system. For complete instructions, see the ***SMS Installation and Configuration Guide*** that shipped with your system.



**Note** The TippingPoint systems have a full set of documentation. These publications are available in electronic format on your installation CDs. For the most recent updates, check the Threat Management Center (TMC) web site at <https://tmc.tippingpoint.com>.

Before you begin, make sure you complete the following items:

- **Hardware Installation** — Prepare your environment, install the server in a rack mount, and connect it to the network
- **SMS Server Setup Wizard** — Configure the server.
- **SMS Client Application** — Install and configure the client interface
- **Software & Device Preparation** — Download the most current Digital Vaccine packages from the TMC, add one or more IPS devices to the SMS, and distribute the security packages to those devices.

Gather the following documents depending on your system:

- The Release Notes that shipped with the product. For updated release notes, visit the Threat Management Center Web site (<https://tmc.tippingpoint.com>)
- Installation, configuration and User's Guide for the TippingPoint devices that the SMS will manage.

After you connect to the SMS using one of the methods described in the SMS Installation and Configuration Guide, you have access to the SMS command line interface (CLI). As the SMS is starting up, a TippingPoint splash screen is displayed for up to 90 seconds on the VGA monitor. Then, a series of system status messages is displayed to the console. Next, a logon prompt appears. At first, you must log on as **SuperUser**. This gives you access to the SMS CLI.



**Note** You do not need a password when you first log on to the CLI. Make sure that an authorized user sets up your SMS.

# Getting Started: What's New

## *Hardware Requirements*

For SMS Client V2.5 and above, the workstation must have 120 MB of disk space.

## How To Tasks

- [“How To: Update Software” on page 34](#)
- [“How To: Install the SMS Client” on page 35](#)
- [“How To: Log On to the SMS Client” on page 36](#)

# Updating Existing Systems

This section contains the following topics:

- [“Software Updates” on page 33](#)
- [“Migration” on page 34](#)

## Software Updates

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the Threat Management Center (TMC) makes these available to customers in the form of SMS software, TippingPoint operating system (TOS), Digital Vaccines, and SMS software updates provide improvement in functionality and default filter signatures for managing and protecting your network security. The TippingPoint operating system (TOS) provides updates for the operations and functions for your devices. The TOS updates the available functionality, behavior, and performance of these devices. For more information about TOS updates, see [“TippingPoint OS” on page 332](#).

Filter packages include updated and new filter options investigated and distributed by the Threat Management Center (TMC). These packages are continually updated to fortify your system against new malicious attack alerts threatening all hosts and network services. You can install these filters by downloading and installing or importing a Digital Vaccine. Digital Vaccine filter packages contain newly developed filters along with improvements to existing filters.

**IMPORTANT! Make sure your system meets TMC port requirements. See [“Port Information” on page 557](#).**

You can also create your own filters using the TippingPoint Custom Shield Writer™. The application creates Custom Shield packages that you can distribute like Digital Vaccine packages in the system. The TMC notifies you that new packages are available through the SMS Dashboard and **Packages** screen.



**Note** To view information about updates and device inventories, you must have Operator authority. To distribute packages, rollback inventory information, and manage distribution entries, you must have Administrator authority. To do all of the above and import security packages from an IPS, you must have Super User authority. For more information about user authority, see [“Administration” on page 431](#).

If you use the SMS to manage your devices, it is recommended that you use the SMS to download and distribute packages. If you download Digital Vaccine to an IPS and not to the SMS, the SMS reports the events passed to it from the IPS device, but 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 at least some of the filters contained in a new filter package. You might also need to add IP filters and enable or edit anomalies. The customizations and additions you make in Filters are bundled into a *profile*. Once you make these changes, you must distribute them to the appropriate IPS devices.

### How To: Update Software

You can update software through the following screens:

- **Digital Vaccine and Custom Shield packages** — You can update Digital Vaccine files and import Custom Shield packages through the **Profiles** screen. See [Chapter 6, “Profiles”](#) for more information.
- **TippingPoint Operating System** — You can update the TOS for your devices through the **Devices** screen. See [Chapter 8, “Devices”](#) for more information.
- **SMS Software** — You can update the SMS software through the Admin screen. See [“Administration” on page 431](#) for more information.

## Migration

To migrate to the new version, you perform an update of the current software to the new release. See [“How To: Update Software” on page 34](#) and [“How To: Install the SMS Client” on page 35](#).

For information on migration issues, refer to the SMS Release Notes that are available through the Threat Management Center (TMC) web site at <https://tmc.tippingpoint.com>.

# Installing the SMS Client

The SMS Client software contains a Java-based interface through which you manage your TippingPoint system. You download, install, and run the SMS Client on a Windows or Linux operating system. The SMS Client installation software is available from your SMS server's home page using a web browser.

During the installation process, the installer checks for currently installed versions of the client. Depending on the findings, the application displays options for installing or updating the software. You can make selections, perform the installation, and review progress through the installation process for Windows and Linux systems. When complete, the application prompts you to end or open the client upon completion. For SMS Client V2.5 and above, the workstation must have the following:

- Windows NT 4.0, Win 2000, Windows 98, XP, or Linux
- 700 MHz Pentium III or equivalent
- SVGA resolution (1024 x 768)
- 256 Mb of RAM
- 120 Mb of disk space

See also [“How To: Install the SMS Client” on page 35](#).

## How To: Install the SMS Client

1. On your workstation, open a web browser.
2. In the **Address** field, enter: `https://<smsipaddr>`  
where **<smsipaddr>** is the IP address you configured for your SMS.
3. If the Web site prompts for login, enter your username and password in the dialog box.
4. On the SMS home page, click the **Install or Upgrade the Client** link under SMS Client Software.
5. Select a Windows or Linux version.
  - For Windows, in the **Download Complete** dialog, click **Open** to start the SMS Client installer.
  - For Linux, from the directory containing the installer, run `chmod 755 SMSInstall.sh; ./SMSInstall.bin`.
6. Follow the instructions for the installer. The installation wizard begins with a scan of your system.
  - If the system does not have a previous SMS client installed, it indicates steps and actions to install the application.
  - The wizard will prompt you to accept a license agreement to proceed.
  - If the system has a previous SMS client installed, it informs you that a version is detected and provides an option to continue and upgrade the current version or change directories retaining the older version.  
If you decide to upgrade your current version, and it is older than V 2.2, the installer will prompt to uninstall the current version prior to upgrading. Perform the uninstall and proceed with the new installation.
  - The installation wizard continues with messages and information regarding the new client and locations for shortcuts. Each step may include further options and progress indicators.
7. When complete, you can access the client from the Start menu. Start the client by double-clicking the TippingPoint SMS Client icon on your desktop.

Figure 3 - 1: SMS Client Icon



8. After installing and opening the application, you should download, install, and activate the latest Digital Vaccine from the TMC Web site. See [“Firewall Profiles \(X-Family Devices\)” on page 237](#).

## Logging On to the SMS Client

When you start the SMS client, the SMS **Log On** dialog box is displayed. It includes the following fields:

- **SMS Server**—the IP address or fully qualified hostname of the SMS server
- **Username**—a user name for a user account defined on the SMS
- **Password**—the password defined for that user account

If you log into multiple SMS systems with the client, the opening screen saves the IP addresses in a drop-down list. For full information on account settings, see [“Administration” on page 431](#).

See also [“How To: Log On to the SMS Client” on page 36](#).

### How To: Log On to the SMS Client

1. Double-click the TippingPoint SMS Client icon on your desktop. The SMS Log On screen displays.

Table 3 - 1: SMS Logon screen



2. In the **SMS Server** field, type the IP address or fully qualified hostname of your SMS Server.
3. In the **Username** field, type your user ID. For initial configuration, use **SuperUser**.
4. In the **Password** field, type the password you defined in the SMS Setup Wizard.
5. Click **Login**.

At the bottom of the dialog box, the status message **Attempting to connect** is displayed. After a few seconds, the message **Connected, logging in** appears. When you log in successfully, the SMS Dashboard displays. Your access to functionality is limited by the role assigned to your user account. To



**Note** If you see the error message “Connect Failed”, verify that you have entered the correct IP address or full qualified host name for the server. You might also need to verify that the server is properly connected to the network and that the network is up.

**Note** If you see the error message “Can’t authenticate! Retype and try again,” verify that you have typed the correct username and password.

**Note** You can verify network connectivity by trying to open the SMS home page through the Internet Explorer browser. The default configuration of the SMS does not respond to pings.

view the role for your account, see [“My Account” on page 37](#). For detailed information about user roles, see [“Administration” on page 431](#).

## Performing Initial Management Tasks

This section contains the following topics:

- [My Account](#)
- [Date and Time Controls](#)

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

- Add one or more IPS devices. See [“Adding a Device” on page 319](#) for detailed instructions.
- Download the latest Digital Vaccine package from the Threat Management Center (TMC).
- Distribute Digital Vaccine packages to your IPS devices.



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


When the distribution is complete, the TippingPoint system immediately begins blocking traffic that belongs to the Vulnerability—Default category. All other categories are disabled. For details about the Vulnerability—Default category and other categories, see [“Threat Management Center” on page 7](#) and [Chapter 6. “Profiles”](#).

### My Account

In the window title bar of the Dashboard, the hostname of the server and your user account name are displayed. You can view more details about your user account by choosing the System—>My Account menu command. This opens the **Admin—Edit User** dialog box. The information loaded in this screen is specific to the username with which you logged in to the SMS. For more information about the Edit User dialog, see [“Administration” on page 431](#).

### Date and Time Controls

Some of the SMS windows and dialog boxes contain date and time controls that allow you to specify a specific date and time or range of dates and times for performing certain functions. To use these

controls, click on the calendar icon to the right of the date and time field. 

A pop-up calendar is displayed. Use the calendar to select a data and time or a range to apply to your task.





# 4 Events

*The Events screen organizes and displays information about your TippingPoint system's response to attack traffic.*

## Overview

This section includes the following topics:

- [“Events: What’s New” on page 40](#)
- [“How To Tasks” on page 41](#)
- [“Navigation and Menu Options” on page 42](#)
- [“Event Monitoring” on page 54](#)
- [“Managing Queries” on page 60](#)
- [“Tuning the System” on page 61](#)
- [“Threshold State” on page 64](#)
- [“Firewall Events \(X-Family Devices\)” on page 66](#)

The TippingPoint system responds to attack traffic according to the action set included in the attack filter. When the action set for the filter includes instructions to notify the management console, the attack event displays on the **Events** screen.

The **Events** screen provides a number of options for monitoring attack detection and responses of your TippingPoint system. Through this screen, the SMS enables you to create and run queries regarding attacks against the accumulated audit and system logs of the TippingPoint system. You can save these queries to run as needed. The SMS provides export functionality to save the results to a comma- or tab-delimited file.

You can view detailed information about an attack including, in some cases, the contents of packets that comprised that attack. To aid with diagnostics, you can export attack data to an external file and generate attack reports.



**Note** To view information about attacks, you must have Operator authority. To create or edit attack filters and related objects, you must have Super User or Administrator authority. For more information about user authority, see [“Administration” on page 431](#).

The **Events** screen also provides information about triggered Traffic Threshold filters and firewall actions. Traffic Threshold filters can be directly edited through the Events Screen.

For more information on viewing and reporting events other than attack events, see the following chapters:

- [Chapter 5. “Reports”](#) — Provides reports for reviewing all types of events in the system
- [Chapter 7. “Quarantine”](#) — Provides features to block or mitigate malicious traffic
- [Chapter 8. “Devices”](#) — Provides system and audit logs according to selected device
- [Chapter 9. “Administration”](#) — Provides system and audit logs for the SMS system

## Events: What’s New

This section outlines the following major changes for the current SMS release:

- [Virtual Segments](#)
- [Category Settings](#)
- [Save Exported Queries to the SMS Server](#)

### Virtual Segments

Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events.

See [“Network Configuration: Segments/Zones Tab” on page 395](#).

## Category Settings

The V 2.5 release of the TippingPoint SMS has new category settings. In addition, some existing category settings were renamed.

### *New Category Settings*

- Vulnerabilities and Exploits
- Virus
- Spyware
- Identity Theft
- Instant Messaging
- Streaming Media

### *Renamed Category Settings*

- Misuse and Abuse - Renamed to Peer to Peer (P2P).
- Informational - This category was removed. The majority of filters in this category were moved to the Security Policy category.

## Save Exported Queries to the SMS Server

You can now save exported queries to the SMS Web server. This feature makes the query results available as a comma- or tab-delimited file that can be downloaded from the Reports section of the SMS Web home page.

# How To Tasks

### *Event Monitoring*

- [“How To: Display the Events Screen” on page 42](#)
- [“How To: Customize the List Pane” on page 48](#)
- [“How To: Update Displayed Results” on page 49](#)
- [“How To: View an Attack Event” on page 58](#)
- [“How To: View the Packet Trace” on page 58](#)
- [“How To: Sort Query Results” on page 48](#)
- [“How To: Create a Query” on page 56](#)
- [“How To: Create a Query with the Taxonomy Tab” on page 56](#)
- [“How To: Export Query Results” on page 59](#)

### *Managing Queries*

- [“How To: Edit a Saved Query” on page 60](#)
- [“How To: Delete a Saved Query” on page 61](#)

### *Tuning the System*

- [“How To: Edit the Attack Filter” on page 62](#)
- [“How To: Create a Filter Exception” on page 63](#)

### *Threshold State*

- [“How To: Edit a Traffic Threshold Filter” on page 65](#)
- [“How To: Reset a Traffic Threshold Filter” on page 66](#)
- [“How To: Reset All Traffic Threshold Filters” on page 66](#)

### *Firewall Events (X-Family Devices)*

- [“How To: Display the Firewall Block Events Screen” on page 67](#)
- [“How To: Customize Displayed Results” on page 68](#)
- [“How To: Display the Firewall Traffic Events screen” on page 69](#)

## Navigation and Menu Options

The Reports screen includes the following panes and options:

- [Main Screen](#)
- [Navigation Pane](#)
- [Query Pane](#)
- [List Pane](#)
- [Menu Bar Options](#)

### Main Screen

The **Events** screen lists the events logged by the SMS. The screen includes a Navigation pane with options that display in the main pane. The options available include attack event and health events. When you select a type of event, the main pane contains a query pane and a list pane. The query pane includes options that allow you to enter criteria for searching and listing events. The events that meet the search criteria are displayed in the list pane. You can then locate and open an event from the list pane items.

#### How To: Display the Events Screen

Click the **Events** button on the Toolbar. The screen displays the **Events - Attack Events** by default. The following figure shows the **Events** screen:



**Note** The time displayed in the Attack Time column for attacks reflects the time of the actual attack on the IPS. This might not correspond to the SMS Receipt Time or the Device Log Time reported in the Attack Details dialog box. The differences might depend on the timekeeping configuration of the IPS and SMS systems, and on the speed of the network.

Figure 4 - 1: Events Screen

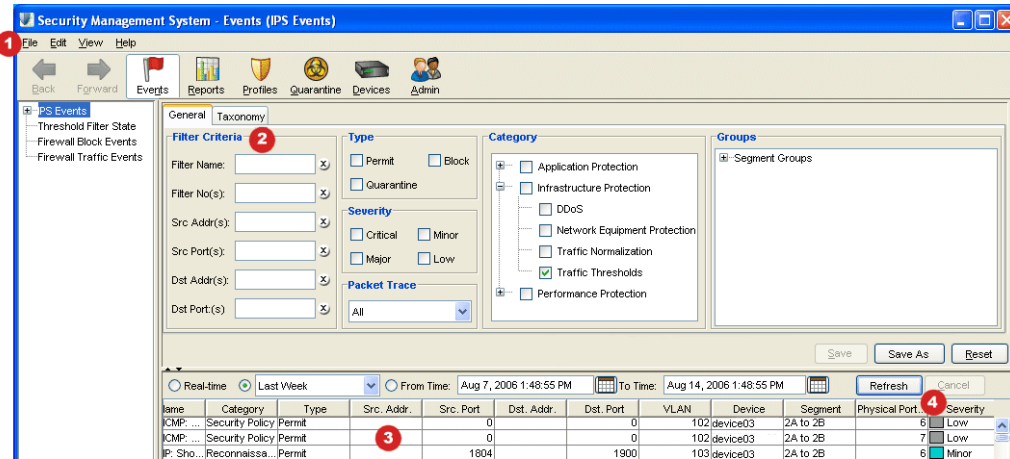


Table 4 - 1: Events Screen - Options

Item No.	Item	Details
1	Menu Bar	Content determined by the current screen and user access settings.
2	Query Pane	Provides filters for building search queries for attack events. Divided into the General tab and the Taxonomy tab,
3	List Pane	Displays query results
4	Severity Levels	Indicates the importance of the attack. See <a href="#">“Event Monitoring” on page 54.</a>

Select options from the Navigation pane or Menu Bar.

## Navigation Pane

From the Navigation pane, the options include the following:

- **IPS Events** — Provides options to query for and view attack events of the SMS system. You can search for and display events for all or specific devices, segment groups, and attack filter elements. See [“Event Monitoring” on page 54](#).
  - **Saved Queries** — *Displays the saved queries for compiling lists of attack events. Entries list in this section by creating and saving queries in the **IPS Events** screen. See [“Managing Queries” on page 60](#).*
- **Threshold State** — Displays triggered Traffic Threshold filters. You can view, edit, and reset filters as they are triggered. See [“Threshold State” on page 64](#).
- **Firewall Block Events** — Displays triggered Firewall Block rules. You can view, edit, and reset rules as they are triggered. See [“Firewall Block Events” on page 67](#).
- **Firewall Traffic Events** — Displays triggered Firewall Traffic events. You can view, edit, and reset rules as they are triggered. See [“Firewall Traffic Events” on page 69](#).

For each attack, the information in the following table is displayed. By default, new attacks appear at the top of the table; however, you can change the sort order of the display by clicking on the heading of any column. For example, you can sort according to severity by clicking the **Severity** heading.

## Query Pane

The **Events** screen provides a Query pane for entering criteria to search for attack events. These events display in the List pane.

When you enter 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.

This section contains the following topics:

- [“Query Pane General Tab” on page 44](#)
- [“Query Pane Taxonomy Tab” on page 46](#)

### Query Pane General Tab

The SMS can perform queries against 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.

The following table lists the fields available in the Query Pane on the General tab.

Section	Description
Filter Criteria	<p>Enables you to enter criteria for searching and displaying events. These options include the following:</p> <ul style="list-style-type: none"> <li>• Filter — Name of the filter</li> <li>• Filter No — Number of the filter</li> <li>• Src Addr — Source IP address</li> <li>• Src Port — Port of the source IP address</li> <li>• Dst Addr — Destination IP address</li> <li>• Dst Port — Port of the destination IP address</li> </ul>
Type	<p>Indicates the type of the event:</p> <ul style="list-style-type: none"> <li>• Permit — Traffic permit event</li> <li>• Block — Block event</li> <li>• Quarantine — IP quarantine event</li> </ul>
Severity	<p>Indicates the importance of the attack. See <a href="#">“Event Monitoring” on page 54</a>.</p>
Packet Trace	<p>Indicates if the query should locate action sets with packet trace enabled:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Events with Packet Trace</li> <li>• Events without Packet Trace</li> </ul>

Section	Description
Category	<p>Enables you to select one or more filter categories:</p> <ul style="list-style-type: none"> <li>• Application Protection <ul style="list-style-type: none"> <li>◦ <i>Exploits</i></li> <li>◦ <i>Identity theft</i></li> <li>◦ <i>Reconnaissance</i></li> <li>◦ <i>Security Policy</i></li> <li>◦ <i>Spyware</i></li> <li>◦ <i>Virus</i></li> <li>◦ <i>Vulnerabilities</i></li> </ul> </li> <li>• Infrastructure Protection <ul style="list-style-type: none"> <li>◦ <i>DDoS</i></li> <li>◦ <i>Network Equipment Protection</i></li> <li>◦ <i>Traffic Normalization</i></li> <li>◦ <i>Traffic Thresholds</i></li> </ul> </li> <li>• Performance Protection <ul style="list-style-type: none"> <li>◦ <i>Instant Messaging</i></li> <li>◦ <i>Peer to Peer</i></li> <li>◦ <i>Streaming Media</i></li> </ul> </li> </ul>
Groups	Enables you to select the events according to segment group.

### Query Pane Taxonomy Tab

The Query Pane also includes a Taxonomy tab that enables you to search filters according to classification, protocol, and platform. You can select multiple options within each grouping.



## List Pane

The **Events** screen displays query results in the List pane. This section of the screen provides a table of returned entries. See Figure 4 - 1, “Events Screen,” on page 43:

Column	Description
Time	The date and time that the attack was processed by the IPS
Name	The name of the filter that generated the alert or block
Category	The type of attack filter
Type	The type of action for the filter.
Src. Addr.	The IP address of the system that sent the attack
Src. Port	The port of the source IP address
Dst. Addr.	The IP address of the system at which the attack was targeted
Dst. Port	The port of the destination IP address
VLAN	The VLAN on which the attack took place
Device	The name of the IPS device responding to the traffic
Segment	The segment of the IPS device that responded to the traffic
Physical Port	The number of the physical device port
Severity	Indicates the importance of the attack. See <a href="#">“Event Monitoring” on page 54.</a>
Hit Count	The number of times the filter was triggered
Trace	Indicates if the attack events has a packet trace (or saved portion of the packet used in the attack)



**Note** Virtual segments are used with V2.5 and above device. For V2.5+ and above, physical segments can be used but cannot be not created. Security zones are used with X-Family devices. For more information, see [“IPS Devices: Network Configuration” on page 366](#) and [“Network Configuration: Segments/Zones Tab” on page 395.](#)

You can perform the following tasks:

- [“Customize the List Pane” on page 48](#)
- [“Sort Query Results” on page 48](#)
- [“Update Displayed Results” on page 49](#)

### How To: Customize the List Pane

The list pane includes options for customizing the displayed results, allowing you to select between one of the following settings:

- Real-time (running) — 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: Last Hour, Last Day, Last Week, Last Month
- Time range — Displays events during a range of time you select, including date, hour, and minute for beginning and ending range settings

### How To: Sort Query Results

You can sort query results using the column headings. To filter and sort the results, select from the following options:

- Real-time Running
- Range of Time: Last 30 seconds, minute, 5 minutes, 15 minutes, 30 minutes, hour, week, month
- Range of Time: Select a date to begin and end with

## How To: Update Displayed Results

To update the displayed results:

- Click **Refresh**, or
- Right-click on list entries according to the column data.

The following table details the options:

Column	Right-Click Options
Time	<ul style="list-style-type: none"> <li>• <b>Copy</b> — Provides the following options for copying data:             <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>Cell Value</i> — Copies the cell content data, such as an event name or IP address</li> </ul> </li> <li>• <b>Export to File</b> — Exports selected rows or all rows to a delimited text file.             <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Exports the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>All rows</i> — Copies all currently viewed rows.</li> </ul> </li> <li>• <b>Place In: From Time</b> — Uses the time value for the list pane display</li> <li>• <b>Place In: To Time</b> — Uses the time value for the list pane display</li> <li>• <b>Details</b> — Displays the details of the event</li> <li>• <b>Packet Trace</b> — Displays the packet trace captured by the filter settings</li> <li>• <b>Filter</b> — Provides the following options:             <ul style="list-style-type: none"> <li>◦ <i>Edit Filter</i> — Opens the editor for the filter associated with the event</li> <li>◦ <i>Create Exception</i> — Creates an exception for the filter associated with the event</li> <li>◦ <i>Create Traffic Management Filter</i> — Creates a Traffic Management filter using the entry's data</li> </ul> </li> <li>• <b>Reports</b> — Provides the following report options:             <ul style="list-style-type: none"> <li>◦ <i>Specific Attack Report</i></li> <li>◦ <i>Specific Source Report</i></li> <li>◦ <i>Specific Destination Report</i></li> </ul> </li> </ul>

Column	Right-Click Options
Name Category Type Scr Addr Scr Port Dst Addr Dst Port Segment	<ul style="list-style-type: none"> <li>• <b>Copy</b> — Provides the following options for copying data:               <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>Cell Value</i> — Copies the cell content data, such as an event name or IP address</li> </ul> </li> <li>• <b>Export to File</b> — Exports selected rows or all rows to a delimited text file.               <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Exports the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>All rows</i> — Copies all currently viewed rows.</li> </ul> </li> <li>• <b>Search on this value</b> — Performs a search query of events using the cell contents</li> <li>• <b>Remove Search on this value</b> — Clears the associated search field</li> <li>• <b>Details</b> — Displays the details of the event</li> <li>• <b>Packet Trace</b> — Displays the packet trace captured by the filter settings</li> <li>• <b>Filter</b> — Provides the following options:               <ul style="list-style-type: none"> <li>◦ <i>Edit Filter</i> — Opens the editor for the filter associated with the event</li> <li>◦ <i>Create Exception</i> — Creates an exception for the filter associated with the event</li> <li>◦ <i>Create Traffic Management Filter</i> — Creates a Traffic Management filter using the entry's data</li> </ul> </li> <li>• <b>Reports</b> — Provides the following report options:               <ul style="list-style-type: none"> <li>◦ <i>Specific Attack Report</i></li> <li>◦ <i>Specific Source Report</i></li> <li>◦ <i>Specific Destination Report</i></li> </ul> </li> </ul>

Column	Right-Click Options
Hit Count	<ul style="list-style-type: none"> <li>• <b>Copy</b> — Provides the following options for copying data: <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>Cell Value</i> — Copies the cell content data, such as an event name or IP address</li> </ul> </li> <li>• <b>Export to File</b> — Exports selected rows or all rows to a delimited text file. <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Exports the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>All rows</i> — Copies all currently viewed rows.</li> </ul> </li> <li>• <b>Details</b> — Displays the details of the event</li> <li>• <b>Packet Trace</b> — Displays the packet trace captured by the filter settings</li> <li>• <b>Filter</b> — Provides the following options: <ul style="list-style-type: none"> <li>◦ <i>Edit Filter</i> — Opens the editor for the filter associated with the event</li> <li>◦ <i>Create Exception</i> — Creates an exception for the filter associated with the event</li> <li>◦ <i>Create Traffic Management Filter</i> — Creates a Traffic Management filter using the entry's data</li> </ul> </li> <li>• <b>Reports</b> — Provides the following report options: <ul style="list-style-type: none"> <li>◦ <i>Specific Attack Report</i></li> <li>◦ <i>Specific Source Report</i></li> <li>◦ <i>Specific Destination Report</i></li> </ul> </li> </ul>

Column	Right-Click Options
Device Packet Trace	<ul style="list-style-type: none"> <li>• <b>Copy</b> — Provides the following options for copying data: <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Copies the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>Cell Value</i> — Copies the cell content data, such as an event name or IP address</li> </ul> </li> <li>• <b>Export to File</b> — Exports selected rows or all rows to a delimited text file. <ul style="list-style-type: none"> <li>◦ <i>Selected Rows</i> — Exports the selected rows. Use the Shift key to select multiple rows or the Ctrl key to select specific rows.</li> <li>◦ <i>All rows</i> — Copies all currently viewed rows.</li> </ul> </li> <li>• <b>Details</b> — Displays the details of the event</li> <li>• <b>Packet Trace</b> — Displays the packet trace captured by the filter settings</li> <li>• <b>Filter</b> — Provides the following options: <ul style="list-style-type: none"> <li>◦ <i>Edit Filter</i> — Opens the editor for the filter associated with the event</li> <li>◦ <i>Create Exception</i> — Creates an exception for the filter associated with the event</li> <li>◦ <i>Create Traffic Management Filter</i> — Creates a Traffic Management filter using the entry's data</li> </ul> </li> <li>• <b>Reports</b> — Provides the following report options: <ul style="list-style-type: none"> <li>◦ <i>Specific Attack Report</i></li> <li>◦ <i>Specific Source Report</i></li> <li>◦ <i>Specific Destination Report</i></li> </ul> </li> </ul>

## Menu Bar Options

The available menu items for the Menu Bar differ according to the displayed screen and user access settings. Each screen provides options for the following:



**Note** The following list may change depending on the displayed screen or selected item in the main pane.

**File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:

- New — Creates a new item based on selection, such as a exception and traffic management filter
- Save/Save As — Saves the entered query in the **Saved Queries** section of the Navigation pane
- Export Query Results — Exports the results of a query to a delimited file
- Logoff — Logs you out of the SMS
- Exit — Closes the SMS

**Edit** — Provides edit options based on the currently selected and displayed screen.

- Delete — Deletes a selected saved entry
- Reset — Resets a selected Threshold Filter
- Attack Filter — Edits a selected Attack Filter
- Preferences — Displays the System Preferences dialog box. See [“System Preferences” on page 27](#).

**View** — Displays the screens for the options listed in the Navigation Pane.

- Details
- Packet Trace
- WhoIs Utility
- Dashboard (see [“SMS Dashboard” on page 24](#))

**Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

# Event Monitoring

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

After entering a query, a list of matching attack events display in the List pane. 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.

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

You can also select a date and time range for displaying events. To use the **Time** field, click on the calendar icon to the right of the time control, and use the pop-up calendar to select a new date and time. For instructions on using the calendar control, see [“Date and Time Controls” on page 37](#). After you change the time, click **Refresh**.

For right-click options in the List Pane, see [“Right-click Options” on page 64](#).

This section contains the following topics:

- [“Searching Events” on page 54](#)
- [“Viewing Events” on page 57](#)
- [“Severity Level” on page 58](#)
- [“View the Packet Trace” on page 58](#)
- [“Exporting Query Results” on page 59](#)
- [“Using the WhoIs Utility” on page 60](#)

## Searching Events

To search for an event, enter criteria in the [Query Pane](#). Results display in the List pane. Saved queries display in the **Saved Queries** section of the **Events** Navigation pane. See [“Managing Queries” on page 60](#) for more information.

A query may take a significant amount of time or resources to run. If necessary, click the **Cancel** button to cancel the query. When you cancel the query, no results are displayed.



The following criteria are available in the Query pane:

Section	Description
Groups	Allows you to select the events according to segment group.
Filter Criteria	<p>Allows you to enter criteria for searching and displaying events. These options include the following:</p> <p><b>Filter Name</b> — Name of the filter  <b>Filter No</b> — Number of the filter  <b>Src Addr(s)</b> — Source IP address  <b>Src Port(s)</b> — Port of the source IP address  <b>Dst Addr(s)</b> — Destination IP address  <b>Dst Port(s)</b> — Port of the destination IP address</p> <p><b>Note:</b> When searching for source or destination IP addresses, you can enter one address or a CIDR block. For information about port queries, see <a href="#">“Queries Against Ports” on page 55</a>.</p>
Severity	Indicates the importance of the attack. See <a href="#">“Event Monitoring” on page 54</a> .
Type	<p>Indicates the type of the attack:</p> <p><b>Permit</b> — Permit event  <b>Block</b> — Block event</p>
Groups	Allows you to select the events according to segment group.

## Queries Against Ports

The SMS can perform queries against single or multiple source and destination ports and filter IDs, and can also query against ranges. Enter ranges with a dash (-) and separate multiple entries with commas (.). An exclamation point (!) functions as an “or” option at the beginning of a query, and functions as an “and” option within a query.

For example, entering “1500-1599,!1591” in the **Dst Port(s)** field displays events that have affected all ports in the ranges 1500-1590 and 1592-1599.

To enhance searches, you can use all of these search options within one query. For example, to display events where the source port number is 22, 25, or between 1000 and 32000, enter “!22,25,1000-32000”.

### How To: Create a Query

For detailed information about the query fields, see [“Query Pane” on page 44](#).

1. On the **Events** screen, click **IPS Events** in the Navigation pane. The **Events - IPS Events** screen displays.
2. In the **Filter Criteria** section, enter any applicable criteria.
3. Select a type of attack from the **Type** drop-down menu.
4. Select a **Severity**.
5. From the **Packet Trace** drop-down menu, select one of the packet trace options.
6. Select one or more categories in the **Category** list.
7. Select a group in the **Groups** list.
8. Click **Refresh**. The returned attack events display in the List pane.

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.



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

### How To: Create a Query with the Taxonomy Tab

1. On the **Events** screen, click **IPS Events** in the Navigation pane. The **Events - IPS Events** screen displays.
2. Select the **Taxonomy** tab.
3. Select one or more criteria from the Classification, Protocol, and Platform columns.
4. Click **Refresh**. The returned attack events display in the List pane.

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.



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

## Viewing Events

To view the details about an attack 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 attack event if the filter triggering the attack event has a packet trace option set. See [“View the Packet Trace” on page 58](#).

The **Events - Attack Details** dialog displays the following information about an attack:

Field	Description
Attack No.	The order in which the attack appeared in the SMS
Action	The flow control action associated with the attack filter that matched the attack
Severity	The importance of the attack. See <a href="#">“Event Monitoring” on page 54</a>
Device/Segment	The segment on the IPS that responded to the traffic
Attack Time	The time on the IPS that the traffic was first encountered
Device Log Time	The time that the aggregation period ended and the attack was logged on the device
SMS Receipt Time	The time the SMS was notified of the traffic
Source Address	The IP address of the system that originated the attack
Destination Address	The IP address of the target of the attack
Hit Count	<p>The number of packets aggregated before notification was sent. Click <b>Packet Trace</b> at the bottom of the screen to view more information about the packets involved in the attack.</p> <p>The <b>Packet Trace</b> button is disabled if the SMS is aware that no packet trace information is available. See <a href="#">“View the Packet Trace” on page 58</a>.</p>
DNS Resolve and WhoIs	The DNS resolved IP address for the source and destination. You can determine the IP using the WhoIs utility. See <a href="#">“Using the WhoIs Utility” on page 60</a> .
Filter Information	The details about the triggered filter and its event information. This information includes the name, category, protocol, and other pertinent information. You can edit the filter by clicking <b>Edit</b> . See <a href="#">“Tuning the System” on page 61</a> .

### How To: View an Attack Event

1. Locate an attack event. See [“Searching Events” on page 54](#).
2. On the Menu Bar, select the **View** —> **Details** menu item.

The **Events - Attack Details** dialog box displays.

### Severity Level

Attack filters are assigned a severity level which indicates the importance of attack traffic. Severity levels are color-coded and appear in the **Events** screen so that you can quickly identify and respond appropriately to attack traffic.

The SMS uses the following severity levels:

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

### Viewing the 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 attack 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 attack filter is configured to log a packet trace, you can view the packet trace log.

For more information about action sets, see [Chapter 6, “Profiles”](#).

### How To: View the Packet Trace

1. On the **Attack Events** screen, locate an entry.
2. Right-click the entry and select **Packet Trace**. The **Packet Trace** dialog box displays.


If the packet trace is enabled for the selected attack's filter, the system enables the **Packet Trace** option.

3. To save the contents of the packet trace, click **Save**.

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

## Exporting Query Results

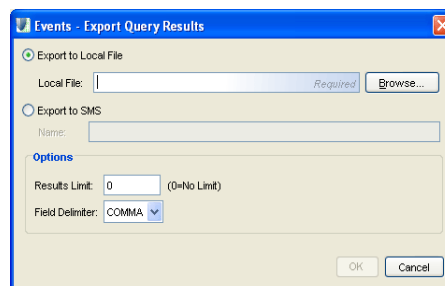
After creating and running an event query, you can export the results of the query to a comma- or tab-delimited file. This file can be imported into programs such as Crystal Reports or Microsoft Excel.

 **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.

### How To: Export Query Results


1. On the **IPS Events** screen, configure and run an attack event query.
2. Select an analysis mode not including Real-Time. The results can export for Last Hour or date/time range.
3. On the menu bar, click **File** -> **Export Query Results**. A **Save** dialog box displays.

Figure 4 - 2: Events - Export Query Results



4. Select **Export to Local File** or **Export to SMS**.
5. Enter the desired file name. If you are exporting the query to a local file, click **Browse...** to select the directory in which you want to save the file.
6. For **Results Limit**, enter an integer to limit the number of results that are exported. Enter 0 if you do not want to impose a limit.
7. Select a Field Delimiter from the drop-down menu.
8. Click **Export**.

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 in the IPS Events screen.

## Using the WhoIs Utility

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. You can have the utility running while you review events. You can access the utility by selecting the **View** —> **WhoIs Utility** menu item, or by clicking **WhoIs Utility** in an **Event Details** screen.

When you have the WhoIs Utility open, you can auto-fill the utility with by right-clicking an event entry. The Utility destination and source IP addresses by right-clicking an IP address in the event entry and selecting **WhoIs Lookup with Src. Addr.** You can also manually enter a source or destination IP address in the **Domain** field of the WhoIs Utility.

## Managing Queries

You can save, run, and manage queries through the **Events** screen. These queries display in the **Saved Queries** screen and section of the **Events** Navigation screen. You can load and modify these saved queries for searching for and displaying attack events. Through the screen, you can also remove queries and run saved queries.

When you enter 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 **Attack Events** screen. You can click **Refresh** to run the query again. The results display in the List pane.

You can do the following tasks:

- [Edit a Saved Query](#)
- [Delete a Saved Query](#)

### How To: 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 **IPS Events** screen.
2. Modify parameters as needed in **Filter Criteria**, **Type**, **Severity**, **Packet Trace**, **Category**, or **Groups**.
3. Click **Refresh**. The returned attack events display in the List pane.
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 **Events** Navigation pane.

### How To: Delete a Saved Query

1. On the **Events** Navigation pane, click **Saved Queries**. The **Saved Queries** screen displays.
2. Select the query to delete.
3. On the Menu Bar, select the **Edit** —> **Delete** menu item.

## Tuning the System

The **Events** screen provides a performance history of attack filters and system behavior. Depending on the event results, you may want to tune, or modify, the attack filters and exceptions to better react to attacks.

This section contains the following topics:

- [Editing Attack Filters](#)
- [Creating Attack Filter Exceptions](#)

You can perform the following tasks:

- [“Edit the Attack Filter” on page 62](#)
- [“Create a Filter Exception” on page 63](#)

### Editing Attack Filters

When you review attack event information, you may want to modify attack filter settings. 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.

When you select an attack event entry from the query results and select the **Attack Filter** option, the SMS client displays a page for the triggered filter, enabling you to modify settings without leaving the **Events** screen. The SMS uses the segment of the selected event to determine the profile that will be edited to add or update the filter associated with the event. The system uses the Profile that was last distributed to the segment and updates that Profile with your filter modifications.

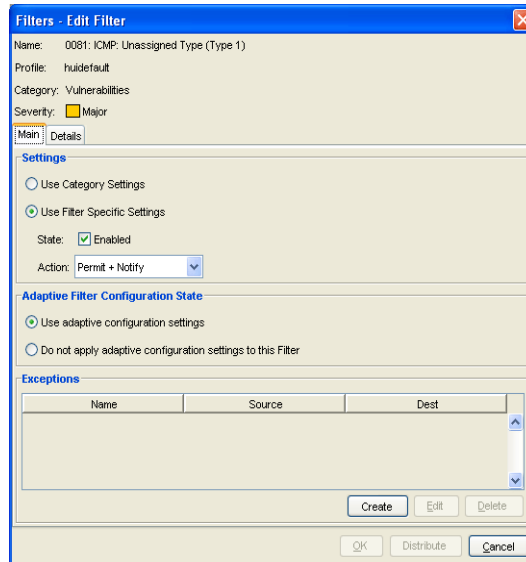



**Note** If the segment specified in the event was not updated from the SMS, you may receive an error indicating that the correct Profile cannot be determined. If the Profile cannot be determined, you must modify the filter directly through the **Profiles** screen. See [Chapter 6, “Profiles”](#).

**How To: Edit the Attack Filter**

1. Select an attack event.
2. On the Menu Bar, select the **Edit** —> **Attack Filter** menu item.  
The **Filter Edits/Details** dialog box displays.
3. Make your changes to the filter. Click **OK**.

Figure 4 - 3: Sample Filter Edits/Details Dialog Box



 **Note** Some filters have different options available on the edit dialog box. For detailed instructions about editing attack filters, see [“IPS Profile Filters” on page 189](#).

## Creating Attack Filter Exceptions

Filters may not always respond correctly to source and destination IP addresses. For example, you may have a filter blocks selected 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.

When you select an attack event entry from query results and select the **Create Exception** option, the SMS client displays a dialog box for the triggered filter, enabling you to modify settings without leaving the **Events** screen. The SMS uses the segment of the selected event to determine the profile that will be edited to add or update the filter associated with the event. The system uses the Profile that was last distributed to the segment and updates that Profile with your filter modifications



For detailed information on exceptions, see [“IPS Profile Filters” on page 189](#).



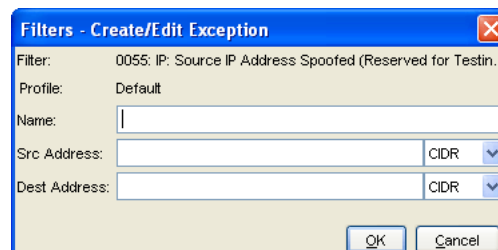
**Note** If the segment specified in the event was not updated from the SMS, you may receive an error indicating that the correct Profile cannot be determined. If the Profile cannot be determined, you must modify the filter's exceptions directly through the **Profiles** screen. See [Chapter 6. “Profiles”](#).

### How To: Create a Filter Exception

1. Right-click on an attack event and select **Filter** —> **Create Exception...**

The **Create/Edit Exception** dialog box displays.

Figure 4 - 4: Filters - Application Protection Filters - Create/Edit Exception Dialog Box



2. Enter a **Name** for the exception.
3. Enter the **Source** IP address.
4. Enter the **Destination** IP address.
5. Click **OK**.



**Note** For details on IP address formats, see [“IP Address Formats” on page 196](#).

For detailed instructions about editing attack filters, see [“IPS Profile Filters” on page 189](#).

# Threshold 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.

This section contains the following topics:

- [“Edit a Traffic Threshold Filter” on page 65](#)
- [“Reset a Traffic Threshold Filter” on page 66](#)
- [“Reset All Traffic Threshold Filters” on page 66](#)

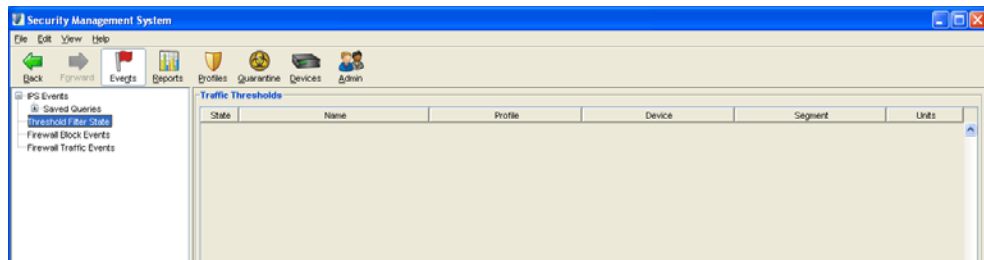
You can perform the following tasks:

- [“Edit a Traffic Threshold Filter” on page 65](#)
- [“Reset a Traffic Threshold Filter” on page 66](#)
- [“Reset All Traffic Threshold Filters” on page 66](#)

For more information on Traffic Threshold filters, see [“Traffic Threshold Filters” on page 223](#).

Through the **Events - Traffic Threshold State** screen, you can review, edit, and reset Traffic Threshold filters:

Figure 4 - 5: Events - Traffic Threshold State Screen



## Right-click Options

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

## How To: Edit a Traffic Threshold Filter

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

The **Filters - Traffic Threshold - Edit** dialog box displays.

Figure 4 - 6: Filters - Traffic Threshold - Edit Dialog Box

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**.

### How To: Reset a Traffic Threshold Filter

1. On the **Events - Traffic Threshold 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 65](#).

### How To: Reset All Traffic Threshold Filters

1. On the **Events - Traffic Threshold 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 65](#).

## Firewall Events (X-Family Devices)

If you have TippingPoint devices with firewall support, you can use your SMS to monitor the following firewall events:

- [“Firewall Block Events” on page 67](#)
- [“Firewall Traffic Events” on page 69](#)


You can perform the following tasks:

- [“Display the Firewall Block Events Screen” on page 67](#)
- [“Customize Displayed Results” on page 68](#)
- [“Display the Firewall Traffic Events screen” on page 69](#)

## Firewall Block Events

The **Firewall Block Events** screen lists events where packets that have been blocked by firewall rules that have logging enabled, including packets that were blocked by the content filtering configuration.

To review and edit firewall rules, use the **Profiles - Firewall Rules** screen. The rules prioritize, permit, block, filter, authenticate, schedule and monitor traffic between security zones. You can define the order in which the firewall rules are applied, so that traffic is checked first against the higher priority rules. For more information about creating and editing firewall rules, refer to [Chapter 6, “Profiles”](#).

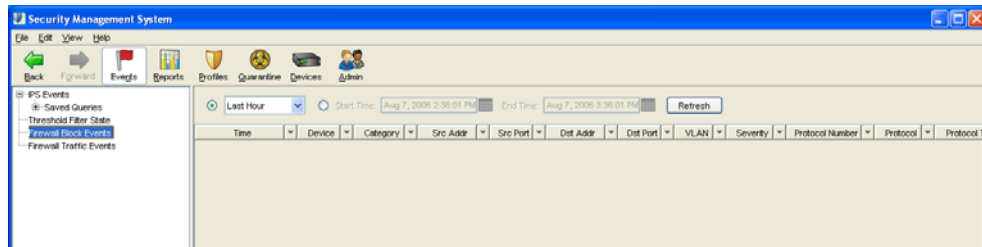
 **Note** Only X-Family devices include firewall and VPN functionality in addition to the TippingPoint IPS features. For more information on X-Family devices, refer to the TippingPoint X-Family documentation.


### How To: Display the Firewall Block Events Screen

1. Click the **Events** button on the Toolbar.
2. In the navigation pane, select **Firewall Block Events**.

The **Firewall Block Events** screen appears:

Figure 4 - 7: Firewall Block Events Screen



 **Note** The time displayed in the Time column reflects the time of the actual event on the IPS. This might not correspond to the SMS Receipt Time or the Device Log Time reported in the Details dialog box. The differences may depend on the timekeeping configuration of the IPS and SMS systems, and on the speed of the network.

### How To: Customize Displayed Results

The list pane includes the following options for customizing the displayed results:

- **Time Range** — You can display results based on the last increment of time or for a specific starting and ending time.
- **Sorting Results** — You can sort query results using the column headings. To filter and sort the results, select from the following options:
  - *Real-time Running*
  - *Range of Time: Last 30 seconds, minute, 5 minutes, 15 minutes, 30 minutes, hour, week, month*
  - *Range of Time: Select a date to begin and end with*

You can update the displayed results by clicking the **Refresh** button.

### List Pane

The **Firewall Block Events** screen displays results in the List pane.:

Column	Description
Time	The date and time that the attack was processed by the IPS
Device	The device on which the firewall rule was activated
Category	The type of traffic filter that was activated
Src/Dst Addr.	The IP address of the system that sent the attack
Src. Port	The port of the source IP address
Dst. Addr.	The IP address of the system at which the attack was targeted
Dst. Port	The port of the destination IP address
VLAN	The local VLAN that was targeted
Severity	The severity of the attack
Protocol Number	The number associated with the protocol in the filter.
Protocol	Packet type
Protocol Type	The protocol that was used to respond to the event
Src Zone	The security zone from which the attack originated
Dst Zone	The security zone at which the attack was targeted
Rule	The firewall rule that was applied
URL	The URL that was associated with the attack, if applicable
URL Info	Any additional information relevant to the URL
Count	The number of times the firewall rule was applied.

Column	Description
Start Time	The time at which the attack started.
Duration	The duration, in minutes, of the attack.
Physical Port	The device port on which the attack was detected.
Sequence	The number of this attack within the total list of events.

### Right-click Options

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

- **Copy** — Copy selected rows or cell contents
- **Export** — Export selected rows or all rows
- **Find** — Search for a term.

## Firewall Traffic Events

The **Firewall Traffic Events** screen lists the traffic events that are logged by the firewalls associated with the SMS. If logging is enabled for a firewall rule, then this screen displays all the information about incoming and outgoing packets that have been permitted according to that firewall rule, including packets permitted by the content filtering configuration.

For more information on firewall traffic filters, refer to [Chapter 6, “Profiles”](#).



**Note** Only X-Family devices include firewall and VPN functionality in addition to the TippingPoint IPS features. For more information on X-Family devices, refer to the TippingPoint X-Family documentation.

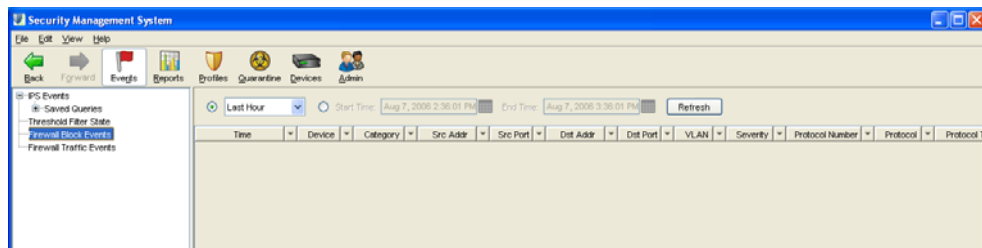
### How To: Display the Firewall Traffic Events screen

1. Click the **Events** button on the Toolbar.
2. From the left navigation pane, select **Firewall Traffic Events**. **Firewall Traffic Events** is displayed.



**Note** The time displayed in the Time column reflects the time of the actual event on the IPS. This might not correspond to the SMS Receipt Time or the Device Log Time reported in the Details dialog box. The differences may depend on the timekeeping configuration of the IPS and SMS systems, and on the speed of the network.

Figure 4 - 8: Firewall Traffic Events Screen



3. To customize the results, see [“How To: Customize Displayed Results” on page 68](#).

## List Pane

The **Firewall Traffic Events** screen displays results in the List pane and uses most of the same headings that appear on the Firewall Block Events screen. This screen also includes a **Message** column, which provides a brief description of the traffic event.

## Right-click Options

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

- **Copy** — Copy selected rows or cell contents
- **Export** — Export selected rows or all rows
- **Find** — Search for a term.



# 5 Reports

*The Reports screen displays reports of accumulated data compiled by the managed device and the SMS. These reports detail the threats encountered by the system and records processing trends. The Reports screen also provides real-time graphs of the IPS network statistics and report management and scheduling features.*

## Overview

This section includes the following topics:

- [“Reports: What’s New” on page 73](#)
- [“How To Tasks” on page 74](#)
- [“Navigation and Menu Options” on page 75](#)
- [“General Instructions for Reports” on page 80](#)
- [“Attacks: All Reports” on page 82](#)
- [“Attacks: Specific Reports” on page 89](#)
- [“Attacks: Top Reports” on page 96](#)
- [“Performance Protection: All Reports” on page 103](#)
- [“Performance Protection: Specific Reports” on page 107](#)
- [“Performance Protection: Top Reports” on page 111](#)
- [“Rate Limit Reports” on page 116](#)
- [“X-Family Reports” on page 120](#)
- [“Device Traffic Reports” on page 124](#)
- [“Traffic Threshold Reports” on page 128](#)
- [“E-Series Advanced DDoS Reports” on page 131](#)
- [“Saved Reports” on page 133](#)
- [“All Schedules” on page 140](#)

As the TippingPoint system detects malicious attacks and manages network usage, data about the events is logged in system files. This information details the behavior of the system as it responds to network traffic. The SMS provides a set of options to generate reports about the compiled and stored log information.

When you create a report, you select a template and modify its settings. These report templates track all issues, specific filters and IP addresses, and the top ten (10) reported issues encountered, such as destination and source IP addresses and attack filters triggered. The templates can be used to create reports for many different events, including attack, performance protection, traffic threshold, and Advanced DDoS events.

Report results can be viewed and printed through the Reports screen, saved and sent to the server, exported to comma- and tab-delimited files, and sent to e-mail recipients. The SMS automatically saves results from scheduled reports, including subsections for results and schedules. The report displays in the **Saved Reports** section of the screen, with the name that you enter for **Saved Report Name**. Each set of results is saved for each scheduled run of the report. You can also create multiple scheduled runs of each report.

Delimited files can be loaded into other programs for review such as Crystal Reports and Microsoft Excel.

The SMS provides templates for the following types of reports:

- **Attacks** — Documents specific types of attacks. These include reports for all, specific, or the top 1-100 of the following:
  - *By Attack*
  - *By Destination IP*
  - *By Source IP*
- **Performance Protection** — Documents misuse and abuse of resources on a network. These include reports for all, specific, or the top 1-100 of the following:
  - *By Peer*
  - *By Filter*
- **Rate Limit** — Documents the usage of bandwidth. The report details rate limit percentage used over time per device.
- **Device Traffic** — Documents traffic per set time amounts by device and port.
- **Traffic Threshold** — Documents traffic units per set time amounts by segment group.

- **X-Family** — Documents network traffic on X-Family devices according to the following groupings:
  - *By Protocol (all traffic)*
  - *By Category (web traffic)*



**Note** Only X-Family devices can provide data for these reports. The TippingPoint X-Family devices include firewall and VPN functionality in addition to the TippingPoint IPS features. For more information on X-Family devices, refer to the TippingPoint X-Family documentation.

- **Advanced DDoS** — Documents Distributed Denial of Service (DDoS) attacks by device and segment.



**Note** Only E-Series 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.

## Reports: What's New

This section outlines the following major changes for the current SMS release:

- [Virtual Segments](#)
- [Reports](#)
- [Category Settings](#)

### Virtual Segments

Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events.

See [“Network Configuration: Segments/Zones Tab” on page 395](#).

### Reports

The V 2.5 of the TippingPoint SMS added the following report templates that support X-Family devices:

- All Traffic by Protocol
- Web Traffic by Category

## Category Settings

The V 2.5 of the TippingPoint SMS has new category settings. In addition, some existing category settings were renamed.

### *New Category Settings*

- Vulnerabilities and Exploits
- Virus
- Spyware
- Identity Theft
- Instant Messaging
- Streaming Media

### *Renamed Category Settings*

- Misuse and Abuse - Renamed to Peer to Peer (P2P).
- Informational - This category was removed. The majority of filters in this category were moved to the Security Policy category.

## How To Tasks

### *Attacks: All Reports*

- [“How To: Generate an All Attacks Report” on page 84](#)
- [“How To: Generate an All Destination Report” on page 86](#)
- [“How To: Generate an All Sources Report” on page 88](#)

### *Attacks: Specific Reports*

- [“How To: Generate a Specific Attack Report” on page 90](#)
- [“How To: Generate a Specific Destination Report” on page 93](#)
- [“How To: Generate a Specific Source Report” on page 95](#)

### *Attacks: Top Reports*

- [“How To: Generate a Top Attacks Report” on page 98](#)
- [“How To: Generate a Top Destination Report” on page 100](#)
- [“How To: Generate a Top Sources Report” on page 102](#)

### *Performance Protection: All Reports*

- [“How To: Generate an All Performance Protection Filters Report” on page 104](#)
- [“How To: Generate an All Performance Protection Peers Report” on page 106](#)

### *Performance Protection: Specific Reports*

- [“How To: Generate a Specific Performance Protection Filter Report” on page 108](#)
- [“How To: Generate a Specific Performance Protection Peer Report” on page 110](#)

***Performance Protection: Top Reports***

- [“How To: Generate a Top Performance Protection Filters Report” on page 113](#)
- [“How To: Generate a Top Performance Protection Peers Report” on page 115](#)

***Rate Limit Reports***

- [“How To: Generate a Device Rate Limit Report” on page 117](#)
- [“How To: Generate a Rate Limit Report” on page 119](#)

***X-Family Reports***

- [“How To: Generate an All Traffic by Protocol Report” on page 121](#)
- [“How To: Generate a Web Traffic by Category Report” on page 123](#)

***Device Traffic Reports***

- [“How To: Generate a Device Traffic Report \(IPS Physical Port\)” on page 126](#)
- [“How To: Generate a Device Traffic Report \(X-Family\)” on page 127](#)

***Device Threshold Reports***

- [“How To: Generate a Traffic Threshold Report” on page 130](#)

***E-Series Advanced DDoS***

- [“How To: Generate a DDoS Report” on page 132](#)

***Saved Reports***

- [“How To: Delete a Report” on page 136](#)
- [“How To: Export Report Results” on page 137](#)
- [“How To: Open Report Results” on page 139](#)

***All Schedules***

- [“How To: Schedule a Report” on page 142](#)
- [“How To: Edit Scheduled Report” on page 144](#)
- [“How To: Delete a Scheduled Report” on page 146](#)

## Navigation and Menu Options

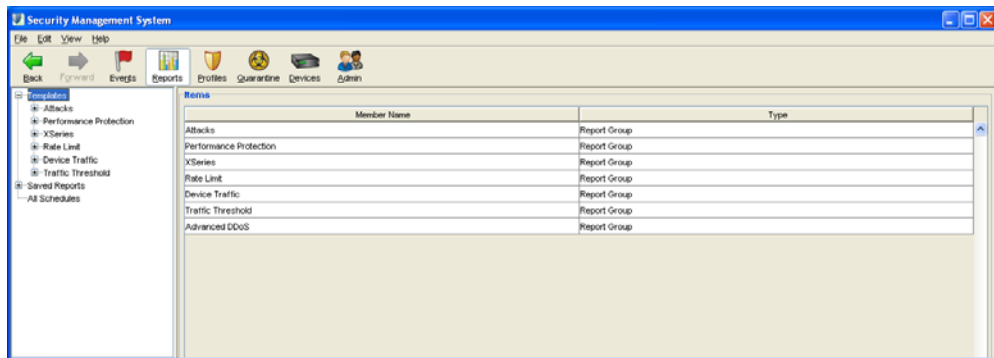
The Reports screen includes the following panes and options:

- [“Main Screen” on page 76](#)
- [“Navigation Pane” on page 76](#)
- [“Reports Query Pane” on page 77](#)
- [“Reports Graph Pane” on page 78](#)
- [“Reports List Pane” on page 78](#)
- [“Menu Bar Options” on page 79](#)
- [“Severity Level” on page 79](#)

## Main Screen

The **Reports** screen provides access to a variety of reports, charts, and logs. To open this window, click the **Reports** icon on the SMS Toolbar.

Figure 5 - 1: Reports Window



## Navigation Pane

The Navigation pane of the Reports screen provides the following options:

- [“Report Templates” on page 76](#)
- [“Saved Reports” on page 77](#)
- [“All Schedules” on page 77](#)

## Report Templates

Provides preset templates for reports. These reports include Attack and Performance Protection reports.

- **Attacks** — generates reports on the Application Protection pillar of filters and logged information. These templates include:
  - [“Attacks: All Reports” on page 82](#)
  - [“Attacks: Specific Reports” on page 89](#)
  - [“Attacks: Top Reports” on page 96](#)
- **Performance Protection** — generates reports on the Performance Protection pillar of filters and logged information. These templates include:
  - [“Performance Protection: All Reports” on page 103](#)
  - [“Performance Protection: Specific Reports” on page 107](#)
  - [“Performance Protection: Top Reports” on page 111](#)
- **X-Family** — generates firewall, VPN, and web traffic reports. These reports include:
  - [“All Traffic by Protocol Reports” on page 120](#)
  - [“Web Traffic Reports” on page 122.](#)

- **Rate Limit** — generates reports on filters and logged information with Rate Limits. These reports include:
  - [“Device Rate Limit Report” on page 116](#)
  - [“Rate Limit Report” on page 118](#)
- **Device Traffic** — generates reports on device traffic. See [“Device Traffic Reports” on page 124](#)
- **Traffic Threshold** — generates reports on Traffic Threshold filters. See [“Traffic Threshold Reports” on page 128](#).
- **Advanced DDoS** — generates reports on Advanced DDoS filters. See [“E-Series Advanced DDoS Reports” on page 131](#).

## Saved Reports

Enables you to view, save, and manage reports that you have generated with the report templates. This section also provides report schedules and results grouped by saved report. See [“Saved Reports” on page 133](#).

## All Schedules

Screen for managing all scheduled reports. See [“All Schedules” on page 140](#).



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this factor when entering criteria. The results display in the [Reports List Pane](#).

## Reports Query Pane

Each report screen includes a Query pane in the Main/List pane, where you select and enter options to generate reports. After you select the report options, click the **Run** button to generate results, which appear in the list pane at the bottom of the screen. For some reports, a second table provides detailed information for the main table and a second level of sorting. If a query takes too much time or resources, you can cancel the query by clicking the **Cancel** button.

The contents of the Query pane depend on the report template. The pane may contain some or all of the following elements:

- **Device tree** — Displays the organization of your devices and includes controls that report locations of devices. You can select All Devices, a group of devices, or a specific device from the tree.
- **Attack Type** — A drop-down menu of event types such as Blocks, Permits, and Blocks + Permits.
- **Severity panel** — A set of check box options. You can select one or more severity levels.
- **Filter Number** — A text field for entering a filter ID number.
- **Date Ranges** — Options for selecting a specific calendar date or general range of dates.



**Note** The maximum range of dates for any report is 90 days.

Some time settings allow you to select a specific date according to the calendar year. To set, click the calendar icon to the right of the time control. The calendar control enables you to select a date and time. For more information, see [“Date and Time Controls” on page 37](#).

## Reports Graph Pane

The Graph pane provides a graphical representation of the generated report and may include some or all of the following information:

- **IP** — Destination and/or source IP address
- **Device** — IPS device responding to the attack
- **Segment** — Segment on the device responding to the attack
- **Attack Type** — The type of the attack (blocks, permits, blocks + permits)
- **Severity** — The severity of the attack (critical, major, minor, low)
- **From** — The beginning of the date range
- **To** — The end of the date range



**Note** Virtual segments are used with V2.5 and above device. For V2.5+ and above, physical segments can be used but cannot be not created. Security zones are used with X-Family devices. For more information, see [“IPS Devices: Network Configuration” on page 366](#) and [“Network Configuration: Segments/Zones Tab” on page 395](#).

## Reports List Pane

Each report includes a sortable List pane. Each column of data in the List pane can be sorted in ascending and descending order to help locate specific results.



**Note** The **Reports** screen can display up to 10,000 rows of results. This limit affects the report you generate, schedule, and save to HTML. You should consider this factor when entering criteria.

To view details about an entry in the List pane, select the entry and perform one of the following actions:

- Double-click the entry.
- On the Menu Bar, select **View** and a menu item.
- On the Menu Bar, select the **Edit** —> **Details** menu item.
- Right-click an entry and click an option.



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



You can also right-click an entry to perform the following tasks:

- Viewing details
- Editing an attack filter
- Creating exceptions
- Creating Traffic Management filters

Some screens may have two List panes, each containing a table of data. The first table provides general information about the returned query results. The second table displays more detailed information. You can sort both tables. When you sort the second table, the first table is automatically updated with options to help locate the specific entry that you want.

## Menu Bar Options

The available Menu Bar options differ according to the displayed screen and user access settings. One user access settings may not permit the user to perform certain actions. In general, the following options are available:

- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:
  - *Run* — *Runs a report*
  - *Schedule...* — *Allows you to schedule a report*
  - *Save/Save As...* — *Allows you to save a report*
  - *Logoff* — *Logs you out of the SMS*
  - *Exit* — *Closes the SMS*
- **Edit** — Provides edit options based on the currently selected and displayed screen.
  - *Details* — *Displays the details of a selected entry*
  - *Delete* — *Deletes a selected entry*
  - *Preferences* — *Displays the System Preferences dialog box. See [“System Preferences” on page 27](#).*
- **View** — Displays the screens for the options listed in the Navigation Pane.
  - *Template Reports*
  - *Saved Reports*
  - *All Schedules*
  - *Dashboard* (see [“SMS Dashboard” on page 24](#))
- **Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

## Severity Level

Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded in the **Reports** screen to help you quickly identify and respond to attack traffic.

The SMS uses the following severity levels:

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

## General Instructions for Reports

This section contains the following topics:

- [“Setting Up Reports” on page 80](#)
- [“Process Time for Reports” on page 81](#)
- [“Viewing Reports” on page 81](#)
- [“Report Permissions” on page 81](#)

When you customize templates for specific types of reports, you can also save the reports and set them to run according to scheduled times. The results are saved to the SMS server and can be reviewed through the SMS client or be e-mailed directly to recipients. For more information on saving and scheduling reports, see [“Saved Reports” on page 133](#) and [“All Schedules” on page 140](#).



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

## Setting Up Reports

This general procedure is used to create, run, save, and schedule all reports.

### 1. Create a custom report

From the Navigation pane, expand the **Templates** option and select the type of report you want to run. Make changes to the template to customize to the search criteria. See [“Report Templates” on page 76](#) for more information.

### 2. Run a Report

After entering the settings for the custom report using a report template, click **Run**. The report displays results in the template screen.

### 3. Reset a Report

After entering data and running, click **Reset** to clear the report settings. If you open a Saved Report, make changes, and click **Reset**, the report resets to the last saved changes.

### 4. Save the Report

Click **Save As** to save your report. When you save a report, the report saves to the **Saved Reports** list in the **Reports** Navigation pane. See [“Saved Reports” on page 133](#) for more information.

### 5. Schedule a Report

After saving a report, you can schedule the report to run according to entered criteria. Scheduled reports display on the **All Schedules** screen and in the **Schedules** section for a saved report. Results of these reports display in the **Results** section for a saved report. See [“All Schedules” on page 140](#) for more information.



**Note** When running a report for CSW imported filters, the filter ID will differ from the CSW assigned ID. When you upload CSW packages, the SMS assigns each filter a new filter ID based on the ID you previously assigned it using the Custom Shield Writer. Each filter created by the CSW numbers the filters with a starting C followed by numbers. The SMS removes the C character and adds one million to the filter number. For example, C001 in CSW becomes 1000001 in SMS.

## Process Time for Reports

The time required to process a report can vary between seconds, minutes, and hours. Many variables affect the amount of time needed for a report to process, including:

- The selected time range for the report
- The number of events accumulated within the time range
- Other activities processed by SMS when the report runs:
  - *The number of events being received*
  - *Other reports or queries executed at that time*
  - *Any database maintenance routines*

## Viewing Reports

When you view a saved report, the Main pane displays the following information:

- A Query pane
- Summary information about your query
- A Graph pane displaying a graphic of the activity for the specified attack
- A List pane that display related information about the item

For more information, see [“How To Tasks” on page 74](#).

## 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.

- Super Users have full access to all reports, results, and schedules.
- Admin users can read, save, and schedule reports to which Super Users have granted them access.
- Operator users can read and run ad hoc reports. But they cannot save or schedule reports.

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 Super Users. Only users with Super User access can modify and reassign reports to new owners.

If a user account is removed or deleted from the SMS, all of the reports and associated scheduled report results that user owned are visible only to users with Super User access.

Saved reports are only visible to users who have read access to the specific segments, devices, and profiles. Specific report types require permissions as follows:

- **Attack and Performance Protection Reports** — Users must have permissions to the segment groups selected for these reports. If the report is for all segment groups, the user must have permissions to all segment groups to view it.
- **Rate Limit Reports** — Users must have permissions to devices selected for these reports. If the report is for all devices, the user must have permissions to all devices to view it.
- **Traffic Threshold Reports** — Users must have permissions to segment groups and the profile selected for these reports. If the report is for all segment groups, the user must have permissions to all segment groups and the selected profile to view it.

If a saved report references “All Segment Groups” and was saved by a Super User account, then other users only require access to all segment groups to see the report. They do not have to have Super User access.

For more information on user permissions, see [“Administration” on page 431](#).

## Attacks: All Reports

The templates provided in the Attacks listing listed with the “All” title provide options for generating reports on instances of all attack filters, destinations, and sources. The available report templates include the following:

- [“All Attacks Report” on page 83](#) — Generates a report on all filters
- [“All Destination Report” on page 85](#) — Generates a report on all targeted destination IP addresses
- [“All Sources Report” on page 87](#) — Generates a report on all source IP addresses originating the attacks

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80](#).
- [“Viewing Reports” on page 81](#).



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

You can perform the following **All Reports** tasks:

- [“Generate an All Attacks Report” on page 84](#)
- [“Generate an All Destination Report” on page 86](#)
- [“Generate an All Sources Report” on page 88](#)

## All Attacks Report

The All Attacks report template generates a report of logged behavior and events for all attack filters. The system generates and displays all instances that meet the entered criteria.:

Figure 5 - 2: Attacks - All Attacks Report - Query Pane

Table 5 - 1: Attacks - All Attacks Report - Graph Details

Heading	Description
Segment Group	The segment group that responded to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attacks: critical, major, minor, low, or all
From	The beginning of the date range
To	The end of the date range

Table 5 - 2: Attacks - All Attacks Report - Details

Column	Description
No.	Matches the Attack No. in the first table. For each attack, there are multiple rows in this table
Filter Name	The name of the of the filter
Severity	The severity of the attack: critical, major, minor, low
Hits	The number of times the attack came from that source

### How To: Generate an All Attacks Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **All Attacks** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to All.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. Select a date range:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or number of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected a **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against that value.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## All Destination Report

The All Destination Report generates a report of logged behavior and events for all destination IP addresses. The system generates and displays all instances that meet the entered criteria.:

Figure 5 - 3: Attacks - All Destination Report - Query Pane

The Graph pane displays the following information for the attack and a graphical representation of the behavior.

Table 5 - 3: Attacks - All Destination Report - Graph Details

Heading	Description
Segment Group	The segment group that responded to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attack: critical, major, minor, low, or all
From	The beginning of the date range
To	The end of the date range

Table 5 - 4: Attacks - All Destination Report - Details

Column	Description
No.	Matches the Attack No. in the Graph pane. For each attack, there are multiple rows in this table
Dest IP Address	The destination IP address receiving attacks
Hits	The number of times the attack came from that source

### How To: Generate an All Destination Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **All Destinations** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected a **General Date Range**, select the days of month, days of week, hour, and or minute ranges that you require. If you select --, the report will not run against that value.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.



## All Sources Report

The All Source Report generates a report of logged behavior and events for all source IP addresses. The system generates and displays all instances that meet the entered criteria.

Figure 5 - 4: Attacks - All Sources Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 5: Attacks - All Sources Report - Graph Details

Heading	Description
Segment Group	The segment group that responded to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 6: Attacks - All Sources Report Details

Column	Description
No.	Matches the Attack No. in the Graph pane. For each attack, there are multiple rows in this table
Source IP Address	The source IP address originating attacks
Hits	The number of times the attack came from that source

### How To: Generate an All Sources Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **All Sources** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or month based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected a **General Date Range**, select the days of month, days of week, hour, and or minute ranges that you require. If you select --, the report does not run against that value.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# Attacks: Specific Reports

Specific attack reports provide options for generating reports on specific attack instances. These reports search for information and generate reports on specified filters, destinations, and sources:

- [“Specific Attack Report” on page 89](#) — Generates a report on a specified filter
- [“Specific Destination Report” on page 92](#) — Generates a report on a targeted destination IP address
- [“Specific Source Report” on page 94](#) — Generates a report on a source IP address originating the attack

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

You can perform the following **Specific Reports** tasks;

- [“Generate a Specific Attack Report” on page 90](#)
- [“Generate a Specific Destination Report” on page 93](#)
- [“Generate a Specific Source Report” on page 95](#)

## Specific Attack Report

The Specific Attack Report generates a report of logged behavior and events of an entered filter. The system generates and displays all instances that meet the entered criteria.

Figure 5 - 5: Attacks - Specific Attack Report Screen

The screenshot shows the configuration interface for a Specific Attack Report. It is divided into several sections:

- Template Name:** A text box containing "Specific Attack".
- Attack Type:** A dropdown menu set to "Permits+Blocks".
- Date Range:** Radio buttons for "Specific Date Range" (selected) and "General Date Range". Below are options for "Last Hour", "Last Day", "Last Week", and "Last 1 Hours". There are also "From" and "To" date pickers showing "Aug 29, 2006 12:32:37 PM".
- Severity:** A list of severity levels with checkboxes: "Critical" (checked), "Major" (checked), "Minor" (checked), and "Low" (checked).
- Chart Type:** A dropdown menu set to "Bar".
- Filter Selection:** Two text boxes labeled "Name:" and "No(s):". To the right, there is a note: "Double-quote multiword names; separate multiple names / ids with commas; negate with exclamation mark; id range with dash."

At the bottom right, there are four buttons: "Run", "Save As", "Reset", and "Cancel".

The Graph pane displays the information for the attack and a graphical representation of the behavior.

**Table 5 - 7: Attacks - Specific Attack Report - Graph Details**

Heading	Description
Filter Selection	The name and/or number of the filter that responded to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Segment Group	The segment group that responded to the attack
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

**Table 5 - 8: Attacks - Specific Attack Report - Details**

Column	Description
Source IP Address	The source IP address from which the specified attack originated
Dest IP Address	The destination IP address the specified attack targeted
Hits	The number of times the attack came from that source
Severity	The severity of the attack: critical, major, minor, low



**Note** When running a report for CSW imported filters, the filter ID will differ from the CSW assigned ID. When you upload CSW packages, the SMS assigns each filter a new filter ID based on the ID you previously assigned it using the Custom Shield Writer. Each filter created by the CSW numbers the filters with a starting C followed by numbers. The SMS removes the C character and adds one million to the filter number. For example, C001 in CSW becomes 1000001 in SMS.

### How To: Generate a Specific Attack Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Specific Attack** report option.  
The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all groups.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.

5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected a **General Date Range**, select the days of month, days of week, hour, and or minute ranges that you require. If you select --, the report does not run against this value.
8. Under **Filter Selection**, select a filter or filters by filter name, number, or both. Separate multiple values with commas. You can also negate an individual name fragment, ID, or ID range using an exclamation mark (!)
  - In the **Name** field, you can enter filter name fragments. You can place double-quotes around filter names that contain spaces.
  - In the **No(s)** field, you can specify an ID range with a dash, such as 1100-1200.

The following example displays all filters with “ICMP” as a substring in the name, excludes any entries with “Modem Hangup” in the name, and includes filter 53 and filters between 1000 and 1500 inclusive while excluding filter 1254.

**Name:** ICMP,!“Modem Hangup”

**No(s):** 53, 1000 - 1500,!1254

9. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Specific Destination Report

The Specific Destination Report generates a report of logged behavior and events that are directed towards a specific destination IP address. The system generates and displays all instances that meet the entered criteria.

Figure 5 - 6: Attacks - Specific Destination Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.:

Table 5 - 9: Attacks - Specific Destination Report - Graph Details

Heading	Description
IP/CIDR	The destination IP address that received attacks
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Segment Group	The segment group that responded to the attack
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 10: Attacks - Specific Destination Report - Details

Column	Description
Filter	The name of the filter that responded to the attack
Severity	The severity of the attack: critical, major, minor, low
Source IP Address	The addresses from which the specified attack originated
Hits	The number of times the attack came from that source

The following options are available for Specific Destination reports:

- [“Generate a Specific Destination Report” on page 93](#)
- [“Saved Reports” on page 133](#)
- [“All Schedules” on page 140](#)

### How To: Generate a Specific Destination Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Specific Destination** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Enter a **IP/CIDR** address for the specific attacker IP address you want to review. You can enter CIDR blocks.
9. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Specific Source Report

The Specific Source Report generates a report of logged behavior and events of a specific source IP address that is originating attacks against the network. The system generates and displays all instances that meet the entered criteria.

Figure 5 - 7: Attacks - Specific Source Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 11: Attacks - Specific Source Report - Graph Details

Heading	Description
Source IP/CIDR	The source IP address that sent attacks
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Device	The device that responded to the attack
Segment Group	The segment group that responded to the attack
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 12: Attacks - Specific Source Report - Details

Column	Description
Filter	Name of the filter that caught the attack
Severity	The severity of the attack
Dest IP Address	The destination IP address the specified attack targeted
Hits	The number of times the attack came from that source



## How To: Generate a Specific Source Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Specific Source** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all groups.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Enter a **Source IP/CIDR** address for the specific attacker IP address you want to review. You can enter CIDR blocks.
9. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Attacks: Top Reports

Reports available in the Top Reports category provide information about the frequency of attacks, destination IP addresses, and source IP addresses within the parameters that you define in the Query pane. The Graph pane includes a summary of query information and a graph with a legend for the top attacks, destinations, or sources along with an eleventh color that represents all others. You can configure the reports to display up to 100 results.

There are two tables located below the graph. The first table is the Top Reports table, which provides an overview of the top ten attacks, destinations, or sources. The second table is the All Details table, which displays more detailed information about the items displayed in the first table.

The top attack reports include the following types:

- [“Top Attacks” on page 97](#) — Details the top 1-100 attacks against the system
- [“Top Destinations” on page 99](#) — Details the top 1-100 destinations for receiving attacks
- [“Top Sources” on page 101](#) — Details the top 1-100 sources for attacks

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

You can perform the following **Top Reports** tasks:

- [“Generate a Top Attacks Report” on page 98](#)
- [“Generate a Top Destination Report” on page 100](#)
- [“Generate a Top Sources Report” on page 102](#)

## Top Attacks

The Top Attacks report lists the top 1-100 attacks that have occurred against the system as recorded by the log files. The attacks are considered attack events. For more information on events, see [Chapter 4, “Events”](#).

Figure 5 - 8: Attacks - Top Attacks Screen

Table 5 - 13: Attacks - Top Attacks - Graph Details

Column	Description
Segment Group	The segment group responding to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 14: Attacks - Top Attacks - Details

Column	Description
No.	The order of the attacks in terms of frequency. Attack No. 1 is the attack that occurred most often.
Filter Name	The name of the attack filter
Severity	The severity of the attack: critical, major, minor, low
Hits	The number of times traffic matched the attack filter

The All Details pane provides more information about the most frequently used source and destination IP addresses involved in the attack. Each item you highlight in this table also highlights the related item in the Top Attacks table. The table displays the following information:

Table 5 - 15: Attacks - Top Attacks - All Details

Column	Description
No.	Matches the Attack No. in the first table. For each attack, there are multiple rows in this table
Filter Name	The name of the attack filter
Severity	The severity of the attack: critical, major, minor, low
Hits	The number of times traffic matched the attack filter
Source IP	The source IP address associated with the attack
Destination IP	The destination IP address associated with the attack

### How To: Generate a Top Attacks Report

- On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Top Attacks** report option.  
The report template screen appears.
- In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
- Select an **Attack Type**.
- Select the check box(es) for **Severity**.
- For the **Date Range**, select one of the following:
  - Specific Date Range** — Enables you to select a start and end time for the date range.
  - General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
- If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
- If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
- Select a **Chart Type**.
- In the **Summary** section, select the number of results that you want the report to display. By default, the report lists the top 10 attacks.
- Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Top Destinations

The Top Destinations report displays information about the frequency at which attacks target IP addresses on your network. The report compiles and details the statistics of the top ten IP addresses targeted by malicious attacks. The report enables you to determine the type of IP hosts that are targeted by specific malicious attacks, how filters react, and the behavior of the traffic during detection and block procedures.

Figure 5 - 9: Reports - Top Destinations Screen

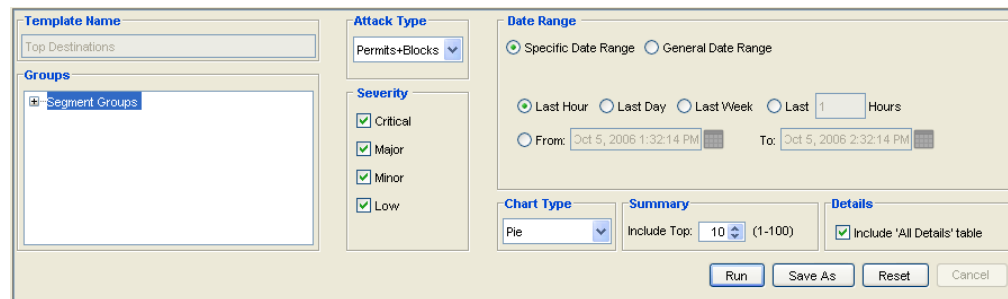


Table 5 - 16: Attacks - Top Destinations - Graph Details

Column	Description
Segment Group	The segment group responding to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 17: Attacks - Top Destinations - Summary

Column	Description
No.	The order of the attacks in terms of frequency. Attack No. 1 is the attack that occurred most often.
Destination IP	The destination IP address for the attack
Hits	The number of times traffic matched the attack filter

The All Details pane provides more information about the most frequently used source and destination IP addresses involved in the attack. Each item you highlight in this table also highlights the related item in the Summary table. The table displays the following information:

Table 5 - 18: Attacks - Top Destinations - All Details

Column	Description
Source IP	The source IP address associated with the attack
Destination IP	The destination IP address associated with the attack
Filter	The name of the attack filter
Severity	The severity of the attack: critical, major, minor, low
Hits	The number of times traffic matched the attack filter

### How To: Generate a Top Destination Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Top Destination** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all groups.
3. Select an **Attack Type**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Select a **Chart Type**.
9. In the **Summary** section, select the number of results that you want the report to display. By default, the report lists the top 10 attacks.
10. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Top Sources

The Top Sources report displays statistics for the top ten IP addresses from which attacks originated.

Figure 5 - 10: Attacks - Top Sources Screen

Table 5 - 19: Attacks - Top Sources - Graph Details

Column	Description
Segment Group	The segment group responding to the attack
Attack Type	The type of attack response. This is the action set: Blocks, Permits, Blocks + Permits
Severity	The severity of the attack: critical, major, minor, low
From	The beginning of the date range
To	The end of the date range

Table 5 - 20: Attacks - Top Sources - Summary

Column	Description
No.	The order of the attacks in terms of frequency. Attack No. 1 is the attack that occurred most often.
Source IP Address	The source IP address for the attack
Hits	The number of times traffic matched the attack filter

The All Details pane provides more information about the most frequently used source and destination IP addresses involved in the attack. Each item you highlight in this table also highlights the related item in the Summary table. The table displays the following information:

Table 5 - 21: Attacks - Top Sources - All Details

Column	Description
Source IP	The source IP address associated with the attack
Destination IP	The destination IP address associated with the attack
Filter	The name of the attack filter
Severity	The severity of the attack: critical, major, minor, low
Action	Action taken: Permit or Block
Hits	The number of times traffic matched the attack filter

### How To: Generate a Top Sources Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Attacks**, and then select the **Top Sources** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. Select an **Attack Type: Permits, Blocks, Permits + Blocks**.
4. Select the check box(es) for **Severity**.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Select a **Chart Type**.
9. In the **Summary** section, select the number of results that you want the report to display. By default, the report lists the top 10 attacks.
10. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.



To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Performance Protection: All Reports

Performance Protection reports provide information about the amount of all peer-to-peer traffic on your network. These reports detail the traffic of all filter in the Performance Protection pillar of filters and peer systems. Peer-to-peer systems allow you to share resources over a network, such as file sharing and services. These reports indicate the behavior and performance of all peer systems and the responses of all filters against malicious attacks or attempted usage:

- [“All Filters” on page 104](#) — Details the behavior of all Performance Protection filters
- [“All Peers” on page 105](#) — Details the traffic blocked from all peer systems on the network

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80](#).
- [“Viewing Reports” on page 81](#).



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

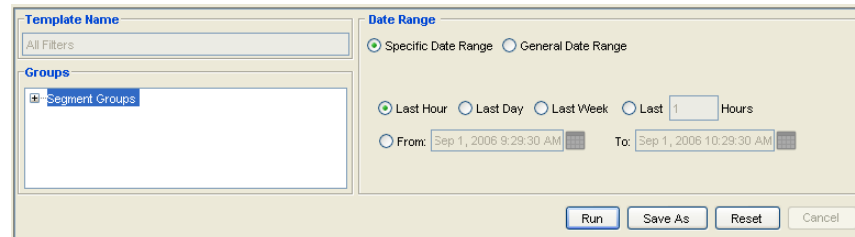
You can perform the following **All Reports** tasks:

- [“Generate an All Performance Protection Filters Report” on page 104](#)
- [“Generate an All Performance Protection Peers Report” on page 106](#)

## All Filters

The All Performance Protection Filters report displays information about the frequency of all peer-to-peer and traffic management filter usage.

Figure 5 - 11: Performance Protection - All Filters Screen



The Graph pane displays the following information:

Table 5 - 22: All Performance Protection Filters - Graph Details

Column	Description
Segment Group	The segment group that responded to the attack
From	The beginning of the date range
To	The end of the date range

Table 5 - 23: All Performance Protection Filters - Details

Column	Description
No.	The initial order of attackers according to frequency
Filter	The name of the Performance Protection filter
Hits	The number of times attack traffic came from the IP address

For more information about Performance Protection filters, see [“Performance Protection Filters” on page 226](#).

### How To: Generate an All Performance Protection Filters Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance and Protection**, and then select the **All Filters** report option.  
The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.

3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## All Peers

The All Performance Protection Peers report displays information about the amount of traffic that was blocked from all peers.:

Figure 5 - 12: Performance Protection - All Peers Screen

Table 5 - 24: All Peers - Graph Details

Column	Description
Segment Group	The segment group that responded to the attack
From	The beginning of the date range
To	The end of the date range

Table 5 - 25: Performance Protection - All Peers - Details

Column	Description
No.	The initial order of attackers according to frequency
Peer IP Address	The IP address of the peer system
Source Hits	The number of times attack traffic originated from the IP address
Dest Hits	The number of times attack traffic targeted the IP address
Total Hits	The total number of source and destination hits

For more information about Performance Protection filters, see [“Performance Protection Filters” on page 226](#).

### How To: Generate an All Performance Protection Peers Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance and Protection**, and then select the **All Peers** report option.  
The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# Performance Protection: Specific Reports

Specific Performance Protection reports provide information about the amount of specific peer-to-peer traffic on your network according to the criteria you enter. These reports detail the traffic of a specific Performance Protection filter in the Performance Protection pillar of filters and specific peer system on the network. Peer-to-peer systems allow you to share resources over a network, such as file sharing and services. These reports indicate the behavior and performance of specified peer systems and the responses of specified filters against malicious attacks or attempted usage.

- [“Specific Filter” on page 107](#) — Details the behavior of a specific Performance Protection filter
- [“Specific Peer” on page 109](#) — Details the traffic blocked from a specified peer system on the network

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

You can perform the following **Specific Reports** tasks:

- [“Generate a Specific Performance Protection Filter Report” on page 108](#)
- [“Generate a Specific Performance Protection Peer Report” on page 110](#)

## Specific Filter

The Specific Performance Protection Filters report displays information about the frequency of a specified peer-to-peer filter used to protect your network.

Figure 5 - 13: Performance Protection - Specific Filter Screen

The screenshot shows a web-based configuration interface for a specific filter report. It is divided into several sections:

- Template Name:** A text input field containing "Specific Filter".
- Groups:** A list box containing "Segment Groups", which is currently selected.
- Date Range:** Two radio buttons are present: "Specific Date Range" (selected) and "General Date Range". Under "Specific Date Range", there are four radio buttons: "Last Hour" (selected), "Last Day", "Last Week", and "Last 1 Hours". Below these are "From" and "To" date pickers, both showing "Sep 1, 2006 10:21:28 AM".
- Filter Selection:** Two text input fields labeled "Name:" and "No(s):". To the right of the "Name:" field is a small text box containing the instruction: "Double-quote multiword names; separate multiple names / ids with commas; negate with exclamation mark; id range with dash."
- Buttons:** At the bottom right, there are four buttons: "Run", "Save As", "Reset", and "Cancel".

Table 5 - 26: Performance Protection - Specific Filter - Graph Details

Column	Description
Filter Selection	The names and/or number of the filter that responded to the attack
Segment Group	The segment group that responded to the attack
From	The beginning of the date range
To	The end of the date range

Table 5 - 27: Performance Protection - Specific Filter - Details

Column	Description
No.	The initial order of attackers according to frequency
Peer IP Address	The IP address of the peer system
Source Hits	The number of times attack traffic originated from the IP address
Dest Hits	The number of times attack traffic targeted the IP address
Total Hits	The total number of source and destination hits

For more information, see [“Performance Protection Filters” on page 226](#).

### How To: Generate a Specific Performance Protection Filter Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance Protection**, and then select the **Specific Filter** report option. The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. Enter a **Filter Number** for the specific filter to review.
4. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
5. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
6. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.

7. Under **Filter Selection**, select a filter or filters by filter name, number, or both. Separate multiple values with commas. You can also negate an individual name fragment, ID, or ID range using an exclamation mark (!)
  - In the **Name** field, you can enter filter name fragments. You can place double-quotes around filter names that contain spaces.
  - In the **No(s)** field, you can specify an ID range with a dash, such as 1100-1200.

The following example displays all filters with “ICMP” as a substring in the name, excludes any entries with “Modem Hangup” in the name, and includes filter 53 and filters between 1000 and 1500 inclusive while excluding filter 1254.

**Name:** ICMP!“Modem Hangup”

**No(s):** 53, 1000 - 1500,!1254

8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Specific Peer

The Specific Performance Protection Peers report displays information about the amount of traffic that was blocked from a specified peer. The system generates a report based on the information you enter.

Figure 5 - 14: Performance Protection - Specific Peer Screen

Table 5 - 28: Performance Protection - Specific Peer - Graph Details

Column	Description
Peers IP	The peer IP that spawned the attack
Segment Group	The segment group that responded to the attack
From	The beginning of the date range
To	The end of the date range

Table 5 - 29: Performance Protection - Specific Peer - Details

Column	Description
No.	The initial order of attackers according to frequency
Filter Name	The name of the Performance Protection filter
Hits	The number of times attack traffic came from the IP address

For more information about Performance Protection filters, see [“Performance Protection Filters” on page 226](#) for more information.

### How To: Generate a Specific Performance Protection Peer Report

- On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance Protection**, and then select the **Specific Filter** report option.  
The report template screen appears.
- In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
- For the **Date Range**, select one of the following:
  - Specific Date Range** — Enables you to select a start and end time for the date range.
  - General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
- If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
- If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
- Enter a **Peer IP/CIDR** address for the specific attacker IP address you want to review. You can enter CIDR blocks.
- Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.
- To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).
- To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.



# Performance Protection: Top Reports

Performance Protection Top reports provide information about the behavior and performance of peer-to-peer filters and peers on your system and the responses of filters and peers against malicious attacks or attempted usage. You can configure the reports to display up to 100 results.

- [“Top Filters” on page 111](#) — Details the behavior of a specific Performance Protection filter
- [“Top Peers” on page 114](#) — Details the traffic blocked from a specified peer system on the network

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

You can perform the following **Top Reports** tasks:

- [“Generate a Top Performance Protection Filters Report” on page 113](#)
- [“Generate a Top Performance Protection Peers Report” on page 115](#)

## Top Filters

The Top Performance Protection Filters report displays information about the frequency of peer-to-peer filter usage on the most used filters.

Figure 5 - 15: Performance Protection - Top Filters Screen

The Graph pane displays the following information:

**Table 5 - 30: Performance Protection - Top Filters Graph Details**

Column	Description
Device	The device that responded to the attack
Segment	The segment of the device that responded to the attack
From	The beginning of the date range
To	The end of the date range

**Table 5 - 31: Performance Protection - Top Filters - Summary**

Column	Description
No.	The initial order of attackers according to frequency
Filter	The name of the Performance Protection filter
Hits	The number of times attack traffic came from the IP address

The All Details pane displays detailed information about the top 1-100 triggered filters listed in the Graph pane table. When you sort and select entries in this table, the actions affect the entries in the first table, allowing you to refine your search.

**Table 5 - 32: Performance Protection - Top Filters - All Details**

Column	Description
No.	The initial order of attackers according to frequency
Filter	The name of the Performance Protection filter
Peer IP Address	The IP address of the peer system
Source Hits	The number of times attack traffic originated from the IP address
Dest Hits	The number of times attack traffic targeted the IP address
Total Hits	The total number of source and destination hits

For more information about Performance Protection filters, see [“Performance Protection Filters” on page 226](#).

## How To: Generate a Top Performance Protection Filters Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance Protection**, and then select the **Top Filters** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. In the **Summary** section, select the number of results that you want the report to display. By default, the report lists the top 10 attacks.
7. Select **Include All Details** to populate the All Details pane.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Top Peers

The Top Performance Protection Peers report displays information about the amount of traffic that was blocked from the top ten peers.:

Figure 5 - 16: Performance Protection - Top Peers Screen

Table 5 - 33: Performance Protection - Top Peers - Graph Details

Column	Description
Segment	The segment group that responded to the attack
From	The beginning of the date range
To	The end of the date range

Table 5 - 34: Performance Protection - Top Peers - Summary

Column	Description
No.	The initial order of attackers according to frequency
Peer IP Address	The IP address of the peer system
Source Hits	The number of times attack traffic originated from the IP address
Dest Hits	The number of times attack traffic targeted the IP address
Total Hits	The total number of source and destination hits

The All Details pane displays detailed information about the top 1-100 triggered filters listed in the Graph pane table. When you sort and select entries in this table, the actions affect the entries in the first table, allowing you to refine your search.

Table 5 - 35: Performance Protection - Top Peers - All Details

Column	Description
No.	The initial order of attackers according to frequency
Peer IP Address	The IP address of the peer system
Filter	The name of the Performance Protection filter
Hits	The number of times attack traffic came from the IP address

For more information about Performance Protection filters, see [“Performance Protection Filters” on page 226](#).

### How To: Generate a Top Performance Protection Peers Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Performance Protection**, and then select the **Top Peers** report option. The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. In the **Summary** section, select the number of results that you want the report to display. By default, the report lists the top 10 attacks.
7. Select **Include All Details** to populate the All Details pane.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# Rate Limit Reports

Rate Limit reports provides options for reporting the percentage of used bandwidth 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.

- [“Device Rate Limit Report” on page 116](#) — Details the behavior of a specific device’s rate limit action set (all or selected)
- [“Rate Limit Report” on page 118](#) — Details the behavior of a specific rate limit action set (selected from menu list)

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81](#)



**Note** The Reports screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this factor when entering criteria. The results display in the [Reports List Pane](#).

You can perform the following tasks:

- [“Generate a Device Rate Limit Report” on page 117](#)
- [“Generate a Rate Limit Report” on page 119](#)
- [“Saved Reports” on page 133](#)
- [“All Schedules” on page 140](#)

## Device Rate Limit Report

A Device Rate Limit report provides information about the behavior of rate limits on specific devices. You can select all devices or a specific devices and rate limit action sets. For more information about rate limit action sets, see [“Action Sets Tab” on page 167.](#)

Figure 5 - 17: Rate Limit - Device Rate Limit Screen

The screenshot shows a web-based configuration interface for generating a Device Rate Limit report. It is divided into several functional areas:

- Template Name:** A dropdown menu currently set to "Device Rate Limits".
- Rate Limits:** A section with a checkbox labeled "All Rate Limits". Below it is a list box for selecting specific rate limit action sets.
- Date Range:** Two radio buttons for "Specific Date Range" (selected) and "General Date Range". Under "Specific Date Range", there are radio buttons for "Last Hour", "Last Day", and "Last Week", along with a "Last" field set to "1" and "Hours". Below these are "From" and "To" date pickers, both showing "Oct 27, 2005 2:25:53 PM".
- Time Units:** Radio buttons for "Minutes", "Hours", and "Days".
- Show Throughput:** A checkbox that is currently unchecked.
- Chart Type:** A dropdown menu currently set to "Stacking Ar...".
- Buttons:** "Run", "Save As", "Reset", and "Cancel" buttons are located at the bottom right of the form.

The Graph pane displays the following information:

Table 5 - 36: Rate Limit Report - Graph Details

Heading	Description
Rate Limit	The Rate Limit action set reported against
Time Units	The time units for the report: minutes, hours, days
Device	The device that triggered the rate limit
From	The beginning of the date range
To	The end of the date range

Table 5 - 37: Rate Limit Report - Rate Limit Details

Column	Description
Time	The date and time of the reported rate limit
Rate Limit	The Rate Limit action set reported against
Bytes	The amount of bytes reported for the triggered rate limit
Mbps	The configured megabits per second rate for the rate limit
Percent	The percentage of utilization in respect to the configured rate

### How To: Generate a Device Rate Limit Report

- On the **Reports** Navigation pane, expand the **Templates** listing, click **Rate Limit**, and then select the **Device Rate Limit** report option.  
The report template screen appears.
- In the **Device** section, select the appropriate item monitored by the SMS.
- In the **Rate Limits** section, select one of the following:
  - To scan all rate limit actions sets, select **All Rate Limits**.
  - To scan specific rate limit action sets, select action sets from list of rate limits.
- For the **Date Range**, select one of the following:
  - Specific Date Range** — Enables you to select a start and end time for the date range.
  - General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
- If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).

6. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
7. Select a **Time Unit**.
8. Select a **Chart Type**.
9. Select **Show Throughput** to display device and rate limiter traffic. If not selected, the chart displays only the rate limiter traffic.
10. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Rate Limit Report

A Rate Limit report provides information about the behavior of rate limits. You can select all or a specific devices and rate limit action sets. For more information about rate limit action sets, see [“Action Sets Tab” on page 167](#).

Figure 5 - 18: Rate Limit - Rate Limit Screen

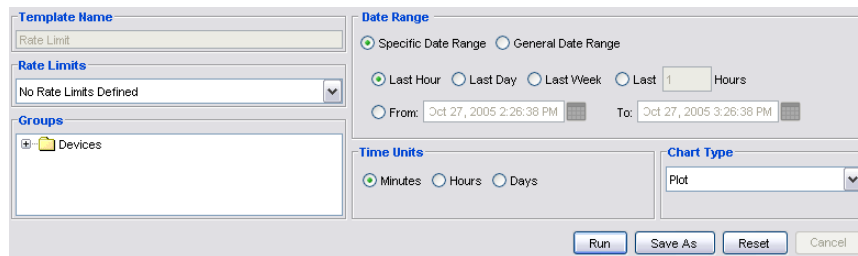


Table 5 - 38: Rate Limit - Rate Limit - Graph Details

Column	Description
Rate Limit	The rate limit action set that responded to the attack
Time Units	The selected time units for the report (minutes, hours, or days)
Device	The device running the rate limit
From	The beginning of the date range
To	The end of the date range
Rate	The rate for the rate limit; n/a if not applicable



The Rate Limit pane includes the following information:

Table 5 - 39: Rate Limit Report - Rate Limit Details

Column	Description
Time	The date and time of the reported rate limit
Rate Limit	The Rate Limit action set reported against
Bytes	The amount of bytes reported for the triggered rate limit
Mbps	The configured megabits per second rate for the rate limit
Percent	The percentage of utilization in respect to the configured rate

### How To: Generate a Rate Limit Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Rate Limit**, and then select the **Rate Limit** report option.

The report template screen appears.

2. Select an action set in the **Rate Limits** section.
3. In the **Groups** section, expand the **Devices** folder and select a device group that SMS monitors. If you do not select a device, it defaults to all.
4. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
5. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
6. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
7. Select a **Time Unit**.
8. Select a **Chart Type**.
9. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# X-Family Reports

X-Family reports provide information about the amount and type of traffic passing through your devices.

The following options are available for X-Family reports:

- [“All Traffic by Protocol Reports” on page 120](#)— generated by protocol
- [“Web Traffic Reports” on page 122](#)— generated by category

You can perform the following tasks:

- [“Generate an All Traffic by Protocol Report” on page 121](#)
- [“Generate a Web Traffic by Category Report” on page 123](#)

## All Traffic by Protocol Reports

An All Traffic by Protocol report displays the amount of traffic experienced, broken down by protocol.

Figure 5 - 19: Device Traffic Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 40: Device Traffic Report - Graph Details

Heading	Description
Segment Group	The segment group for the reported traffic
From	The beginning of the date range
To	The end of the date range

The list pane provides the following information:

**Table 5 - 41: Devices Traffic Details**

Column	Description
No.	The ranking of the protocol based on the amount of traffic it has received.
Sessions	The number of sessions for that protocol.
Bytes	The amount of traffic in bytes.
Protocol	The protocol name
Service Name	The service used to access the protocol.
Destination Port	The port at which the traffic events were directed.

### How To: Generate an All Traffic by Protocol Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, **XSeries**, and then select **All Traffic by Protocol**.  
The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Web Traffic Reports

A Web Traffic by Category report displays the amount of web traffic experienced, broken down by content category.

Figure 5 - 20: Device Traffic Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 42: Web Traffic by Category Report - Graph Details

Heading	Description
Segment Group	The segment group for the reported traffic
From	The beginning of the date range
To	The end of the date range

Table 5 - 43: Summary by Category Details

Column	Description
No.	The ranking of the category according the amount of traffic it has received.
Category	The content category name.
Bytes	The amount of traffic in bytes.
Hits	The number of web hits.

The Traffic Details by Category, Source IP Address pane provides the following information:

**Table 5 - 44: Traffic Details by Category, Source IP Address**

Column	Description
No.	The ranking of the category according the amount of traffic it has received.
Source	The source IP address.
Category	The content category name.
Bytes	The amount of traffic in bytes.
Hits	The number of web hits.

### How To: Generate a Web Traffic by Category Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **XSeries**, and then select **Web Traffic by Category**.  
The report template screen appears.
2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. If desired, select a **Category**.
4. If desired, enter a source IP address in the **Source** section.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# Device Traffic Reports

This section contains the following topics:

- [“IPS Physical Port Report” on page 125](#)
- [“X-Family Physical Port Report” on page 127](#)

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 report includes the following templates:

- IPS Physical Port
- X-Family Physical Port

Device Traffic templates allow you to enhance reporting by configuring the following items:

- **Chart Type** as bar, stacking bar, area, stacking area, plot, or scatter plot
- **Traffic Direction** as A to B, B to A, and both
- **Data Display** as average bps or total bytes
- **Data Aggregation** as group or to show all

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this factor when entering criteria. The results display in the [Reports List Pane](#).

You can perform the following tasks:

- [“Generate a Device Traffic Report \(IPS Physical Port\)” on page 126](#)
- [“Generate a Device Traffic Report \(X-Family\)” on page 127](#)

## IPS Physical Port Report

An IPS Physical Port report displays information about port traffic over time.

Figure 5 - 21: Device Traffic Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 45: Device Traffic Report - Graph Details

Heading	Description
Device and Segment	The device and segment for the reported traffic
Direction	The direction of the reported traffic: A to B, B to A, both
From	The beginning of the date range
To	The end of the date range

Table 5 - 46: Devices Traffic Details

Column	Description
Time	Date and time of the reported rate limit
Device	Device that triggered the filter
Segment	Device segment that triggered the filter
Port A In	Amount of traffic reported incoming to Port A
Port B Out	Amount of traffic reported outgoing through Port B
Port B In	Amount of traffic reported incoming to Port B
Port A Out	Amount of traffic reported outgoing through Port A
All In	Amount of traffic reported incoming for all ports
All Out	Amount of traffic reported outgoing for all ports

### How To: Generate a Device Traffic Report (IPS Physical Port)

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Device Traffic**, and then select **IPS Physical Port** or **Segment** report option.  
The report template screen appears.
2. In the **Devices** section, select a device. If you do not select one, it defaults to all.
3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. Select a **Time Unit** and a **Chart Type**.
7. Select the **Traffic Direction**. You can also select the **In** and/or **Out** check boxes.
8. Select the **Data Display**.
9. Select the **Data Aggregation**.
10. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.



## X-Family Physical Port Report

An IPS Physical Port report displays information about port traffic over time.

Figure 5 - 22: Device Traffic Report Screen

The Graph pane displays the information for the attack and a graphical representation of the behavior.

Table 5 - 47: Device Traffic Report - Graph Details

Heading	Description
Device and Segment	The device and segment for the reported traffic
From	The beginning of the date range
To	The end of the date range

Table 5 - 48: Devices Traffic Details

Column	Description
Time	The date and time of the reported rate limit
Device	The device that triggered the filter
Port	Port number
Port In	The amount of incoming port traffic
Port Out	The amount of outgoing port traffic

### How To: Generate a Device Traffic Report (X-Family)

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Device Traffic**, and then select **IPS Physical Port** or **Segment** report option.

The report template screen appears.

2. In the **Devices** section, select a device. If you do not select one, it defaults to all.

3. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
4. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
5. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
6. Select a **Time Unit**.
7. Select a **Chart Type**.
8. Select the **Traffic Direction**.
9. Select the **Data Display**.
10. Select the **Data Aggregation**.
11. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Traffic Threshold Reports

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 return to normal, and the exceeded amount. These amounts include an amount exceeded above and below normal levels.

For instructions on how to create a Traffic Threshold report, see [“Generate a Traffic Threshold Report” on page 130](#).

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80.](#)
- [“Viewing Reports” on page 81.](#)



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this factor when entering criteria. The results display in the [Reports List Pane](#).

The Graph pane displays information about the attacks and a graphical representation of the behavior.

**Table 5 - 49: Traffic Threshold Report - Graph Details**

Heading	Description
Profile Name	The name of the profile containing the filter
Threshold Filter	The Traffic Threshold filter the report generated against
Segment Group	The segment group that triggered the threshold filter
From	The beginning of the date range
To	The end of the date range
Time Units	The time units for the report: minutes, hours, days

**Table 5 - 50: Traffic Thresholds by Device: Segment Details**

Column	Description
Time	Date and time of the reported rate limit
Device	Device that triggered the filter
Segment	Device segment that triggered the filter
Value	Estimated value of traffic for the filter

### How To: Generate a Traffic Threshold Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Traffic Threshold**, and then select the **Traffic Threshold** report option.

The report template screen appears.

2. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
3. In the **Traffic Threshold Filters** section, select a **Profile** or a **Threshold Filter**. You can select one, both, or neither.
4. In the **Groups** section, expand the **Segment Groups** folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
5. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
6. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
7. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
8. Select a **Time Unit**.
9. Select a **Chart Type**.
10. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

# E-Series Advanced DDoS Reports

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 E-Series devices have access to these reports. E-Series devices include **Advanced DDoS Protection** filters. 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.

For instructions on how to create a DDoS report, see [“Generate a DDoS Report” on page 132](#).

For general information about using the reports feature, see the following items:

- [“How To Tasks” on page 74](#)
- [“Setting Up Reports” on page 80](#).
- [“Viewing Reports” on page 81](#).



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria.

The screenshot shows a configuration window for generating a DDoS report. It is divided into several sections:

- Template Name:** A text box containing "DDoS".
- Date Range:** Radio buttons for "Specific Date Range" (selected) and "General Date Range". Below are options for "Last Hour", "Last Day", "Last Week", and "Last 1 Hours". There are also "From" and "To" date pickers.
- Advanced DDoS Filters:** A "Profile" dropdown menu set to "No DDoS Filters defined" and a "DDoS Filter" dropdown menu.
- Groups:** A section with a checked "Segment Groups" checkbox and a list box.
- Time Units:** Radio buttons for "Minutes" (selected), "Hours", and "Days".
- Chart Type:** A dropdown menu set to "Plot".
- Types:** A grid of checkboxes:
  - SYNs Proxied
  - SYNs Rejected
  - Conns Allowed (CPS)
  - Conns Blocked (CPS)
  - Conns Allowed (Conn Flood)
  - Conns Blocked (Conn Flood)

At the bottom right, there are four buttons: "Run", "Save As", "Reset", and "Cancel".

The Graph pane displays the information for the attack and a graphical representation of the behavior. The information includes the following:

**Table 5 - 51: Advanced DDoS Report - Graph Details**

Heading	Description
Profile Name	Name of the profile containing the filter
DDoS Filter	DDoS filter the report generated against
Segment Group	Segment group that triggered the filter
From	Beginning of the date range
To	End of the date range
Time Units	Time units for the report: minutes, hours, days

**Table 5 - 52: Advanced DDoS Report - Details**

Column	Description
Time	Date and time of the reported DDoS attack
Device	Device that triggered the filter
Segment	Device segment that triggered the filter
Syn Proxied	Amount of SYNs proxied
Syn Rejected	Amount of SYNs rejected
CPS conns allowed	Amount of connections per second allowed to connect to the network
CPS conns blocked	Amount of connections per second blocked from connecting to the network
Conn Flood allowed	Amount of established connections allowed to the network
Conn Flood blocked	Amount of established connections blocked from the network

### How To: Generate a DDoS Report

1. On the **Reports** Navigation pane, expand the **Templates** listing, click **Advanced DDoS**, and then select the **DDoS** report option.

The report template screen appears.

2. In the **Advanced DDoS Filters** section, do the following:
  - Select a profile for the filter from the **Profile** drop-down menu.
  - Select a filter from the **DDoS Filters** drop-down menu.

3. In the Groups section, expand the Segment Groups folder and select a segment group that SMS monitors. If you do not select a group, it defaults to all.
4. For the **Date Range**, select one of the following:
  - **Specific Date Range** — Enables you to select a start and end time for the date range.
  - **General Date Range** — Enables you to select a general time according to day of the week or month and the hours and minutes during that day.
5. If you selected **Specific Date Range**, select one of the following:
  - The last hour, day, week, or amount of hours based on the current runtime.
  - Start and end times for the range. See [“Date and Time Controls” on page 37](#).
6. If you selected **General Date Range**, select the days of month, days of week, hour, and/or minute ranges that you require. If you select --, the report does not run against this value.
7. Select a **Time Unit**.
8. Select a **Type**:
  - SYNs Proxied
  - Conns Allowed (CPS)
  - Conns Allowed (Conn Flood)
  - SYNs Rejected
  - Conns Blocked (CPS)
  - Conns Blocked (Conn Flood)
9. Click **Run** or select the **File** —> **Run** menu item. The List pane lists the attack entries that meet the entered criteria.

To save the report, click **Save As**. The report saves to the **Saved Report** section on the **Reports** Navigation pane. For more information, see [“Saved Reports” on page 133](#). For information about scheduling saved reports, see [“All Schedules” on page 140](#).

To enter a new report using the current report template, click **Reset**. The template settings revert to the last saved settings.

## Saved Reports

This section contains the following topics:

- [“Edit or Delete Saved Reports” on page 135](#)
- [“View/Export Report Results” on page 136](#)

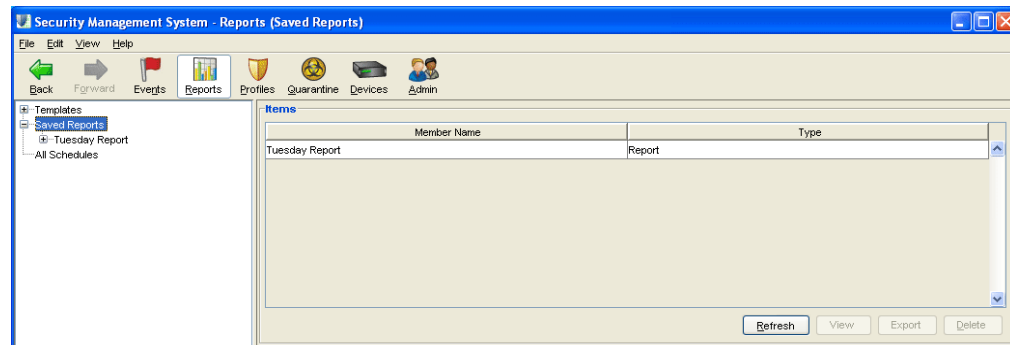
As you create and generate report templates, you can save these modified templates as saved reports. Through the **Reports** Navigation pane, you can view, modify, run, and schedule saved reports from the **Save Reports** screen. The **Saved Reports** section stores all report templates you customized and saved.

Each report template you save lists in the **Saved Reports** section of the **Reports** Navigation screen. You can select a report from the list to display the customized settings. Through these screens, you can do the following:

- **View and edit a saved report** — Saved reports are based on an existing template. When you edit and save the report, a new report result is saved to the Saved Reports subsection for that report name.
- **Save results** — Results of reports can also be saved in PDF format through the Saved Reports screen. Scheduled reports can be exported and emailed in other formats.
- **Run a saved report** — When you run the saved report, the new results are saved to the Results subsection for the saved report.
- **Schedule a saved report** — Results of scheduled reports display in the Schedules subsection for a saved report. You can also access the scheduled report through the All Schedules screen.

The following is the **Saved Reports** screen:

Figure 5 - 23: Reports - Saved Reports Screen



When you save a report, it displays in the Navigation pane with sub-options for **Results** and **Schedules**. All saved results are listed and available for review in the **Results** section. All saved report schedules are listed in the **Schedules** section.

If you open a Saved Report, edit settings, and click **Reset**, the report resets to the last set of saved settings.

You can perform the following tasks:

- [“Delete a Report” on page 136](#)
- [“Export Report Results” on page 137](#)
- [“Open Report Results” on page 139](#)



## Edit or Delete Saved Reports

When you modify a saved report, the report uses the **Report Templates** screen for the report. For example, if you created an All Attacks report to record information about network vulnerabilities and saved it with the name “Vulnerabilities”, the “Vulnerabilities” report uses the All Attacks report template with the settings for the custom created report.

To edit a saved report, select the report from the **Saved Report** section of the **Reports** Navigation pane. The reports displays in its appropriate report template screen with the custom settings.

Table 5 - 53: Report Types

Report Type	Template
Attacks	<ul style="list-style-type: none"> <li>• <a href="#">“Generate an All Attacks Report” on page 84</a></li> <li>• <a href="#">“Generate an All Destination Report” on page 86</a></li> <li>• <a href="#">“Generate an All Sources Report” on page 88</a></li> <li>• <a href="#">“Generate a Specific Attack Report” on page 90</a></li> <li>• <a href="#">“Generate a Specific Destination Report” on page 93</a></li> <li>• <a href="#">“Generate a Specific Source Report” on page 95</a></li> <li>• <a href="#">“Generate a Top Attacks Report” on page 98</a></li> <li>• <a href="#">“Generate a Top Destination Report” on page 100</a></li> <li>• <a href="#">“Generate a Top Sources Report” on page 102</a></li> </ul>
Performance Protection	<ul style="list-style-type: none"> <li>• <a href="#">“Generate an All Performance Protection Filters Report” on page 104</a></li> <li>• <a href="#">“Generate an All Performance Protection Peers Report” on page 106</a></li> <li>• <a href="#">“Generate a Specific Performance Protection Filter Report” on page 108</a></li> <li>• <a href="#">“Generate a Specific Performance Protection Peer Report” on page 110</a></li> <li>• <a href="#">“Generate a Top Performance Protection Filters Report” on page 113</a></li> <li>• <a href="#">“Generate a Top Performance Protection Peers Report” on page 115</a></li> </ul>
X-Family	<ul style="list-style-type: none"> <li>• <a href="#">“Generate an All Traffic by Protocol Report” on page 121</a></li> <li>• <a href="#">“Generate a Web Traffic by Category Report” on page 123</a></li> </ul>
Rate Limit	<ul style="list-style-type: none"> <li>• <a href="#">“Generate a Device Rate Limit Report” on page 117</a></li> <li>• <a href="#">“Generate a Rate Limit Report” on page 119</a></li> </ul>
Device Traffic	<ul style="list-style-type: none"> <li>• <a href="#">“Generate a Device Traffic Report (IPS Physical Port)” on page 126</a></li> </ul>
Traffic Threshold	<ul style="list-style-type: none"> <li>• <a href="#">“Generate a Traffic Threshold Report” on page 130</a></li> </ul>
Advanced DDoS	<ul style="list-style-type: none"> <li>• <a href="#">“Generate a DDoS Report” on page 132</a></li> </ul>

After entering modifications to the saved report, click **Save** to save the new changes. To save the modifications as a new saved report, click **Save As...** and enter a new report name.

You can also delete a saved report.

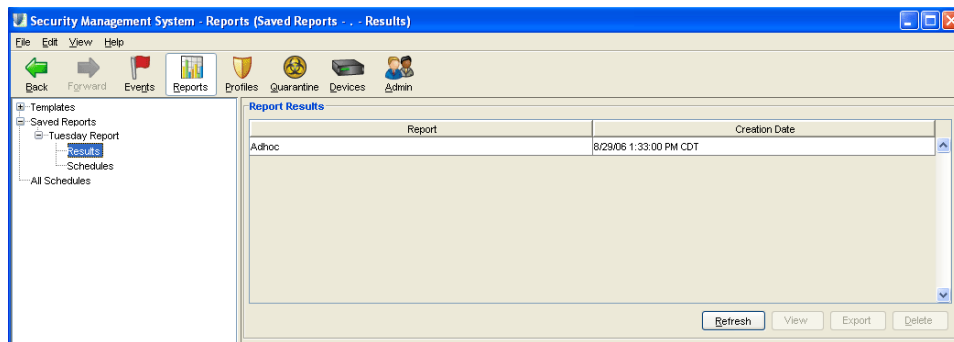
### How To: Delete a Report

1. On the **Reports** Navigation pane, click **Saved Reports**.
2. Select a report.
3. On the Menu Bar, select the **Edit** —> **Delete** menu item.
4. A verification message displays. Click **Yes**.

## View/Export Report Results

Through the Results screen for a saved report, you can view the report results or export the results.

Figure 5 - 24: Report Results Screen



When viewing a report result, the SMS Client displays the information in a pop-up window. From this this window or the main results screen, you can select to export the results. You can also right-click to select rows or copy cell content.

You can save report results in by exporting results. An export button is displayed on the results screen for a saved report and through the **Results - Export Results** pop-up window. To open export results, see [Open Report Results](#).

Exported results can be in the following formats:

- PDF — Generated PDF file accessed using Adobe Reader. This option can include images of graphs.
- 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.



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria and saving the report to email and a web server. The results display in the [Reports List Pane](#).



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

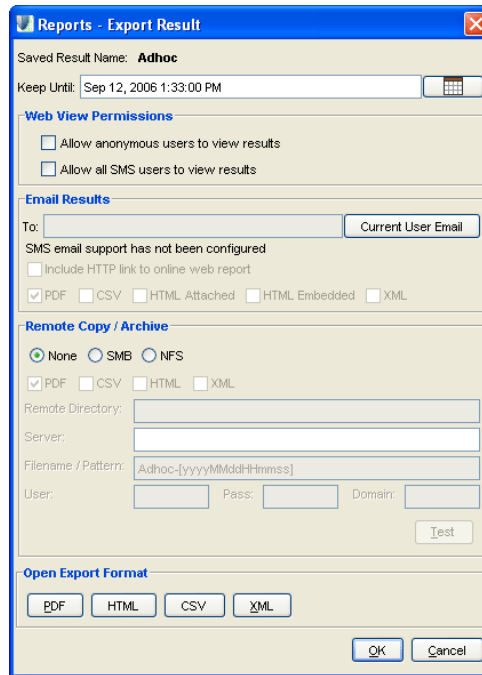
For more information on scheduling and exporting results, see [“Scheduling Reports” on page 140](#).

### How To: Export Report Results

1. On the **Reports** Navigation pane, select **Saved Reports**, expand the report heading that has the report you want to export, and then select **Results**.
2. On the **Report Results** screen, select the report and click **Export**.

3. The **Report - Export Results** pop-up window displays.

Figure 5 - 25: Report - Export Results Window



4. Select a date for **Keep Until**. This date specifies how long the system saves a report result until it is automatically deleted. The system removes results every two weeks after they are created (either by a **Run** command or through a scheduled run).
5. For the **Web View Permissions**, select from the following:
  - **Allow anonymous users to view results** — Selecting this option allows any user to view the report results from the SMS Web Server.
  - **Allow all SMS users to view the results** — Selecting this option allows any SMS authenticated user to view the report from the SMS Web Server regardless of user account settings.
6. For **Email Results**, enter an email address in the field. To send to yourself, click **Current User Email**.
7. Select a format for the results email:
  - PDF
  - CSV
  - HTML attached
  - HTML embedded
  - HTTP link to online web report

The HTTP Link option sends a URL that links to the report's location on the SMS web server. Make sure that the recipient has the correct web permissions to access the report.

8. For **Remote Copy/Archive**, do the following:
  - Select from the options: None (report results are available through the SMS Client and SMS Server Web site), SMB, or NFS.
  - Select a format: PDF, CSV, HTML, and XML.
  - Enter the Remote Directory and Server name.
  - For SMB, enter a user account and password for **User** and **Pass**. Enter the **Domain** to access. This information is required to log into the SMB server to transfer the file(s).
  - To verify the settings, click **Test**.
9. Click **OK**.

### How To: Open Report Results

1. On the **Reports** Navigation pane, select **Saved Reports**, expand the report heading that has the report you want to export, and then select **Results**.
2. On the **Report Results** screen, select the report and click **Export**. The **Report - Export Results** pop-up window displays.

Figure 5 - 26: Results - Export Result Window

3. In the **Open Export Format** section, select one of the following formats: PDF, HTML, CSV, XML. The SMS Client opens the results in a viewer according to the selection, such as executing the Adobe Acrobat Reader program when PDF is selected.
4. The results display.

# All Schedules

This section includes the following topics:

- [“Scheduling Reports” on page 140](#)
- [“Managing Scheduled Reports” on page 143](#)

The SMS system provides report scheduling options to run reports and export results according to date, time, and recurrence. When you create a saved report using a report template or when viewing a saved report, you have the option of scheduling the report.

When you schedule a report, the SMS creates a scheduled report available through the **Saved Reports** and **All Schedules** screens. The SMS groups together the schedules and results for a saved report in the **Saved Reports**. You can browse and display the schedule to view and edit. You can also locate, view, and edit schedules through the **All Schedules** screen.

You can perform the following tasks:

- [“Scheduling Reports” on page 140.](#)
- [“Edit Scheduled Report” on page 144](#)
- [“Delete a Scheduled Report” on page 146](#)

## Scheduling Reports

You can modify a scheduled report through the **Schedule Item** screen for the schedule entry. The scheduled report displays in with the saved report in the **Saved Reports** section and on the **All Schedules** screen. When you create or edit a schedule, you access and display the settings on the **Reports - Schedule Report Details View** dialog box. You can modify schedule settings to generate the report on a specific date or to reoccur according to a set schedule.



**Note** When you schedule the report, it displays in the **Reports** Navigation pane. If the report has expired, a notation follows the name of the listed schedule.

You can edit and manage scheduled report on the **All Schedules** screen. See [“Managing Scheduled Reports” on page 143](#) for details. To schedule a report for running, you must select, modify, and save a report template. Once you save the report, you can select and schedule the report through the **Saved Reports** section. When you create or edit a schedule, the **Reports - Schedule Report Details View** dialog box displays.

## Web View Permissions

Each scheduled report's results are accessible through the SMS Server Web site. When scheduling a report, you can select the permission settings for the reports accessibility. These options include the following:

- **Allow anonymous users to view results** — Selecting this option allows any user to view the report results from the SMS Web Server.
- **Allow all SMS users to view the results** — Selecting this option allows any SMS authenticated user to view the report from the SMS Web Server regardless of user account settings.

## Export Formats

Exported reports can be in the following formats:

- **PDF** — Generated PDF file accessed using Adobe Reader. This option can include images of graphs.
- **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.



**Note** The **Reports** screen can display up to 10,000 rows for results. This limit affects the report you generate, schedule, and save to HTML. You should consider this when entering criteria and saving the report to email and a web server.



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


## Remote Copy/Archive

You can export the results to remote servers and the SMS server archive for saving and reviewing. The system provides options for copying report results in several output formats to a remote SMB or NFS file system. The client allows you to enter remote location information (including the server name and location), a filename and pattern, a user account with password, and the domain. An optional test button allows you to verify the entered settings for the remote server connection before saving the entered settings. The Remote Directory and Server settings control the host and location for exported files. The User, Pass, and Domain settings apply to SMB file systems.

The Filename/Pattern setting describes the base name of the files to be created during export and archiving. The name of the report lists as the Filename. The Pattern is a bracketed timestamp [yyyyMMddHHmmss], which you can modify or remove. When the report runs, the generated filename(s) include the file creation time based on the format of the pattern. If you remove the timestamp pattern, running the report will replace previously saved results (the filename always remain the same). When you select a format option, the export creates a number of files in that format with the appropriate name. For example, Report1 with the PDF and XML formats chosen generates the

following files on the remote server: Report1-20050215120012.pdf and Report1-20050215120012.xml. HTML files export in zip format including any additional files such as image graphs.

### How To: Schedule a Report

1. On the **Reports** Navigation pane, save a report. Select a saved report from the **Saved Reports** section.
2. Do one of the following in the saved report screen:
  - Click **Schedule**.
  - On the Menu Bar, select the **File** —> **Schedule** menu item.
  - You can also create a schedule from the Schedules screen for the selected saved report. The **Reports - Schedule Report Details View** dialog box displays. Select the **General** tab.
3. Enter a **Schedule Name**. The screen displays the report name.
4. For the **Recurrence Pattern**, choose one of the following:
  - **Run Now** — Generates the report immediately.
  - **One Time** — Generates the report one time.
  - **Hourly** — Generates the report once per hour
  - **Daily** — Generates the report once per day
  - **Weekly** — Generates the report once per week
  - **Monthly** — Generate the report once per month
5. For the **Range of Recurrence**, do the following:
  - **No end date** — The report does not have an end date
  - **End By** — Select an end date for the report recurrence. Click the calendar icon  to select the date and time. See [“Date and Time Controls” on page 37](#) for more information.
6. Select the **Permissions and Remote Export** tab.
7. For the **Web View Permissions**, select from the following:
  - **Allow anonymous users to view results** — Selecting this option allows any user to view the report results from the SMS Web Server.
  - **Allow all SMS users to view the results** — Selecting this option allows any SMS authenticated user to view the report from the SMS Web Server regardless of user account settings.
8. For **Email Results**, enter an email address in the field and select a format: PDF, CSV, HTML attached, and/or HTML embedded for the format. An example for the email is: someone@some-where.com. To send to yourself, click **Current User Email**.



9. For **Remote Copy/Archive**, do the following:
  - Select from the options: None (report results are available through the SMS Client and SMS Server Web site), SMB, or NFS.
  - Select a format: PDF, CSV, HTML, and XML.
  - Enter the Remote Directory and Server name.
  - For SMB, enter a user account and password for **User** and **Pass**. Enter the **Domain** to access. This information is required to log into the SMB server to transfer the file(s).
  - To verify the settings, click **Test**.
10. Click **OK**. The scheduled report displays in with the saved report in the **Schedules** section for a report listed in the **Saved Reports** section and on the **All Schedules** screen.

## Managing Scheduled Reports

After creating scheduled reports, you can manage these reports through the **All Schedules** screen. The screen provides options for sorting, viewing, editing, and deleting reports. To sort the listed entries, click the column heading. Each time you click the heading, it toggles between sorting the entries in ascending and descending order depending on the selected column. When you view or edit a scheduled report, the information displays on the **Reports - Schedule Reports Detail View** dialog box.

You can view scheduled reports for a specific saved report through the **Saved Reports** section of the Navigation pane. You can also view all scheduled reports through the **All Schedules** screen.

The following is the **All Schedules** screen:

Figure 5 - 27: All Schedules Screen

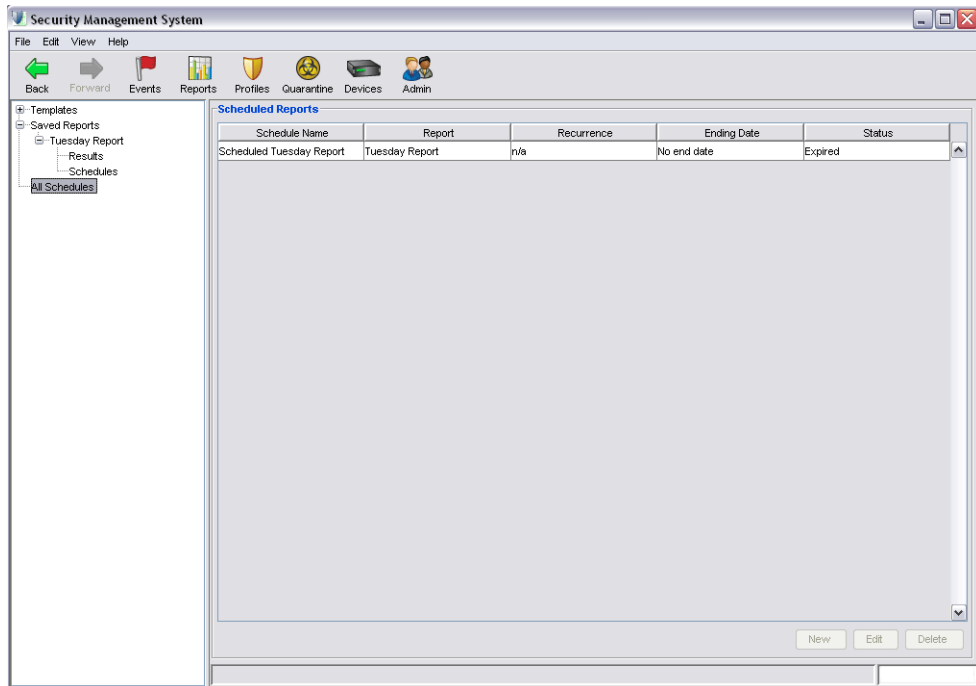



Table 5 - 54: All Scheduled Screen

Column	Description
Schedule Name	Name of the scheduled item
Report	The report to generate
Recurrence	The setting for generation recurrence
Ending Date	The end date for the report generation
Expired	Identifies if the report has expired

#### How To: Edit Scheduled Report

1. On the **Reports** Navigation pane, do one of the following:
  - Select a scheduled report in the **Schedules** section for **Saved Reports**
  - Select **All Schedules**
2. Select a report entry from the list.

3. Do one of the following:
  - Click **Edit**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.
  - Right-click an entry and click **Edit**.

The report displays in the **Reports - Schedule Reports Details View** dialog box.
4. Modify the **Schedule Name**. The screen displays the report name.
5. For the **Recurrence Pattern**, modify the following choice:
  - **Run Now** — Generates the report immediately.
  - **One Time** — Generates the report one time.
  - **Hourly** — Generates the report once per hour
  - **Daily** — Generates the report once per day
  - **Weekly** — Generates the report once per week
  - **Monthly** — Generate the report once per month
6. For the **Range of Recurrence**, modify the following:
  - **No end date** — The report does not have an end date
  - **End By** — Select an end date for the report recurrence. Click the calendar icon  to select the date and time. See [“Date and Time Controls” on page 37](#) for more information.
7. Select the **Permissions and Remote Export** tab.
8. For the **Web View Permissions**, modify the following:
  - **Allow anonymous users to view results** — Selecting this option allows any user to view the report results from the SMS Web Server.
  - **Allow all SMS users to view the results** — Selecting this option allows any SMS authenticated user to view the report from the SMS Web Server regardless of user account settings.
9. For **Email Results**, modify the email address in the field and select a format: PDF, CSV, HTML attached, and/or HTML embedded for the format. An example for the email is: someone@some-where.com. To send to yourself, click **Current User Email**.
10. For **Remote Copy/Archive**, modify the following:
  - Select from the options: None (report results are available through the SMS Client and SMS Server Web site), SMB, or NFS.
  - Select a format: PDF, CSV, HTML, and XML.
  - Enter the Remote Directory and Server name.
  - For SMB, enter a user account and password for **User** and **Pass**. Enter the **Domain** to access. This information is required to log into the SMB server to transfer the file(s).
  - To verify the settings, click **Test**.
11. Click **OK**.

### How To: Delete a Scheduled Report

1. On the **Reports** Navigation pane, do one of the following:
  - Select a scheduled report in the **Schedules** section for **Saved Reports**
  - Select **All Schedules**
2. Select a report entry from the list.
3. Do one of the following:
  - Click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete** menu item.
  - Right-click an entry and click **Delete**.A verification message displays. Click **Yes**.

# 6 Profiles

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

## Overview

This section includes the following topics:

- [“Profiles: What’s New” on page 149](#)
- [“How To Tasks” on page 152](#)
- [“Navigation and Menu Options” on page 154](#)
- [“IPS Profiles \(All Devices\)” on page 157](#)
  - [“IPS Profile Management” on page 157](#)
  - [“IPS Profiles Shared Settings” on page 166](#)
  - [“Profile Overview” on page 183](#)
  - [“Profile Settings” on page 183](#)
  - [“IPS Profile Filters” on page 189](#)
  - [“Application Protection” on page 196](#)
  - [“Infrastructure Protection Filters” on page 208](#)
  - [“Performance Protection Filters” on page 226](#)
  - [“Traffic Management Filters” on page 230](#)
  - [“DDoS Filters \(E-Series Devices\)” on page 235](#)
- [“Firewall Profiles \(X-Family Devices\)” on page 237](#)
- [“VPN Profiles \(X-Family Devices\)” on page 244](#)
- [“Digital Vaccine Management” on page 246](#)
- [“Custom Shield Package Management” on page 254](#)

Profiles provide a method for setting up security configuration options for the TippingPoint solutions. The SMS supports the following types of network security profiles:

**IPS Profile** - a collection of filters that are the key to protection and prevention of malicious invasion on your network and data. IPS devices and X-Family devices support IPS Profiles.

**Firewall Profile** - a collection of rules that control the flow of traffic between Security Zones, provide bandwidth management and ensure quality of service. X-Family devices support Firewall Profiles

**VPN Profiles** - a collection of rules for defining a secure private network connection between devices across a public network. X-Family devices support VPN Profiles

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.

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 Custom Shield 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 Custom Shield packages also fall under this type of protection as you can distribute these packages to individual devices.
- **Segmental** — These settings affect only a particular segment or segment group; segmental settings do not affect an entire device. Examples of these include an IPS profile or firewall profile distributed to a segment group.



**Note** Virtual segments are used with V2.5 and above device. For V2.5+ and above, physical segments can be used but cannot be not created. Security zones are used with X-Family devices. For more information, see [“IPS Devices: Network Configuration” on page 366](#) and [“Network Configuration: Segments/Zones Tab” on page 395](#).

Each filter, action set, notification contact, and Digital Vaccine package affects your devices and segments according to these levels of security. Enterprise-wide changes affect all devices and supersede device-wide and segmental settings. And Device-wide changes supersede Segmental settings. See [“Segments and Security Zones” on page 12](#) for more information.

# Profiles: What's New

This section outlines the following major changes for the current SMS release:

- [“Virtual Segments” on page 149](#)
- [“Profile Snapshots” on page 149](#)
- [“X-Family Devices” on page 149](#)
- [“IPS Profiles” on page 150](#)
- [“IPS Profile Filters” on page 150](#)

## Virtual Segments

Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events. See [“Network Configuration: Segments/Zones Tab” on page 395](#).

## Profile Snapshots

Exported profile snapshots now save the action sets, contacts, and services that are reference by Filters and Category Settings in the profile. Then the profile is imported, the actionsets and contacts are also imported. The additional ports defined by the exported service are updated on the SMS as well, but do not overwrite any existing Service definitions. For example, if the SMS does not have an updated **auth-tcp** service, both that service is defined in the exported profile, an update is made to the **auth-tcp** service. If the SMS receiving the imported profile already has a definition for auth-tcp, no updates are made to that service when importing a profile.

## X-Family Devices

### *Firewall Profiles*

This release adds SMS support for configuring firewall rules for X-Family devices. This is available under the new Firewall Profile tree item. Like the IPS Profile, there are Enterprise-wide Shared Settings that all devices using the Firewall Profile share. These Shared Settings include Services, Service Groups, and Schedules.

Multiple firewall profiles can be created and distributed to appropriate X-Family devices in your network. This allows you to maintain a single firewall profile that can be used by similar X-Family devices. This can save you time because firewall rules do not have to be defined for each individual device. Rather, you can define a firewall profile and then distribute the profile to devices with similar network configurations. If individual device firewall rules are desired, they can also be created through the firewall profile. See, [“Firewall Profiles \(X-Family Devices\)” on page 237](#).

### *VPN Network Profiles*

The current release adds SMS support for X-Family devices with the following tabs:

- IKE Proposals
- Security Zones

See, [“VPN Profiles \(X-Family Devices\)” on page 244](#).

## IPS Profiles

With this release, the **Profiles** listing in the Navigation pane was renamed to **IPS Profiles**. The profiles apply to all devices including IPS and X-Family devices. See [“IPS Profiles \(All Devices\)” on page 157](#).

### *Quarantine Actions*

Quarantine actions are now incorporated into IPS profiles. Before they were under the Quarantine actions tab. X-Family devices features, such as Firewall and VPN, have separate profiles, and profile listing in the Navigation pane.

### *Categories*

This release of the TippingPoint SMS has new category settings. In addition, some existing category settings were removed or renamed. This provides finer grained control over various filter groupings, such as Virus and Spyware filters.



**Note** The SMS continues to support removed or changed categories for devices running previous TippingPoint software versions.

### *Profile Overview*

Profile Overview is now a separate tree listing item for an IPS profile in the Navigation pane. This item was previously on a tab on the Profile Details screen. The Profile Overview shows the modified filters in the profile as well as displaying Shared Setting objects that are used by the profile. For example, if a filter uses action set **My Block Action**, then the Profile Overview will list that action set.

### *Advanced Search*

**Advanced Search** for IPS profiles now allows you to save searches. These saved searches can be named and later re-run at a future time. See [“Advanced Search” on page 150](#).

## IPS Profile Filters

This section contains the following topics:

- [Application Protection](#)
- [Infrastructure Protection](#)
- [Performance Protection](#)
- [Segments](#)

### **Application Protection**

The SMS previously displayed the Attack Protection as the two groups, **Exploits** and **Vulnerabilities**. The IPS devices support the two categories having different settings. However, the LSM does not



display the categories separately. **Exploits** will not be seen on pre-2.5 LSM. **Vulnerabilities** is displayed on LSM as the old category name, Attack Protection.

- **Exploits** — New. Filters in this category were previously under **Attack Protection**, but were displayed as **Attack - Exploits**. Attack Protection has now been split into its component parts and **Exploits** is now a separate category.
- **Identity Theft** — New
- **Informational** — This category was removed from the current release. The majority of filters in this category were moved to the Security Policy category.
- **Reconnaissance** — This category setting has not changed, but the display of the filters in this category has changed. The Scans and Sweeps filters are now displayed directly under the Reconnaissance tree listing. To view these entries, use the scroll bar to scroll to the bottom of the filter listing.
- **Security Policy** — This category has new listings from the Informational category.
- **Spyware** — New
- **Virus** — New
- **Vulnerabilities** — New. Filters in this category were previously under Attack Protection, but were displayed as **Attack - Vulnerabilities**. **Attack Protection** has now been split into its component parts and **Vulnerabilities** is now a separate category.

See [“Application Protection” on page 196](#).

## Infrastructure Protection

- **DDoS** — This category only applied to 1.4.2 DDoS (Distributed Denial of Service) filters. Release 1.4.2 is no longer supported, so this category has been removed.
- **Network Equipment Protection** — No change
- **Traffic Normalization** — No change

See [“Infrastructure Protection Filters” on page 208](#).

## Performance Protection

- Peer to Peer (P2P) — Renamed from Misuse and Abuse
- Instant Messaging — New
- Streaming Media — New

See [“Performance Protection Filters” on page 226](#).

## Segments

Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events. See [“Network Configuration: Segments/Zones Tab” on page 395](#).

# How To Tasks

## ***IPS Profile Management***

- [“How To: Create a Profile” on page 161](#)
- [“How To: Copy a Profile” on page 161](#)
- [“How To: Edit a Profile Details” on page 162](#)
- [“How To: Delete a Profile” on page 162](#)
- [“How To: Snapshot a Profile Version” on page 162](#)
- [“How To: Activate a Profile Version” on page 163](#)
- [“How To: View Profile Version Details” on page 163](#)

## ***IPS Profile Distribution***

- [“How To: Distribute a Profile” on page 165](#)
- [“How To: Cancel a Distribution In-Progress” on page 166](#)

## ***IPS Profile Shared Settings***

- [“How To: Create/Edit an Action Set” on page 172](#)
- [“How To: Configure a Quarantine Action Set” on page 174](#)
- [“How To: Set Aggregation Settings” on page 179](#)
- [“How To: Create an Email Notification Contact” on page 179](#)
- [“How To: Edit an Email Notification Contact” on page 179](#)
- [“How To: Create a SNMP Notification Contact” on page 180](#)
- [“How To: Edit an SNMP Notification Contact” on page 180](#)
- [“How To: Set Aggregation Settings” on page 181](#)
- [“How To: Add a Non-Standard Port” on page 183](#)
- [“How To: Delete a Non-Standard Port” on page 183](#)

## ***IPS Profile Settings***

- [“How To: Create an Attack Filter Profile Restriction” on page 185](#)
- [“How To: Edit an Attack Filter Profile Restriction” on page 185](#)
- [“How To: Delete an Attack Filter Profile Restriction” on page 186](#)
- [“How To: Create an Attack Filter Profile Exception” on page 186](#)
- [“How To: Edit an Attack Filter Profile Exception” on page 186](#)
- [“How To: Delete an Attack Filter Exception” on page 187](#)
- [“How To: Create a Profile Performance Protection Restrictions” on page 188](#)
- [“How To: Edit Global Performance Protection Restrictions” on page 188](#)
- [“How To: Delete Global Performance Protection Restriction” on page 188](#)

## ***IPS Profile Filters***

- [“How To: Search/View a Filter” on page 191](#)
- [“How To: Perform an Advanced Search” on page 192](#)
- [“How To: Edit Multiple Filters” on page 194](#)

***Application Protection Filters***

- [“How To: Edit Application Protection Category Settings” on page 200](#)
- [“How To: Edit an Application Protection Filter” on page 200](#)
- [“How To: Create Filter Exception” on page 203](#)
- [“How To: Delete Filter Exception” on page 204](#)

***Infrastructure Protection Filters***

- [“How To: Edit Infrastructure Protection Category Settings” on page 210](#)
- [“How To: Create Filter Exception” on page 211](#)
- [“How To: Delete Filter Exception” on page 211](#)
- [“How To: Create/Edit an Advanced DDoS Filter for 100E/200E/210E Models” on page 213](#)
- [“How To: Create/Edit an Advanced DDoS Filter for 1200E/2400E/5000E Models” on page 216](#)
- [“How To: Create an Advanced DDoS Exception for 100E/200E/210E Models” on page 217](#)
- [“How To: Edit an Advanced DDoS Exception for 100E/200E/210E Models” on page 218](#)
- [“How To: Delete an Advanced DDoS Exception for 100E/200E/210E Models” on page 219](#)
- [“How To: Create/Edit an Advanced DDoS Exception for 1200E/2400E/5000E Models” on page 219](#)
- [“How To: Edit a Network Equipment Filter” on page 220](#)
- [“How To: Edit a Traffic Normalization Filter” on page 222](#)
- [“How To: Create/Edit a Traffic Threshold Filter” on page 224](#)
- [“How To: Delete a Traffic Threshold Filter” on page 225](#)

***Performance Protection Filters***

- [“How To: Edit Performance Protection Category Settings” on page 228](#)
- [“How To: Edit a Performance Protection Filter” on page 229](#)

***Traffic Management Filters***

- [“How To: Create/Edit a Traffic Management Filter” on page 232](#)
- [“How To: Delete a Traffic Management Filter” on page 234](#)
- [“How To: Save the Traffic Management Filter Order” on page 234](#)

***DDoS Filters (E-Series)***

- [“How To: Edit a DDoS Filter” on page 236](#)
- [“How To: Add a Firewall Profile” on page 238](#)

***Firewall Profiles (X-Family)***

- [“How To: Distribute a Firewall Profile” on page 238](#)
- [“How To: Add a Firewall Rule” on page 239](#)
- [“How To: Manage Firewall Rules” on page 240](#)
- [“How To: Edit a Firewall Rule” on page 240](#)
- [“How To: Add a Custom Service” on page 241](#)
- [“How To: Edit a Custom Service” on page 242](#)
- [“How To: Add a Service Group” on page 242](#)
- [“How To: Edit a Custom Service” on page 242](#)
- [“How To: Add a Schedule” on page 243](#)

- [“How To: Edit a Schedule” on page 243](#)
- [“How To: Set up a common definition for common parameters” on page 243](#)
- [“How To: Associate a common name with a firewall profile” on page 244](#)

### ***VPN Profiles (X-Family)***

- [“How To: Set up a VPN Profile” on page 245](#)
- [“How To: Deploy a VPN Profile” on page 245](#)
- [“How To: Set up IPSec Security Association” on page 246](#)

### ***Digital Vaccine Management***

- [“How To: Auto-Download New Digital Vaccine Packages” on page 250](#)
- [“How To: Download a Digital Vaccine Package” on page 250](#)
- [“How To: Import a Digital Vaccine Package” on page 250](#)
- [“How To: Delete a Digital Vaccine Package” on page 251](#)
- [“How To: Activate a Digital Vaccine Package” on page 251](#)
- [“How To: View Details of a Digital Vaccine Package” on page 252](#)
- [“How To: Auto-Distribute New Packages” on page 253](#)
- [“How To: Distribute New Packages” on page 253](#)
- [“How To: Cancel a Distribution Process” on page 254](#)
- [“How To: New Scheduled Distribution” on page 254](#)
- [“How To: Edit Scheduled Distribution” on page 254](#)

### ***Custom Shield Package Management***

- [“How To: Import and Activate a Custom Package” on page 256](#)
- [“How To: Import a Custom Shield Package” on page 257](#)
- [“How To: Delete a Custom Shield Package” on page 258](#)
- [“How To: Activate/Deactivate a Custom Shield Package” on page 258](#)
- [“How To: View Details of a Custom Shield Package” on page 258](#)
- [“How To: Uninstall a CSW Package” on page 259](#)
- [“How To: Distribute New Packages” on page 259](#)

## Navigation and Menu Options

### Profiles Screen

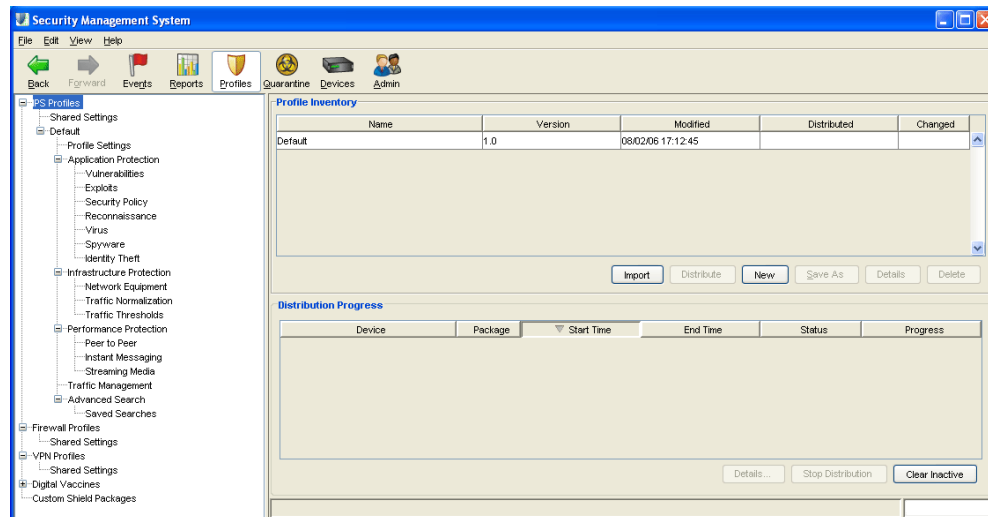
To open the **Profiles** screen, click the **Profiles** button on the Toolbar. This screen is designed for managing and tuning your system's response to attack traffic, customizing shared settings, implementing firewall rules, configuring VPN, and implementing Digital Vaccine and Custom Shield packages.



**Note** You must distribute any modifications to the IPS devices for your changes to take effect. See [“Distributing Profiles” on page 163](#).

The following is the **Profiles** screen:

Figure 6 - 1: Profiles Screen



From the left Navigation pane on the **Profiles** screen you can manage the following types of profiles and network protection packages:

- [IPS Profiles \(All Devices\)](#) — Encapsulate all 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:
  - Application Protection
  - Infrastructure Protection
  - Performance Protection
  - Traffic Management

See [IPS Profile Filters](#) and subsequent filter pillar sections for more information.

- [“Firewall Profiles \(X-Family Devices\)” on page 237](#) — Prioritize, permit, block, filter, authenticate, schedule and monitor traffic
- [“VPN Profiles \(X-Family Devices\)” on page 244](#) — Create and deploy a VPN profile for VPN networks among the X-Family devices that the SMS manages.
- [Digital Vaccine Management](#) — Import and distribute a Digital Vaccine package to devices on the SMS system.
- [Custom Shield Package Management](#) — Import and distribute a Custom Shield package to devices on the SMS system.

## Menu Bar Options

The available menu items for the Menu Bar differ according to the displayed screen and user access settings. Each screen provides options for the following:



**Note** The following list may change depending on the displayed screen or selected item in the main pane. Selected options display in the Main/List pane. For more information on that pane, see “Main/List Pane” on page 18.

- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:
  - *New* — Creates a new item based on selection, such as a new profile for IPS, firewall, or VPN. You can also add entries to the appropriate **Shared Settings**.
  - *Download Digital Vaccine from TMC* — Downloads the latest Digital Vaccine package
  - *Import* — Imports the selected data, such as Digital Vaccine or Custom Shield package
  - *Distribute to Device* — Distributes data based on selection, such as an IPS profile, firewall profile, VPN profile or Digital Vaccine package.
  - *Logoff* — Logs you out of the SMS
  - *Exit* — Closes the SMS
- **Edit** — Provides edit options based on the currently selected and displayed screen
  - *Details* — Displays the details of a selected entry
  - *Copy* — Creates a copy of a selected entry
  - *Permissions...* — Provides permission control to a selected profile based on account type
  - *Delete* — Deletes a selected entry
  - *Profile Settings* — Allows you to edit the restrictions and exceptions for a select IPS profile
  - *Category Settings* — Allows you to edit the IPS category settings based on the selected category
  - *Filters* — Displays IPS filters of the category selected for editing
  - *Preferences* — Displays the System Preferences dialog box. See [“System Preferences” on page 27](#).
- **View** — Displays the screens for the options listed in the Navigation Pane.
  - *Profiles*
  - *Shared Settings*
  - *Firewall Profiles*
  - *Digital Vaccines*
  - *Custom Shield Packages*
  - *Dashboard* (see [“SMS Dashboard” on page 24](#))
- **Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

# IPS Profiles (All Devices)

This section contains the following topics.

- [“IPS Profile Management” on page 157](#)
- [“IPS Profiles Shared Settings” on page 166](#)
- [“Profile Settings” on page 183](#)
- [“IPS Profile Filters” on page 189](#)
- [“Application Protection” on page 196](#)
- [“Infrastructure Protection Filters” on page 208](#)
- [“Performance Protection Filters” on page 226](#)
- [“Traffic Management Filters” on page 230](#)
- [“DDoS Filters \(E-Series Devices\)” on page 235](#)

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 depending 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 IPS 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.

**Shared Settings** are used by all IPS profiles on the SMS. These settings are enterprise-wide, affecting all devices on your system. Shared Settings include the following:

- **Action Sets** — The instructions for handling traffic. See [“Action Sets Tab” on page 167](#).
- **Notification Contacts** — The recipients of notification alerts. These contacts include the SMS, management console, the remote syslog, and other users. See [“Notification Contacts Tab” on page 176](#)
- **Services** — The services for managing additional non-standard ports. See [“Services” on page 181](#).

## IPS Profile Management

This section contains the following sections:

- [“Viewing Profile Information” on page 158](#)
- [“Managing IPS Profiles” on page 159](#)
- [“Profile Management Tasks” on page 160](#)
- [“Distributing Profiles” on page 163](#)

You can create, copy, distribute, and create version snapshots of profiles in your system. As you enter changes, the profile updates to include all changes such as the following:

- Download any updates for the Digital Vaccine and Custom Shield packages
- Create, modify, or delete shared and custom filter exceptions
- Create, modify, or delete custom filters
- Modify the order of Traffic Management filters
- Create and manage services
- Create, modify, or delete notification contacts and action sets

Each profile contain modified filters and category settings. Each profile contains a set of filters that you can modify with custom settings including action sets, exceptions, and selected notification contacts.

### Viewing Profile Information

Through the **Profiles** screen for a select profile, you can review the details and versioning of the entire profile at a glance. The screen displays general details with options for distributing updates as well as saving versions of your profile using snapshots

#### *Profile Versioning*

The SMS provides versioning for profiles allowing you to create or snapshot, distribute, and revert to specific versions of a profile. A version of a profile gives a numbered sequence for a profile as you manage, modify, and distribute it across your system. Through versioning, you can create a snapshot of a profile that stores an image of the profile including filters, exceptions, and IP restriction filters.

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 details of each version listed on the **Profiles - Versions** screen lists the changes entered and saved or distributed for the version. You can use snapshots as saved versions of the profile to revert to at any time for associated segments or segment group.



The following is the **Profile** screens for general details and version information:

Figure 6 - 2: Profiles - Details Screen

Segment/Segment Group	Distributed	Version	Changed
qlab-device07:LAN-LAN2 (LAN->LAN2...	8/30/06 3:21:43 PM CDT	1.1	
qlab-device07:LAN2-LAN (LAN2->LAN...	8/30/06 3:21:43 PM CDT	1.1	
qlab-dev7-LANs	8/30/06 3:21:43 PM CDT	1.1	

Figure 6 - 3: Profiles - Versions Screen

Active	Version	Created	Distributed	Comment
	1.0			Active version

The **Profile - Overview** screen provides detailed information regarding modifications of the profile. You can sort through the information 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 actions sets, notification contacts, and services used by profile.

## Managing IPS Profiles

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. When you create a new profile, the system builds a profile. You can then manage the profile and filters.

The tree under **IPS Profiles** screen also includes Shared Settings. The Shared Settings of the SMS include services, action sets, and notification contacts shared by all categories of filters in the system.



**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.

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. When you create a new profile, the system builds a profile based on the currently activated Digital Vaccine settings.

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.

### Profile Management Tasks

When creating a profile, you can do one of the following:

- Create a new profile with the Digital Vaccine set of filters
- Copy an existing profile and modify the contained filters
- Delete an existing profile
- Create a snapshot of the profile version

You can perform the following tasks:

- [“Create a Profile” on page 161](#)
- [“Copy a Profile” on page 161](#)
- [“Delete a Profile” on page 162](#)
- [“Snapshot a Profile Version” on page 162](#)
- [“Activate a Profile Version” on page 163](#)
- [“View Profile Version Details” on page 163](#)

IPS Profiles include the following pillars of filters and Shared Settings:

- [“IPS Profiles Shared Settings” on page 166](#)
  - [“Action Sets Tab” on page 167](#)
  - [“Notification Contacts Tab” on page 176](#)
  - [“Services” on page 181](#)
- [“IPS Profile Filters” on page 189](#)
  - [“Application Protection” on page 196](#)
  - [“Infrastructure Protection Filters” on page 208](#)
  - [“Performance Protection Filters” on page 226](#)
- [“Traffic Management Filters” on page 230](#)

### How To: Create a Profile

1. In the **Profiles** navigation pane, click the **Profiles** tab. The **Profiles** screen displays.
2. Do one of the following:
  - From the **Profile Inventory** area, Click **New**.
  - On the Menu Bar, select the **File** —> **New** —> **IPS Profile** menu item.
  - Right-click an entry in the **Profile Inventory** table and click **New**.

The **Profiles - Create New Profile** screens displays.

3. Enter a **Name** for the profile.
4. Enter a **Description** for the profile.
5. Click **OK**.

### How To: Copy a Profile

1. In the **Profiles** navigation pane, click **Profiles**. The **Profiles** screen displays.
2. Select a profile from the inventory.
3. Do one of the following:
  - From the **Profile Inventory** area, click **Save As**.
  - Right-click and entry in the **Profile Inventory** table and 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.

4. Enter a **Name**. The default name is “Copy of” added to the copied profile name.
5. Enter a **Description**.
6. Click **OK**.

### How To: Edit a Profile Details

1. In the **Profiles** navigation pane, click **Profiles**. The **Profiles** screen displays.
2. Do one of the following:
  - From the **Profile Inventory** area, select a profile, and click **Details**.
  - From the **Profile Inventory** area, select a profile, and then select the **Edit** —> **Details** menu item from the Menu Bar.
  - Double-click a profile from the **Profile Inventory** table.
  - Click the profile from the **Profiles** navigation pane.
  - Right-click and entry in the **Profile Inventory** table and select **Edit > Details**.

The **Profile Details** screen displays.

3. Make any changes and click **Save**.

### How To: Delete a Profile

1. In the **Profiles** navigation pane, click **Profiles**. The **Profiles** screen displays.
2. Select a profile from the inventory.
3. Do one of the following:
  - From the **Profile Inventory** area, click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete** menu item.
  - Right-click an entry and select **Edit** —> **Delete**.
4. A deletion verification alert message displays. Click **Yes** to delete.

### How To: Snapshot a Profile Version

1. In the **Profiles** navigation pane, click **Profiles**. The **Profiles** screen displays.
2. Do one of the following:
  - From the **Profile Inventory** area, select a profile, and click **Details**.
  - From the **Profile Inventory** area, select a profile, and then select the **Edit** —> **Details** menu item from the Menu Bar.
  - Double-click a profile from the **Profile Inventory** table.
  - Click the profile from the **Profiles** navigation pane.
  - Right-click and entry in the **Profile Inventory** table and select **Edit > Details**.

The **Profile Details** screen displays.

3. Click **Snapshot**. A snapshot of the current version of the profile is created.
4. Click the **Versions** tab. The new entry displays in the **All Versions** table.

### How To: Activate a Profile Version

1. In the **Profiles** navigation pane, select a profile. The **Profiles Details** screen for the selected profile displays.
2. Click the **Versions** tab.
3. Select a profile version.
4. Click **Activate**. The selected profile activates as the current profile replacing all filter changes with changes from the snapshot.

### How To: View Profile Version Details

1. In the **Profiles** navigation pane, select a profile. The **Profiles Details** screen for the selected profile displays.
2. Click the **Versions** tab.
3. Select a profile version.
4. Click **Details**. The selected profile version displays the change list of modifications.

## Distributing Profiles

When you distribute a profile, you send the modified and updated profile to all selected segments. 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 or a single segment. For more information on segment grouping, see [“Segment Groups” on page 337](#).



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



**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.

### DV Version Verification

When distributing a profile, there is a check to verify that the SMS and the IPS are running the same DV version. This check prevents the SMS from being updated with a new DV while the IPS is not updates. You can view DV version for single segments distribution.

### High/Low Priority Distributions — Performance

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 distribution files and profile updates before low priority updates. 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. High-priority distributions send files and filter updates through the system over other processes. However, during the update, you may experience 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.

### ***Profile Inventory and Distribution Process Details***

You distribute profiles from the **Profiles** main screen or the Details screen for a selected profile. This screen includes the following information:

**Table 6 - 1: Profile Inventory Details**

Column	Description
Name	The name of the profile
Modified	The date and time the profile was last modified
Distributed	The date and time the profile was last distributed successfully

**Table 6 - 2: Distribution Process Details**

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 <i>Complete (Success)</i>
Progress	Current progress of the distribution

Modifications that require a distribution:

- 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 filters



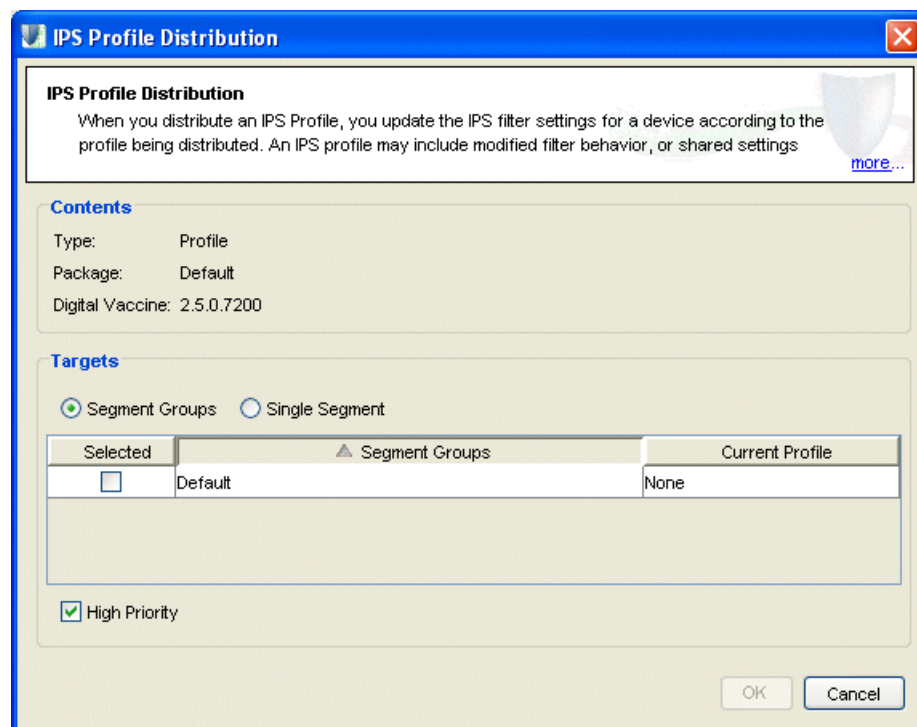
**Note** If you receive errors or have issues distributing profiles due to exceeded limits of filters or exceptions, see [“SMS Error Messages” on page 543](#).

See [“Distribute a Profile” on page 165](#) and [“Cancel a Distribution In-Progress” on page 166](#).

### How To: Distribute a Profile

1. On the Toolbar, click **Profiles**, and then select **IPS Profiles** from the navigation pane. The **Profiles** screen displays.
2. Do one of the following:
  - From the **Profile Inventory** area, select a profile, and click **Distribute**.
  - From the **Profile Inventory** area, select a profile, and then select the **Edit** —> **Distribute** menu item from the Menu Bar.
  - Double-click a profile from the **Profile Inventory** table and then click **Distribute**.
  - Click the profile from the **Profiles** navigation pane and then click and click **Distribute**.
  - Right-click an entry in the **Profile Inventory** table and select **Edit** > and click **Distribute**.
3. In the **Profile Inventory** section, select a profile entry to distribute. You can also distribute a profile from the **Profile** > **Details** screen.  
The **Profiles - Profile Distribution** dialog box displays.

Figure 6 - 4: Profiles - Profile Distribution Dialog Box



4. Select the distribution segments: **Segment Group** or **Single Segment**. Selecting a single segment distributes the profile only to that segment.
5. Select the check box for each entry you want to distribute.
6. For a high priority distribution, select the **High Priority** check box.
7. Click **OK**.

The system begins 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. For more information on segment grouping, see [“Segment Groups” on page 337](#).



**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.

### How To: Cancel a Distribution In-Progress

1. On the Toolbar, click **Profiles**. The **Profiles** screen displays.
2. In the **Distribution Progress** section, select a distribution process to cancel.
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 greyed out, the distribution cannot be cancelled.

## IPS Profiles Shared Settings

This section contains the following topics:

- [“Action Sets Tab” on page 167](#)
- [“Notification Contacts Tab” on page 176](#)
- [“Services” on page 181](#)

Shared Settings include common configuration objects that are shared by all IPS profiles on the SMS. These settings include action sets, notification contacts, and services. Shared settings affect the entire system. When you create or modify action sets, notification contacts, and services, all devices and their segments receive the available settings.



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

You can create the following types of shared settings:

- [Action Sets Tab](#) — Define actions that take place when a filter reacts to an attack.
- [Notification Contacts Tab](#) — Define recipients of alert messages, such as email and SNMP alerts. Notifications are specified in the action set.
- [Services](#) — Add and manage additional Non-Standard Ports for services.



You can perform the following tasks:

- [“Create/Edit an Action Set” on page 172](#)
- [“Configure a Quarantine Action Set” on page 174](#)
- [“Set Aggregation Settings” on page 179](#)
- [“Create an Email Notification Contact” on page 179](#)
- [“Edit an Email Notification Contact” on page 179](#)
- [“Create a SNMP Notification Contact” on page 180](#)
- [“Edit an SNMP Notification Contact” on page 180](#)
- [“Set Aggregation Settings” on page 181](#)
- [“Add a Non-Standard Port” on page 183](#)
- [“Delete a Non-Standard Port” on page 183](#)

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

- 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.

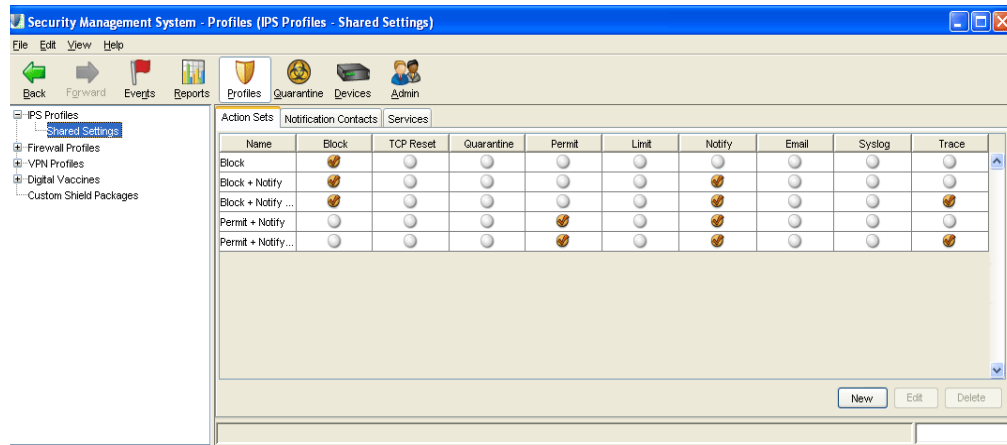
## Action Sets Tab

This section contains the following topics:

- [“Setting Up Action Sets” on page 169](#)
- [“Block Options” on page 170](#)
- [“Creating Action Sets” on page 171](#)
- [“Rate-Limiting” on page 175](#)

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. Action sets determine what the IPS does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action.


Figure 6 - 5: Shared Settings - Action Sets Tab



The **Shared Settings - Actions Sets** tab displays the following information:

Table 6 - 3: Action Sets: Inventory Details

Column	Description
Name	The name of the action
Block	Indicates if the action sets provides the Block action enabled
TCP Reset	Indicates if the action set has a TCP reset setting enabled (for either source, destination, or both)
Quarantine	Indicates if the action set has the Quarantine option enabled (requires additional configuration)
Permit	Indicates if the action set has the Permit action enabled
Limit	Indicates if the action sets provides the Rate-Limit action enabled
Notify	Indicates if the action set provides notifications
Email	Indicates if the action set has notification contacts enabled
Syslog	Indicates if the action set has syslog logging enabled
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.



**Note** Devices using V 2.1 use a feature called Blacklist for Block action sets. Devices using V 2.2 use a feature called Quarantine for Block actions sets (replacing Blacklist functionality). For these devices, create quarantine action sets. The SMS will use the actions appropriately for the older version device.

Performance Protection filters cannot use permit actions.

## Setting Up Action Sets

Actions sets can include any combination of the following actions:

- **Block** — Blocks a packet from being transferred to the network
- **Permit** — Permits a packet
- **Notify** — Notifies all selected contacts of the packet
- **Trace** — Logs all information about the packet according to the packet trace settings

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

Table 6 - 4: Action Sets: Default Actions Sets and Options

Type	Description	Block Options
<b>Block</b>	Blocks a packet from being transferred to the network.	<b>TCP Reset</b> —resets blocked TCP flows <b>Quarantine</b> —manages internal and external threats by quarantining network connections.
<b>Block + Notify</b>	Blocks a packet from being transferred and notifies all selected contacts of the blocked packet.	<b>TCP Reset</b> —resets blocked TCP flows <b>Quarantine</b> —manages internal and external threats by quarantining network connections.
<b>Block + Notify + Trace</b>	Blocks a packet from being transferred, notifies all selected contacts of the blocked packet, and logs all information about the packet according to the packet trace settings.	<b>TCP Reset</b> —resets blocked TCP flows <b>Quarantine</b> —manages internal and external threats by quarantining network connections.
<b>Permit + Notify</b>	Permits a packet and notifies all selected contacts of the packet.	
<b>Permit + Notify + Trace</b>	Permits a packet, notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings.	

## Block Options

Block options include the following items:

**TCP Reset Block Action**— Enables the device to reset TCP flows, which ends the session. You can set the option to reset the source or destination IP. The TCP Reset can also affect both sides of the connection, source and destination.

If you configure a TCP Reset option with Quarantine, the TCP Reset will be sent in response to the first packet which triggers the action. All other packets after that are treated according to the quarantine settings for that action set.

**Quarantine Block Action** — Enhances your devices to contain or remove offending network users or devices and provides the ability to automate sophisticated responses to security events. By enabling quarantine with a Block action set, you reduce the exposure of your network to internal and external threats.

When an IP address/system is quarantined, you can review the list and manage the status of these systems through the **Quarantine - Quarantined Addresses** screen. See [“Quarantined Hosts” on page 266](#).



**Note** The quarantine option is a sub-action of the Block action set. This is because the first packet that triggers the action will be blocked, regardless of the quarantine settings specified. If you configure TCP Reset as part of your quarantine action set, the TCP Reset is sent in response to the first packet that triggers the action. All other packets after that are managed according to the quarantine settings for that action set.

The Quarantine Block action set allows you to enter settings for:

- **Web Requests** — manages all HTTP traffic from the quarantined addresses. Block the requests entirely, redirect the client to another web server, or display the triggered filter, its description, and a customized message (the feature also provides options for non-HTTP traffic to be blocked or permitted.)



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

- **Other Traffic** — Configures the response to other non-HTTP traffic from the quarantined host.
- **Thresholds** — Configures hit count, and period in minutes
- the following Quarantine items:
- **Restrictions (tab)** — allows you to create a list of “limit to” IP addresses, or Restrictions. This option limits the filter using this action set to quarantine only those connections and systems matching the IP addresses listed.
- **Exceptions (tab)** — allows you to create a list of excluded IP addresses, or Exceptions, which will not be quarantined. Despite the filter triggering, these IP addresses will not be quarantined, continuing with any other commands in the action set. For example, the action set may include quarantine commands to block the traffic and redirect web requests to a particular server.
- **Quarantined Access (tab)** — When a client is detected as malicious and is quarantined, network administrators may need to access 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.

## Creating Action Sets

The types of actions and associated options that can be specified are outlined in the following table:

Table 6 - 5: Action Sets: Available Actions Sets and Options

Action	Options
<b>Flow Control</b> Determines where a packet is sent after it is inspected.	<b>Permit</b> — allows a packet to reach its intended destination
	<b>Block</b> — discards a packet <ul style="list-style-type: none"> <li>• <b>TCP Reset</b> —resets blocked TCP flows</li> <li>• <b>Quarantine</b> —manages internal and external threats by quarantining network connections</li> </ul> See <a href="#">“Block Options” on page 170</a> .
	<b>Rate Limit</b> — enables you to define a maximum bandwidth.
<b>Notify</b> Lists the contacts to notify about the event. These contacts can be systems, individuals, or groups	<b>Email Notification Contacts</b>
	<b>SNMP Notification Contacts</b>
<b>SMS Actions</b> Provides the option of using SMS Quarantine	
<b>Log</b> Provides tracking	<b>Remote Syslog</b>
	<b>Packet Trace</b> 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. <ul style="list-style-type: none"> <li>• <b>Priority</b> — Sets the relative importance of the information captured. Low priority items will be discarded before medium priority items if there is a resource shortage.</li> <li>• <b>Level</b> — 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.</li> </ul>

See also [“Create/Edit an Action Set” on page 172](#) and [“Configure a Quarantine Action Set” on page 174](#).

### How To: Create/Edit an Action Set

1. On the **Shared Settings - Action Sets** screen, to create an action set:
  - Click **New**.
  - On the Menu Bar, select the **File** —> **New** —> **Action Set** menu item.
  - Right click an entry and click **New**.

To edit, select an action set and:

- Click **Edit**.
- On the Menu Bar, click **Edit** —> **Details**.
- Double-click the filter.
- Right-click the filter and choose **Edit**.

The **Profiles - Action Set - Edit** screen displays.

Figure 6 - 6: Profiles - Action Set - Edit Dialog Box

The screenshot shows the 'Filters - Action Set - Edit' dialog box. It features a title bar with a close button. Below the title bar is a 'Name:' field with a 'Required' label. The main area is divided into several sections:

- Flow Control:** Contains radio buttons for 'Block', 'TCP Reset', 'Quarantine', 'Permit', and 'Rate Limit'. The 'Block' option is selected. There are also dropdown menus for 'Source' and 'Rate' (set to 50 Kbps).
- Notify:** Contains two lists: 'Email Notification Contacts' and 'SNMP Notification Contacts'. Each list has 'Add' and 'Delete' buttons.
- SMS Actions:** Contains a checkbox for 'SMS Quarantine' and a dropdown menu for 'Default Quarantine'.
- Log:** Contains checkboxes for 'Remote Syslog' and 'Packet Trace'. Below these are dropdown menus for 'Level' (set to Full) and 'Priority' (set to High), along with a text input for 'bytes' (set to 0).

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

2. Enter a **Name** for the action set.

3. Select a **Flow Control**:
  - **Block** — Select to block traffic
  - **TCP Reset** — Used with the **Block** action, resets the source, destination, or both IPs of an attack. This option resets blocked TCP flows.
  - **Quarantine** (V 2.2 and above) — Used with the **Block** action, blocks an IP (source or destination) that triggers the filter. See [“Configure a Quarantine Action Set” on page 174](#) for instructions.
  - **Permit** — Select to permit traffic
  - **Rate Limit** — Select to limit the traffic rate and enter an amount for the bandwidth. See [Rate-Limiting](#). Select a rate for the rate limit setting.
4. In the **Notify** section, select notification contacts:
  - To add an email notification contact, click **Add** in the **Email Notification Contacts** area.
  - To add a SNMP notification contact, click **Add** in the **SNMP Notification Contacts** area.

You can select entries to add or click **Create** to create new notification contacts. See [“Create an Email Notification Contact” on page 179](#) for more information.
  - Select **Management Console** to have the SMS receive an alert.
5. To begin a SMS Quarantine action in the action set, in the **SMS Actions** section:
  - Select the **SMS Quarantine** check box.
  - Choose the Quarantine policy from the drop-down list that is be tied to this action set as an action.
6. In the **Log** section, make further log selections:
  - Select **Remote Syslog** to enable the remote syslog for the action set. The syslog server that is defined on the device is the syslog server that will be used.
  - Select Packet Trace to enable the packet trace for the action set.
  - For the enabled packet trace, select a **Length** size and value of bytes. Sizes include **Full** and **Partial**.
  - Select the **Priority**: **High**, **Medium**, or **Low**.
7. Click **OK**.

### How To: Configure a Quarantine Action Set

1. For the **Block** action, select the **Quarantine** check box. Click **Configure Quarantine**. The **Filters - Action Set - Configure Quarantine Response** dialog box displays.

Figure 6 - 7: Filters - Action Set - Configure Quarantine Response Dialog Box

2. To configure the quarantine response to future web requests, select one of the following: **Block**, **Redirect to a web server**, or **Display quarantine web page**.
  - Selecting **Block**, web requests are blocked entirely.
  - Selecting redirection, enter a web server address. Any web requests are redirected to the URL specified.
  - Selecting display, the quarantined web page displays according to the options you select. You can select to display the filter triggering the quarantine and its description.



You can also select to display an entered HTML message for the incident. The maximum number of characters is 1500. You can include HTML code in this field.



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

3. For non-HTTP **Other Traffic**, choose an action: **Block** or **Permit**.
4. To limit the quarantine actions to a specific IP addresses, do the following:
  - Select the **Restrictions** tab and click **New**.
  - Enter a **Name**.
  - Enter a **Source Address** and select the type: CIDR, IP Mask, or Any IP.
  - Click **Ok**. Repeat to add multiple IP addresses.
5. To perform the quarantine actions without affecting specific IP addresses, do the following:
  - Select the **Exceptions** tab and click **New**.
  - Enter a **Name**.
  - Enter a **Source Address** and select the type: CIDR, IP Mask, or Any IP.
  - Click **Ok**. Repeat to add multiple IP addresses.
6. To allow quarantined clients access to other specific hosts while they are quarantined, do the following:
  - Click the Quarantined Access tab and click **New**.
  - Enter a **Name**.
  - Enter a **Source Address** and select the type: CIDR, IP Mask, or Any IP.
  - Click **Ok**. Repeat to add multiple IP addresses.
7. Complete the action set and click **Save**.

### Rate-Limiting

A rate limiting 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. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both “Echo Requests” and “Redirect Undefined Codes” filters share the 10 Mbps “pipe” as opposed to each filter getting a dedicated 10Mbps pipe.

The supported rates are subject to restrictions according to the device model. Any of these listed rates can be used as long as it does not exceed 25% percent of the total bandwidth of the product.

The following table details the models and their supported rates.

Table 6 - 6: Rate Limit Rates per Model

IPS Model	Supported Rates (listed in Kbps)	Supported Rates (listed in Mbps)
50	50, 100, 150, 200, 300, 400, 500, 600, 700, 900	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40
100E	50, 100, 150, 200, 300, 400, 500, 600, 700, 900	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83
200/ 200E	100, 150, 200, 300, 400, 500, 600, 700, 900	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83
400	200, 300, 400, 500, 600, 700, 900	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83, 125, 200
1200/ 1200E	700, 800, 900	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83, 125, 200, 250, 320, 500
2400/ 2400E	--	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83, 125, 200, 250, 320, 500, 1000
5000E	--	1, 1.5, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 25, 30, 35, 40, 50, 62, 83, 125, 200, 250, 320, 500, 1000



**Note** The rates are not implemented exactly according to rate—higher rates are less precise. For example, on a 5000E device, the observed rate on a 125Mbps limiter will be closer to 130Mbps.

## Notification Contacts Tab

Alerts are messages that are sent to a specific recipient (either human or machine) when traffic flowing through the IPS triggers a filter that requires notification. [Alert Aggregation](#) 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 interested parties or *contacts* about matching traffic. Contacts include the *management console*, which encompasses both the SMS and LSM, e-mail addresses, SNMP servers, and the remote syslog. The management console is a predefined contact. All e-mail 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 e-mail 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, an operator may want to be notified about all UDP flood commands that have occurred within a five-minute period.



**Note** The TippingPoint limits the number of e-mail alerts sent in a minute. This feature supplements the currently used aggregation functionality in the TippingPoint. The system by default allows the sending of ten (10) e-mail 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. E-mail alerts beyond the limit in a minute are blocked. After one minute, the system resumes sending e-mail alerts. If any e-mail 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 an Email Notification Contact](#) for more information.



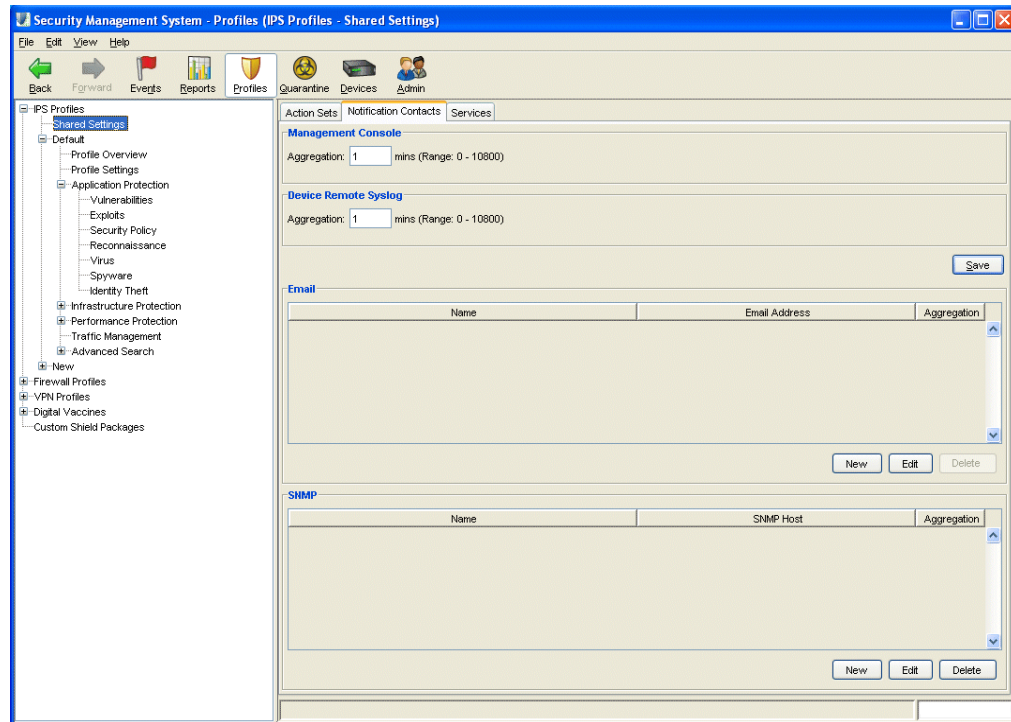
**CAUTION** Only use remote syslog on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. Therefore, you should not use remote syslog unless you can be sure that syslog messages 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 following is the **Shared Settings - Notification Contacts** screen:

**Figure 6 - 8: Shared Settings - Notification Contacts Screen**



The **Shared Settings - Notification Contacts** page displays the following information:

**Table 6 - 7: Notification Contacts Details**

Column	Description
Management Console Aggregation	The amount of minutes (from 0 to 10,800) between messages sent to the Management Console
Device Remote Syslog Aggregation	The amount of minutes (from 0 to 10,800) between messages sent to the Remote Syslog
Name	The name of the notification contact
Email Address	The email address for the notification contact

You can perform the following tasks:

- [“Set Aggregation Settings” on page 179](#)
- [“Create an Email Notification Contact” on page 179](#)
- [“Edit an Email Notification Contact” on page 179](#)
- [“Create a SNMP Notification Contact” on page 180](#)
- [“Edit an SNMP Notification Contact” on page 180](#)

For information on associating a notification contact to an action set, see [“Action Sets Tab” on page 167](#).

### How To: Set Aggregation Settings

1. From the Navigation pane, expand IPS Profiles and select **Shared Settings**.
2. Select the **Notification Contacts** tab.
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**.

### How To: Create an Email Notification Contact

1. From the Navigation pane, expand IPS Profiles and select **Shared Settings**.
2. Select the **Notification Contacts** tab.
3. From the **Email** area, do one of the following:
  - Click **New**.
  - On the Menu Bar, select the **File** —> **New** —> **Email Contact** menu item.
  - Right-click an entry and click **New**.

The **Filters - Notification Contacts - Edit** dialog box displays.

4. Enter the **Name** of the contact.
5. Enter the **Email Address** of the contact, such as bob@mail.com. The limit is 36 characters for email addresses.
6. Enter the amount of **Aggregation** in minutes.
7. Click **OK**.

### How To: Edit an Email Notification Contact

1. From the Navigation pane, expand IPS Profiles and select **Shared Settings**.
2. Select the **Notification Contacts** tab.

3. Select an email notification contact and do one of the following:
  - Click **Edit**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.
  - Right-click an entry and click **Details**.

The **Filters - Notification Contacts - Edit** dialog box displays.

4. Modify the **Name** of the contact.
5. Modify the **Email Address** of the contact, such as bob@mail.com.
6. Modify the amount of **Aggregation** in minutes.
7. Click **OK**.

### How To: Create a SNMP Notification Contact

1. From the Navigation pane, expand IPS Profiles and select **Shared Settings**.
2. Select the **Notification Contacts** tab.
3. From the **SNMP** area, do one of the following:
  - Click **New**.
  - On the Menu Bar, select the **File** —> **New** —> **SNMP Contact** menu item.
  - Right-click an entry and click **New**.

The **Filters - Notification Contacts - Edit** dialog box displays.

4. Enter the **Name** for the contact.
5. Enter the **SNMP Host Address** and **SNMP Port** (generally 162) for the contact.
6. Enter the amount of **Aggregation** in minutes.
7. Click **OK**.

### How To: Edit an SNMP Notification Contact

1. From the Navigation pane, expand IPS Profiles and select **Shared Settings**.
2. Select the **Notification Contacts** tab.
3. Select an SNMP notification contact and do one of the following:
  - Click **Edit**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.
  - Right-click an entry and click **Details**.

The **Filters - Notification Contacts - Edit** dialog box displays.

4. Modify the **Name** for the contact.
5. Modify the **SNMP Host Address** and **SNMP Port** for the contact.
6. Modify the amount of **Aggregation** in minutes.
7. Click **OK**.

## Alert Aggregation

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 also [“Set Aggregation Settings” on page 179](#).

## Aggregation Period

Alert notification is controlled by the aggregation period that you configure when you [Create an Email Notification Contact](#). 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.

## How To: Set Aggregation Settings

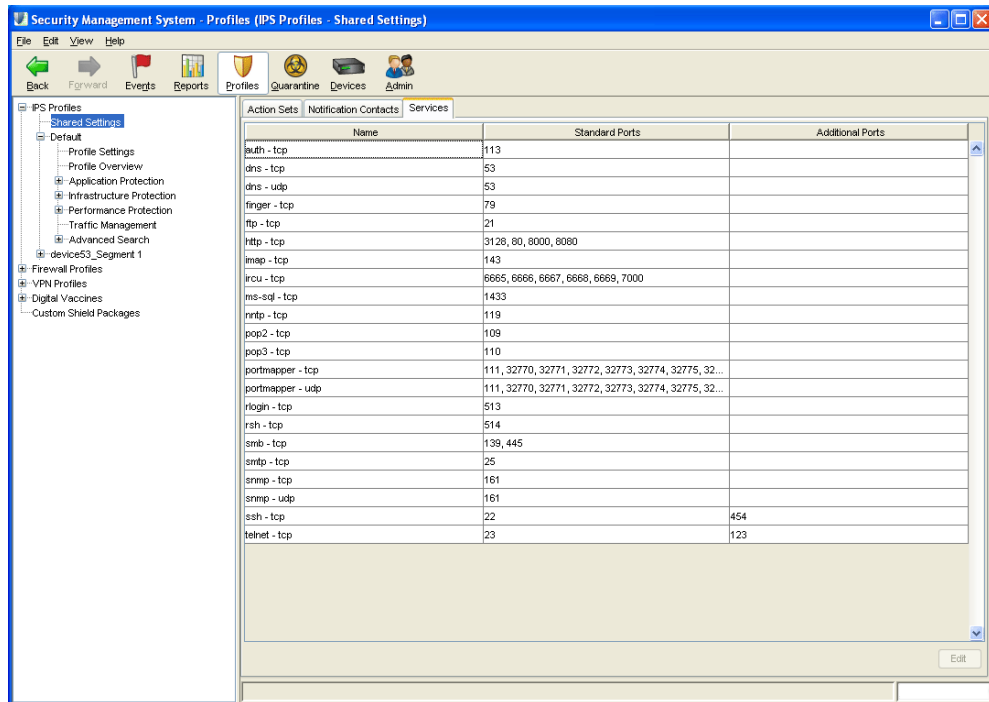
1. On the **Shared Settings - Notification Contacts** screen, locate the top options for aggregation.
2. For the **Management Console**, enter an aggregation setting in minutes.
3. For the **Device Remote Syslog**, enter an aggregation setting in minutes.
4. Click **Apply**.

## 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 following is the **Shared Settings - Services** screen:

Figure 6 - 9: Shared Settings - Services Screen



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

Table 6 - 8: Services Details

Column	Description
Name	Name of the service or protocol
Standard Ports	List of standard, supported ports
Additional Ports	List of added additional ports, non-standard for the service or protocol

You can perform the following tasks:

- [“Add a Non-Standard Port” on page 183](#)
- [“Delete a Non-Standard Port” on page 183](#)



### How To: Add a Non-Standard Port

1. Select **Shared Settings** in the Navigation pane. Select the **Services** tab.
2. Select a service name and click **Edit**. The **Filters - Service - Edit** dialog box displays.
3. Click **Add**. Each service supports 16 additional ports.
4. Enter a **Port** number.
5. Click **Save**.
6. Click **OK**.

### How To: Delete a Non-Standard Port

1. Select **Shared Settings** in the Navigation pane. Select the **Services** tab.
2. Select a service name and click **Edit**. The **Filters - Service - Edit** dialog box displays.
3. Select a port to delete. Click **Delete**.
4. Click **OK**.

## Profile Overview

The Profile Overview screen provides a convenient location to view profile information for a specific IPS profile. From this screen you can also take a snapshot and distribute the specific IPS profile.

The tabbed format presents information regarding the following items:

- Category Settings
- Filters
- Profile Settings
- Shared Settings

## Profile Settings

This sections contains the following topics:


- [Attack Filter Restrictions/Exceptions Tab](#) — Limits filter monitoring to IP addresses entered on the Shared Settings screen. You can create restrictions for attack traffic.
- [Performance Protection Restrictions Tab](#) — Limits Performance Protection filter monitoring to IP addresses that are specified.

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.

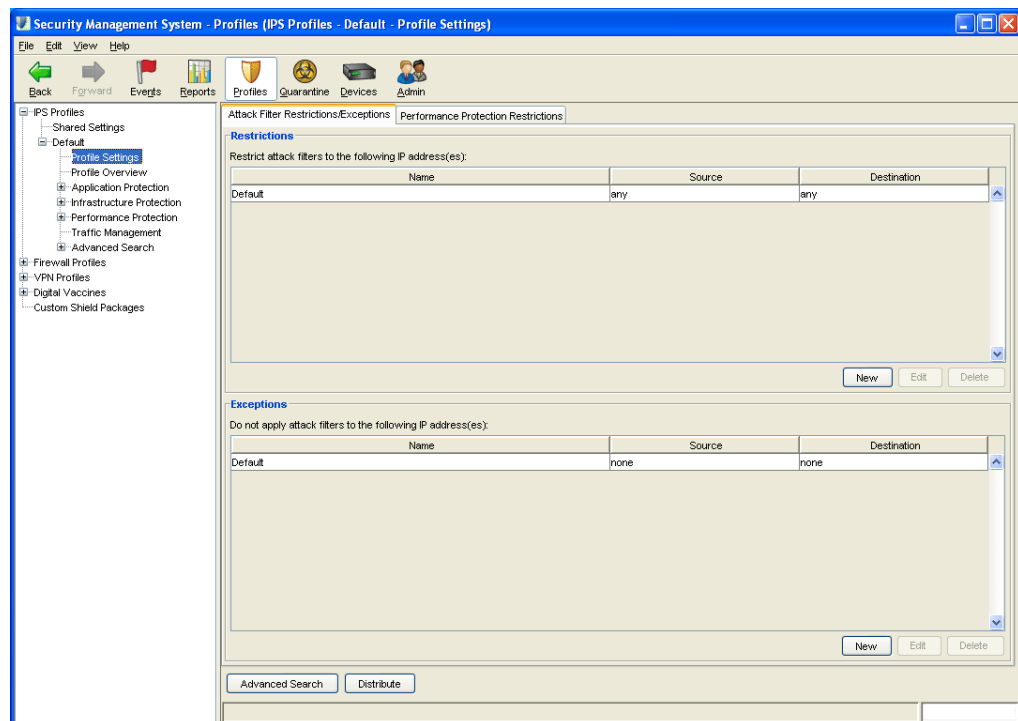
 **Note** When you distribute a profile, all profile settings are also distributed. To distribute profile settings, distribute a profile.

## Attack Filter Restrictions/Exceptions Tab

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 **Profile Setting** 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.

Figure 6 - 10: Profile Settings - Attack Filter Restrictions/Exceptions Tab



You can perform the following tasks:

- [“Create an Attack Filter Profile Restriction” on page 185](#)
- [“Edit an Attack Filter Profile Restriction” on page 185](#)
- [“Delete an Attack Filter Profile Restriction” on page 186](#)
- [“Edit an Attack Filter Profile Exception” on page 186](#)
- [“Delete an Attack Filter Exception” on page 187](#)
- [“Search/View a Filter” on page 191](#)

### How To: Create an Attack Filter Profile Restriction

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Restrictions** table, click **New**.  
The **Profile Settings - Edit** dialog box displays.
3. Enter a **Name** for the restriction.
4. For the **Source**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

### How To: Edit an Attack Filter Profile Restriction

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Restrictions** table, select a restriction. Click **Edit**.  
The **Profile Settings - Edit** dialog box displays.
3. Modify the **Name** for the restriction.
4. For the **Source**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

### How To: Delete an Attack Filter Profile Restriction

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Restrictions** table, select a restriction. Click **Edit**.
3. Click **Delete**.

### How To: Create an Attack Filter Profile Exception

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Exceptions** table, click **New**.  
The **Profile Settings - Edit** dialog box displays.
3. Enter a **Name** for the restriction.
4. For the **Source**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

### How To: Edit an Attack Filter Profile Exception

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Exceptions** table, select an exception. Click **Edit**.  
The **Profile Settings - Edit** dialog box displays.
3. Modify the **Name** for the restriction.
4. For the **Source**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

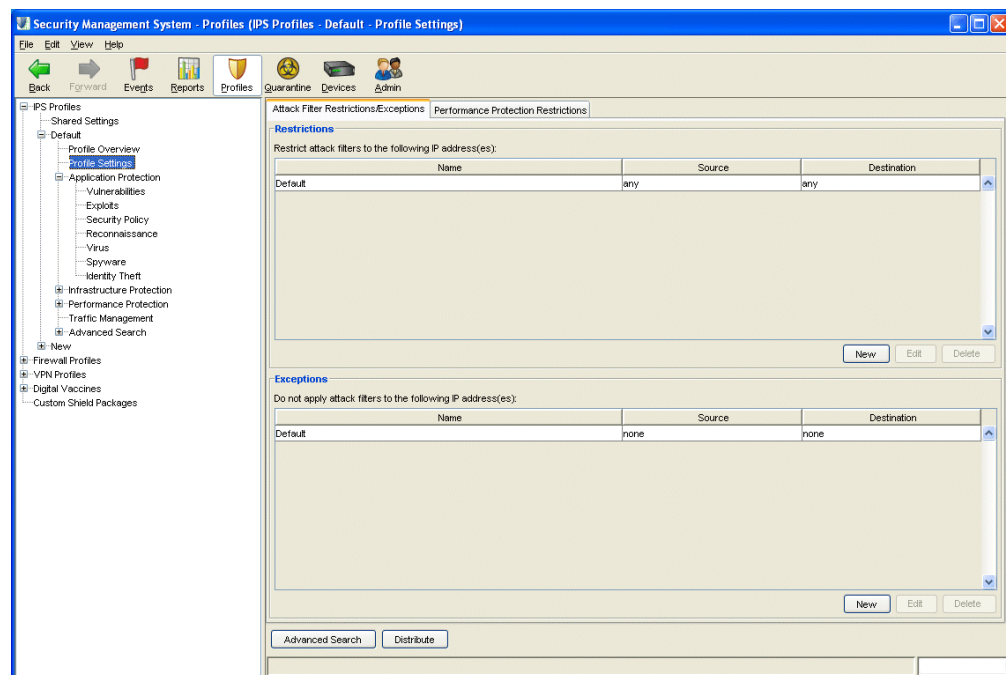
## How To: Delete an Attack Filter Exception

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays.
2. In the **Exceptions** table, select an exception.
3. Click **Delete**.

## Performance Protection Restrictions Tab

At times, you may need to have these filters focus on a specific set of IP addresses according to the needs of your network. To restrict all Performance Protection filters to run against specific IP addresses, you create a restriction. Profile restrictions created affect all Performance Protection filters. Custom settings for a filter override profile restrictions.

Figure 6 - 11: Profile Settings - Performance Protection Restrictions Tab



You can perform the following tasks:

- [“Create a Profile Performance Protection Restrictions” on page 188](#)
- [“Edit Global Performance Protection Restrictions” on page 188](#)
- [“Delete Global Performance Protection Restriction” on page 188](#)
- [“Search/View a Filter” on page 191](#)

### How To: Create a Profile Performance Protection Restrictions

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays. Select the **Performance Protection Restrictions** tab.
2. Click **New**.  
The **Profile Settings - Misuse & Abuse Restrictions - New** dialog box displays.
3. Enter a **Name** for the restriction.
4. For the **Source**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, enter an IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

### How To: Edit Global Performance Protection Restrictions

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays. Select the **Performance Protection Restrictions** tab.
2. Select a restriction. Click **Edit**.  
The **Profile Settings - Misuse & Abuse Restrictions - Edit** dialog box displays.
3. Modify the **Name** for the restriction.
4. For the **Source**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.



**Note** For examples and information on these formats, see [“IP Address Formats” on page 196](#).

5. For the **Destination**, modify the IP address and select the format. Formats include **CIDR**, **IP Mask**, and **Any IP**.
6. Click **OK**.

### How To: Delete Global Performance Protection Restriction

1. On the **Profiles** navigation pane, click **Profile Settings** for a profile. The **Profile Settings** screen displays. Select the **Performance Protection Restrictions** tab.
2. Select a restriction.
3. Click **Delete**.

## IPS Profile Filters

This section includes the following topics:

- [“Adaptive Filtering” on page 190](#)
- [“Searching for Filters” on page 190](#)
- [“Edit Multiple Filters” on page 194](#)
- [“Editing Filters” on page 195](#)
- [“Severity Level” on page 195](#)
- [“IP Address Formats” on page 196](#)

Profiles provide a management facility for packaging and distributing filters to your devices. Filters provide information and instructions for the devices protecting your network against malicious attacks. These filters enable your devices to monitor and respond to network traffic according to a particular pillar, or type. These pillars separate filters into types that apply to different attacks and sections of your network. You can create, modify, and manage these filters to block and protect against malicious attacks and piracy of your bandwidth and network services. Each filter consists of customizable options and settings that detail how the system should monitor, investigate, process, and block traffic.

If the system identifies traffic that matches a filter, it responds to that traffic based on the instructions defined in the filter’s action set. All action sets require a flow control action—the system could block, permit, or a react in a combination of ways to the traffic. As an added measure of safety and information dissemination, you can configure alerts to inform interested parties about detection and responses to malicious attacks and usage by notifying the SMS and LSM management consoles or sending emails to specified email addresses. You can also log information about matching traffic to a packet trace log or a remote syslog server for review and reporting.

All filters are assigned to protect a segment on your system. When you change the settings of these filters, only the target distribution segments receives the changes. You can also create Segment Groups to configure filter settings to a grouping of selected segments.



**Note** When a TippingPoint device is added to the SMS, any unused virtual ports (those that are not in a virtual segment in a profile) are deleted by the SMS. In order to keep any such virtual ports, put them into a virtual segment as SMS valid combinations before adding the TippingPoint device.

Filters are the key to protection and prevention of malicious invasion on your network. The SMS includes the following sets of filters categories:

- [“Application Protection” on page 196](#) — Defend against exploits targeting applications and operating systems. These filters include a variety of vulnerability and security policy filters.
- [“Infrastructure Protection Filters” on page 208](#) — Protect network bandwidth and network infrastructure elements such as routers and firewalls from attack, DDoS (Distributed Denial of Service) protection is also under this grouping and is for use with E-Series IPS devices.
- [“Performance Protection Filters” on page 226](#) — Allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of

high congestion. types of filters in this group include Peer-to-Peer, Instant Messaging, and Streaming Media.

- [“Traffic Management Filters” on page 230](#) — React to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values.



**Note** To create or edit filters and related objects, you must have Super User or Administrator authority. To view information about filters, you must have Operator authority. For more information about user authority, see [“Administration” on page 431](#).

You can perform similar actions on filters regardless of the type of filter. The following sections detail common instructions for managing filters:

- [“Searching for Filters” on page 190](#) — Details how to search for and view a filter. The section details how to perform keyword and advanced searches.
- [“Edit Multiple Filters” on page 194](#) — Details how to edit multiple filters.

## Adaptive Filtering

On rare occurrences, the system may experience extreme load conditions that may cause the device to enter a High Availability (HA) state. This state will maintain traffic inspection and processing, but can be slower due to traffic congestion. To prevent the device from entering this HA state, the TippingPoint disables filters causing the possible congestion. This functionality is called adaptive filtering, which automatically manages your devices under extreme load conditions. The SMS lists any filters for each device that consume excessive resources and which are disabled. These filters are listed in the Events area under Device Configuration.

Most filters provide configuration settings for adaptive filtering. If you do not want a filter to be subject to adaptive filtering, you can edit the filter and disable Adaptive Filtering. You can also modify the device-wide adaptive filter configuration for a device using Device Configuration. The Adaptive Filter Configuration (AFC) is under the AFC section of the Device Configuration. See [“AFC Settings” on page 380](#).

If a filter is disabled on a device due to adaptive filtering, the current state of the filter is displayed on the Events tree node on the device configuration for each device.

## Searching for Filters

The SMS provides two methods for searching for filters: searching through the filter screens and Advanced Search. On each filter screen, you can enter keywords to search filter names in that category. 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. When you search for filters, you can only search on the displayed page.

To perform advanced searches, you click the **Advanced Search** button on a filter screen or the option in the Navigation pane of the selected profile. Advanced Search enables 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 **Advanced Search** screen, you can select filter results to edit the filter, create an exception, or distribute the filter. Displayed results include the state, name, control, action set, category, and severity of the filter.



You can perform the following tasks:

- [“Search/View a Filter” on page 191](#)
- [“Perform an Advanced Search” on page 192](#)
- [“Edit Multiple Filters” on page 194](#)

### How To: Search/View a Filter

1. On the appropriate profile screen, click **Find**. The **Find in View** dialog box displays.
2. Enter the name of a filter in the **Find in View** dialog box.



**Note** The SMS searches the names of the filters displayed on the screen. To perform an advanced search, click **Advanced Search**. See [“Perform an Advanced Search” on page 192](#).

3. Click **Find**. The results display in the appropriate profile screen.
4. Select a filter. To view, do one of the following:
  - Click **Edit**.
  - Double-click the filter.

The appropriate **Edit Filter** screen displays. The screen displays the **Main** tab by default. This tab allows you to create customized filter behavior and define specific exceptions for the filter. This screen may differ depending on the type of filter accessed.

Figure 6 - 12: Filter Edits/Details Screen (Main tab)

**Filters - Edit Filter**

Name: 0081: ICMP: Unassigned Type (Type 1)  
 Profile: huidefault  
 Category: Vulnerabilities  
 Severity: Major

Main | Details

**Settings**

Use Category Settings  
 Use Filter Specific Settings

State:  Enabled  
 Action: Permit + Notify

**Adaptive Filter Configuration State**

Use adaptive configuration settings  
 Do not apply adaptive configuration settings to this Filter

**Exceptions**

Name	Source	Dest

Create Edit Delete

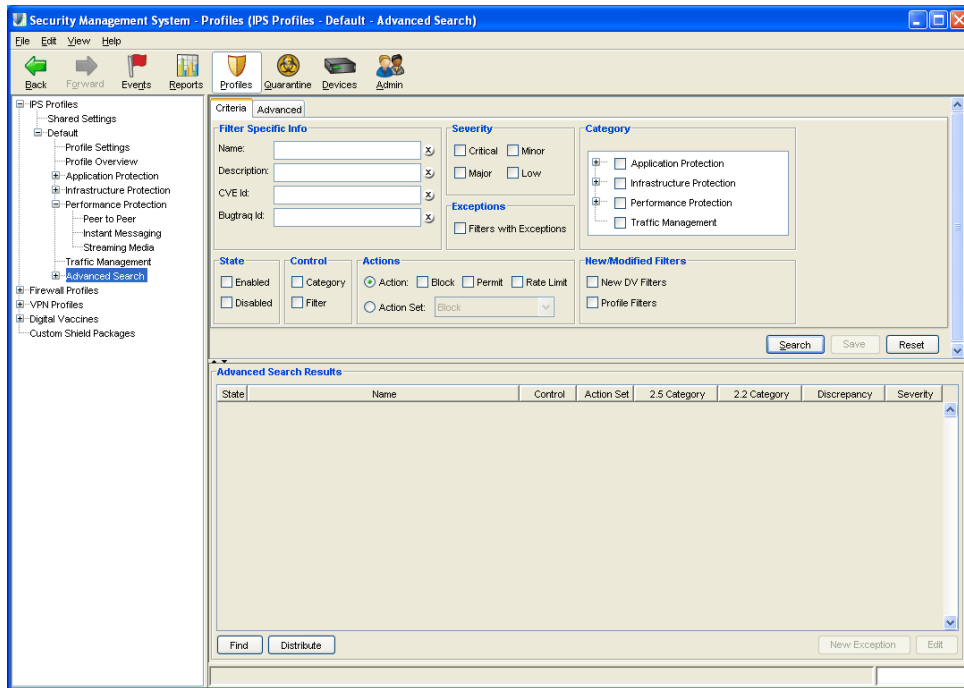
OK Distribute Cancel

5. Click the **Details** tab. This tab displays the description for the filter. This screen may differ depending on the type of filter accessed.
6. Click **OK** or **Cancel** to close.

**How To: Perform an Advanced Search**

1. On the appropriate profile screen, click **Advanced Search**. The **Profiles - Advanced Search** screen displays.

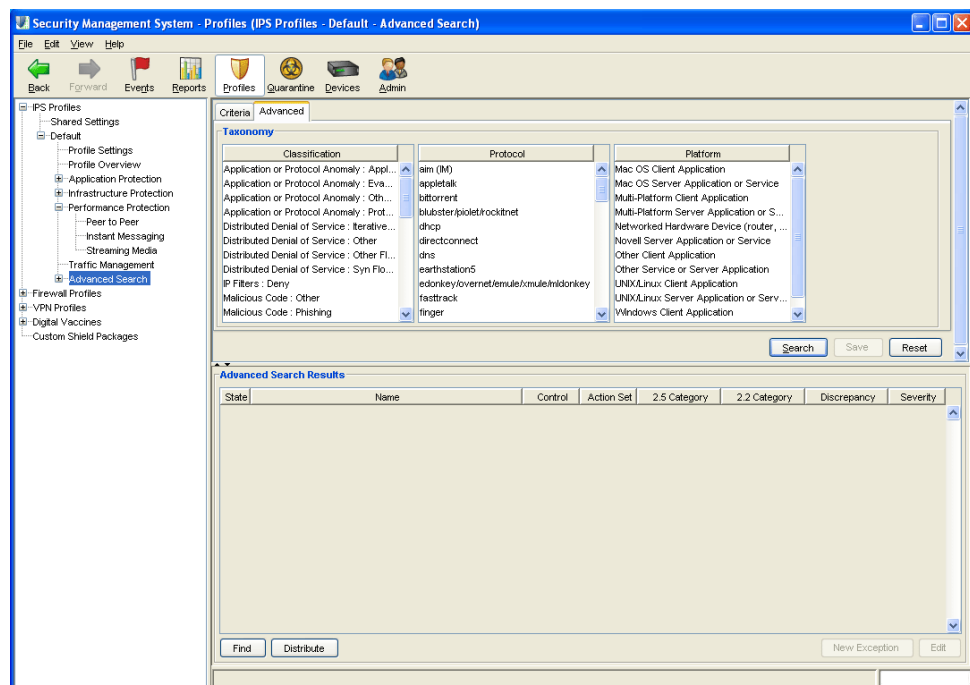
Figure 6 - 13: Profiles - Advanced Search - Criteria Screen



2. Select the **Criteria** tab.
3. In the **Filter Specific Info** section, enter the following:
  - **Name**
  - **Description**
  - **CVE Id**
  - **Bugtraq Id**
4. Select the **Severity**:
  - **Critical**
  - **Major**
  - **Minor**
  - **Low**

5. Select **User Settings**:
  - **State** — Select Enabled and/or Disabled for the state
  - **Control** — Select Category and/or Filter
 You can select also by Action or Action Set:
  - **Action** — Select Block, Permit, and/or Rate-Limit (cannot search by action and action set)
  - **Action Set** — Select a listed Action Set (cannot search by action and action set)
6. In the **Category** section, expand the appropriate category or categories:
  - **Application Protection**
  - **Infrastructure Protection**
  - **Performance Protection**
7. Select a main category, such as Application Protection, to search on all items in that category or select individual items in one or more main categories  
For more information on categories, see [“IPS Profiles” on page 150](#).
8. To search **Modified Filters**, check the following options:
  - New DV Filters — Searches the filters added from a Digital Vaccine update
  - Profile Filters — Searches the filters modified in the current profile
9. To enhance your search, you can select additional criteria by clicking the Advanced tab.

Figure 6 - 14: Profiles - Advanced Search - Advanced Screen



10. Select a **Classification**, such as SYN Flood Attack or Worm. You can use the **Shift** and **Ctrl** keys to select multiple entries.
11. Select a **Protocol**, such as AIM (IM) or BitTorrent. You can use the **Shift** and **Ctrl** keys to select multiple entries.
12. Select a **Platform**, such as MAC OS Client Application or Windows Client Application. You can use the **Shift** and **Ctrl** keys to select multiple entries.
13. Select **Search**. To reset the Advanced Search screen, click **Reset**. Results display in the **Advanced Search Results** list pane.

### How To: Edit Multiple Filters

When viewing a list of filters, you can select multiple filters to edit. When editing multiple filters, you can only modify the assigned Action Set. Specific settings per filter require editing each filter separately.

To select and edit multiple filters

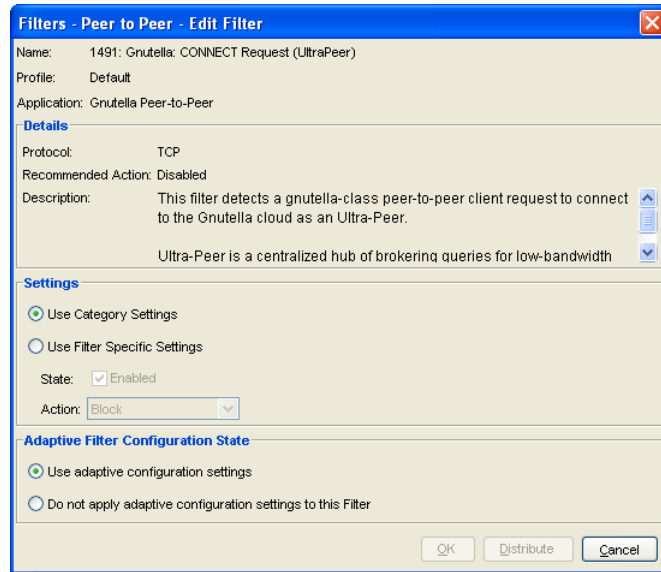
1. Hold down the Shift key while selecting filters and then:
  - Click the **Edit** button, right click and select **Edit**.

Or

  - Select **Edit** —> **Details** from the menu options.
2. On the appropriate filter screen, locate and select multiple filters (hold down the Shift key while selecting).
3. To edit, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Right-click the selected filter and choose **Edit**.

The **Filter - Change Action Set** dialog box displays.

Figure 6 - 15: Filter - Change Action Set Dialog Box (Multi-Edit)



4. To set the filters to the category settings, select **Use Category Settings**.
5. To enter specific action sets settings, do the following:
  - Click **Use Filter Specific Settings**.
  - For **State**, click the **Enabled** check box. If you do not click this check box, the filter is disabled
  - From the **Action** drop-down menu, select an action set.
6. Click **OK**.

## Editing Filters

The dialog box for editing filters opens a page for modifying the settings, parameters, action sets, and exceptions for filters. Depending on the type, each filter has a different set of editing options. To review the specific editing instructions for your filter, review the following:

- [Edit an Application Protection Filter](#)
- [Edit a DDoS Filter](#)
- [Edit a Network Equipment Filter](#)
- [Edit a Traffic Normalization Filter](#)
- [Create/Edit a Traffic Management Filter](#)
- [Edit a Performance Protection Filter](#)

## Severity Level

Filters are assigned a severity level which indicates the severity of the potential attack traffic. Severities are color-coded allowing you to quickly identify and respond appropriately to attack traffic.

The following severity levels exist:

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

## IP Address Formats

The IP addresses required in the SMS application may have varying formats. The optional formats include the following:

- **CIDR** — requires the *n.n.n.n/n* format; see the following paragraph for details.
- **IP Mask** — requires an IP address followed by a subnet in the format *n<sub>1</sub>.n<sub>1</sub>.n<sub>1</sub>.n<sub>1</sub> n<sub>2</sub>.n<sub>2</sub>.n<sub>2</sub>.n<sub>2</sub>*
- **Any IP** — specifies that the exception applies to all addresses; fills the Address field with the value **0.0.0.0/0**.

By default, the **Source** and **Destination Address** fields use the Classless Inter-Domain Routing (CIDR) format. The CIDR format is similar to an IP address except that it is followed by a slash (/) and a specified number of bits. The number of bits indicates the significant bits in the address. In the following example, the IP source address of a packet must match all 32 bits of the IP address specified:

10.3.4.5/32

## Application Protection

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's 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 Tab” on page 167](#) for more information.

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.

These filters include the following:

- [Exploit Filters](#) — Category of filters that protect against known exploits of software components.
- [Identity Theft Filters](#) — Category of filters that protect against viruses and similar malware that gathers information to compromise personal accounts.
- [Identity Theft involves various methods of obtaining key pieces of data related to personal or financial information and using that information to gain goods and services.](#) [Informational Filters](#) — Category of filters that are classically used for IDS testing (e.g. Blade signatures) These filters are used for devices. This category will only be valid for profiles associated with devices running previous TippingPoint software versions. It has been removed from V 2.5 TippingPoint devices.
- [Advanced Search — Search for a filter with advanced criteria options](#) — Category of filters that detect and block reconnaissance scans of your network.
- [Security Policy Filters](#) — Category of filters that require deployment knowledge and/or operational policy.
- [Spyware Filters](#) — Category of filters that protect against attempts by spyware software to obtain information.
- [Virus Filters](#) — Category of filters that protect against known viruses.
- [Vulnerabilities Filters](#) — Category of filters that protect potentially vulnerable software of the network such as operating systems.

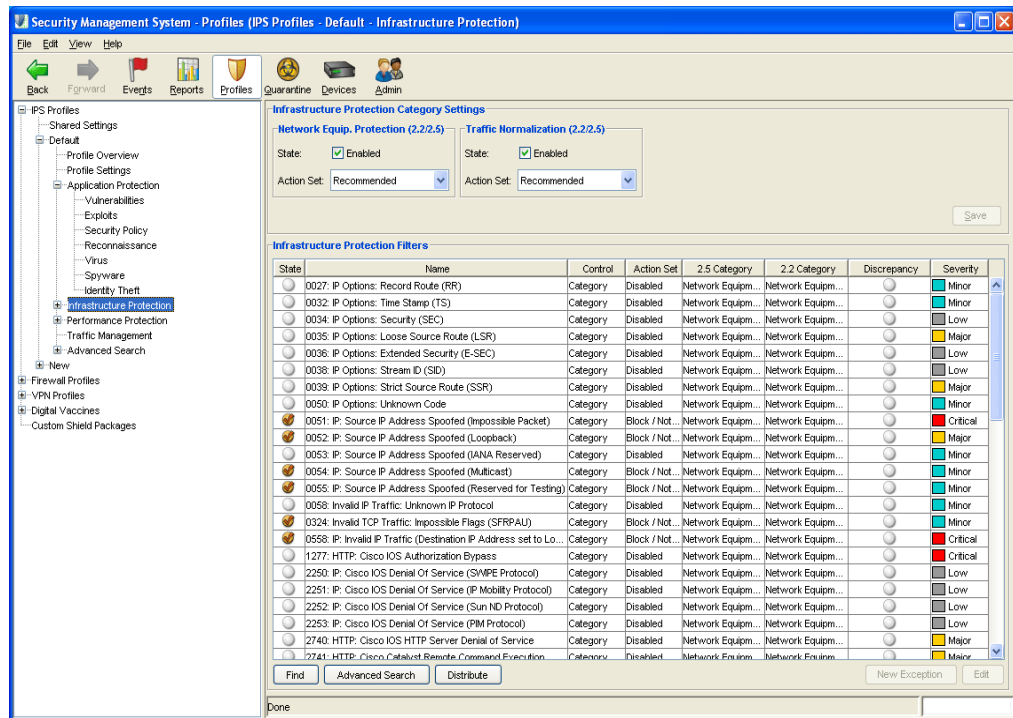


**Note** To enable these filters, see [“Editing Application Protection Category Settings” on page 200.](#)

You can view filters of each type or all Application Protection filters through the **IPS Profiles - Application Protection** screen.

The following is the **IPS Profiles - Application Protection** screen:

Figure 6 - 16: IPS Profiles - Application Protection



**Note** Some filters only apply to previous versions of the software. Some filters only apply to current versions of the software. The List Pane indicates what Filters are available to current and previous application versions. The 2.2 Category heading applies to all release of 2.2 and earlier.



These filters have the following settings:

**Table 6 - 9: IPS Profiles - Application Protection Screen Information**

Column	Definition
State	Indicates if the filter is currently enabled, disabled, or invalid.
Name	Name of the filter. Click on the filter name link to view and configure filter details.
Control	Location of where the action set is defined for the attack filter.
Action Set	The action set that is performed when the filter is triggered.
2.5 Category	Category that the filter is in for release 2.5
2.2 Category	Category that the filter was previously in for release 2.2 and earlier f
Discrepancy	Indicates if there is a difference in settings between V 2.2 and V 2.5 configurations
Severity	Indicates the potential consequences of the traffic that matches the filter. See <a href="#">“Severity Level” on page 195.</a>



**Note** To modify Application Protection category settings, see [“Editing Application Protection Category Settings” on page 200.](#)



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543.](#)

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

- **Copy** — copy selected rows or cell value
- **Edit** — Edit a selected filter
- **New Exception** — Create a new exception
- **View Action Set** — Display the action set for the filter
- **What is Discrepancy** — Provides information about handling differences in filter behavior due to different IPS versions
- **View Related Events** — Display any events relating to the filter
- **Find** — Search for a filter
- **Advanced Search** — Search for a filter with advanced criteria options

You can perform the following tasks for all Application Protection filters:

- [“Editing Application Protection Category Settings” on page 200](#)
- [“Edit an Application Protection Filter” on page 200](#)
- [“Create Filter Exception” on page 203](#)
- [“Delete Filter Exception” on page 204](#)
- [“Search/View a Filter” on page 191](#)

## Editing Application Protection Category Settings

On the **Application Protection** screen, the **Application Protection Category Settings** section allows you to set filter category settings.



**Note** When you select settings in this section, you globally change the category settings for all filters of that type.

### How To: Edit Application Protection Category Settings

1. On the **Application Protection** screen, the **Application Protection Category Settings** section allows you to set filter category settings.
2. For each category, do the following:
  - Check the **Enabled** check box. If you the check box is not selected, the filters are disabled.
  - Select an **Action Set** for the filters.
3. After making desired changes, click **Apply**.

## Editing an Application Protection Filter

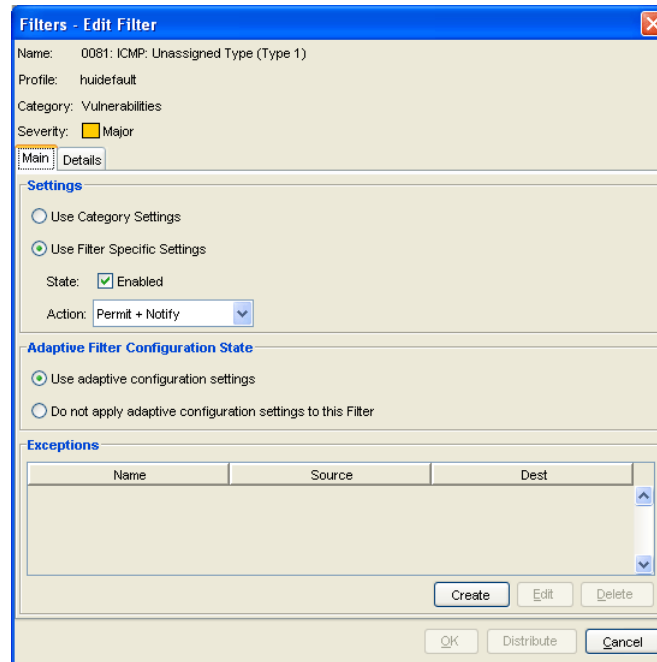
You can tune filters to meet the needs of your enterprise. You can modify a filter or add an exception to a filter. You also can alter the system's response to an attack filter by editing the action set, changing how or when contacts are notified, or even disabling the filter.

### How To: Edit an Application Protection Filter

1. On the appropriate **Application Protection** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the filter and choose **Edit**.

The appropriate **Filter Edits/Details** dialog box displays. The screen displays the **Main** tab by default. This tab allows you to create customized exceptions for the specific filter.

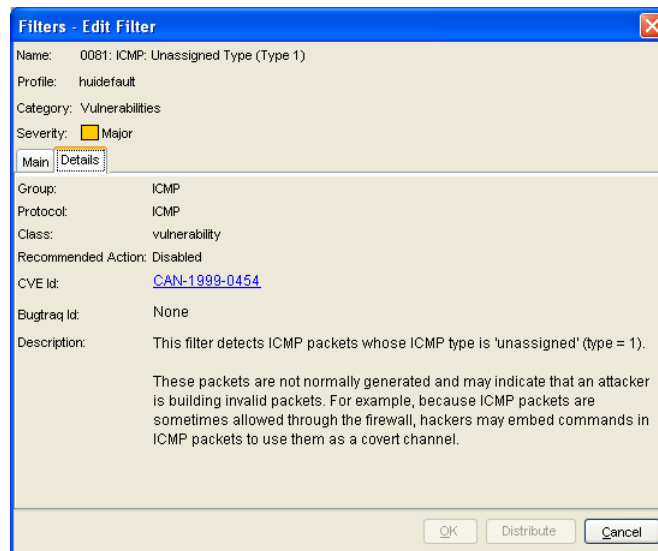
Figure 6 - 17: Action Sets Box (Main tab)



3. To enter custom category settings, do the following:
  - Click **Use Filter Specific Settings**.
  - For **State**, click the **Enabled** check box. If you do not click this check box, the filter custom settings are disabled.
  - From the **Action** drop-down menu, select an action set.
4. Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Config State** section, select one of the following:
  - **Use adaptive configuration settings** — Applies the global adaptive filter settings
  - **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter
5. To create a custom filter exception, see [“Application Protection” on page 196](#).

- Click the **Details** tab. This tab displays the description for the filter.

Figure 6 - 18: Filter Edits/Details Dialog Box (Details tab)



- Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

## 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 create 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 create an exception to a filter that protects a service that you do not know about, you may increase your network's vulnerability.

You can create an exception directly on a selected filter in the following methods:

- Clicking **New Exception** on the appropriate filter listing screen.
- Selecting the **File** —> **New** —> **Exception** menu option from the Menu Bar.
- Clicking **Create** in the **Exceptions** section of the filter editor.

You can also create exceptions that globally affect all Application Protection filters in a profile. For more information, see ‘



**Note** If you receive errors or have issues editing and saving filter exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

### How To: Create Filter Exception

1. On the appropriate screen, select a filter.
2. To create an exception, do one of the following:
  - Click **New Exception**.
  - On the Menu Bar, click **File** —> **New** —> **Exception**.
  - Edit the selected filter and click **Create** in the **Exceptions** section.
  - Right-click a selected entry and choose **New Exception**.

The **Filters - Create/Edit Exception** dialog box displays. The dialog box lists the name of the attack filter receiving the exception.
3. Optionally, enter a **Name** for the exception.
4. For the **Src Address**, enter an IP address. Select the format for the address: **CIDR**, **IP Mask**, or **Any IP**.
5. For the **Dest Address**, enter an IP address. Select the format for the address: **CIDR**, **IP Mask**, or **Any IP**.
6. Click **OK**. You can also click **Distribute** to distribute the change.



**Note** If you receive errors or have issues creating/editing and saving filter exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

### How To: Delete Filter Exception

1. On the appropriate Application Protection screen, select and open a filter.
2. In the **Exceptions** section, select an exception to delete.
3. Click **Delete**.

## Application Protection Filters

This section contains the following topics:

- [“Vulnerabilities Filters” on page 205](#)
- [“Exploit Filters” on page 205](#)
- [“Security Policy Filters” on page 205](#)
- [“Advanced Search — Search for a filter with advanced criteria options” on page 206](#)
- [“Virus Filters” on page 207](#)
- [“Spyware Filters” on page 207](#)
- [“Identity Theft Filters” on page 207](#)

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 perform the following tasks:

- [“Editing Application Protection Category Settings” on page 200](#)
- [“Edit an Application Protection Filter” on page 200](#)
- [“Create Filter Exception” on page 203](#)
- [“Delete Filter Exception” on page 204](#)
- [“Search/View a Filter” on page 191](#)

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
- Advanced Search — Search for a filter with advanced criteria options

## Vulnerabilities Filters

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.

## Exploit Filters

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.

## Security Policy Filters

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 [“Editing Application Protection Category Settings” on page 200](#).

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's 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 your environment's requirements.



**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 create an exception to a filter that protects a service that you do not know about, you may increase your network's 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

Advanced Search — Search for a filter with advanced criteria options

## Reconnaissance Filters

A Reconnaissance filter 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. Scans/Sweeps filters protect against scan attacks and possible exceeded threshold limits against your ports and hosts.s



**Note** By default, these filters include disabled filters and some set to Block/Notify. To enable these filters or modify their category settings, see [“Editing Application Protection Category Settings” on page 200](#).

## Scans/Sweeps Filters

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/Sweeps filters prevent these port scan and host sweep attacks.

These filters scans for potential scan and sweep attack against a network, constantly analyzing traffic across several sessions and packets. 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** Scans/Sweeps filters are not affected by the restrictions and exceptions 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.

## Virus Filters

A virus is an application or piece of malicious code that can infects other programs. Viruses can embed a copy of itself in programs making them Trojan Horses. When you run these infected programs, the embedded virus also runs and propagates the infection. Generally, this process is invisible to the user.

## Spyware Filters

Spyware is a type of software that transmits information without the user's knowledge or permission. Spyware may be the result of a virus infection or may be installed along with other applications. Spyware often consumes vast resources and can slow systems and, in some cases, cause systems to become unstable or unusable.

## Identity Theft Filters

Identity Theft involves various methods of obtaining key pieces of data related to personal or financial information and using that information to gain goods and services. **Informational Filters**

The SMS continues to support this category for devices running previous TippingPoint software versions. Informational filters provide a means for classic Intrusion Detection System (IDS) testing. These filters allow you to perform tests against your network security. The behavior of these filters provide detailed information as to the strength of your security. An example of these filters includes Blade signatures.



**Note** Informational filters are typically disabled by default as a Recommended Setting. To enable these filters or modify their category settings, see [“Editing Application Protection Category Settings” on page 200](#).

## Infrastructure Protection Filters

This sections contains the following topics:

- [“Advanced DDoS Filters” on page 212](#)
- [“Network Equipment Protection Filters” on page 219](#)
- [“Traffic Normalization Filters” on page 221](#)
- [“Traffic Threshold Filters” on page 223](#)

Infrastructure Protection is a set of filter categories that protect network bandwidth and network infrastructure elements such as routers and firewalls from attacks. These filters use a combination of traffic normalization, DDoS protection, and application, protocol, and statistical anomaly detection. Infrastructure Protection filters include DDoS, network equipment protection, and traffic normalization filters.

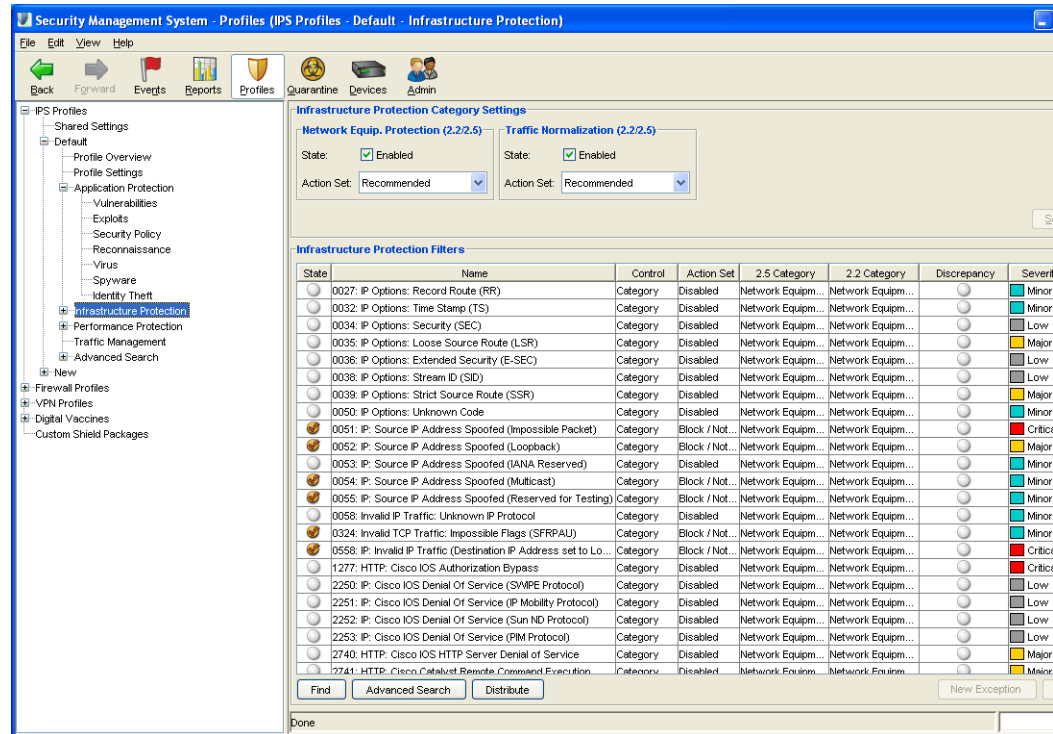
Infrastructure Protection filters include the following categories:

- [Advanced DDoS Filters](#) — Detect and block a wider range of Denial of Service attacks, including SYN, Connection Per Second (CPS), and Established Connection floods.  
**Only E-Series devices provide Advanced DDoS Protection filter creation and management, such as the TippingPoint 100E/200E/1200E/2400E/5000E. You create these filters; the SMS does not include default filters.**  
For more information on E-Series systems, contact your TippingPoint Sales Representative.
- [Network Equipment Protection Filters](#) — Detect and block exploit and anomaly based attacks against networking equipment. These filters are enabled and use the Recommended action set by default.
- [Traffic Normalization Filters](#) — Detect and manage traffic on a network. The 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*
- [Traffic Threshold Filters](#) — Detect issues in bandwidth usage. These filters enable you to perform bandwidth-shaping. You create these filters; the SMS does not include default filters.

You can view filters of each type or all Application Protection filters through the **Profiles - Infrastructure Protection** screen

The following is the **Profiles - Infrastructure Protection** screen:

Figure 6 - 19: Profiles - Infrastructure Protection Screen



These filters have the following settings:

Table 6 - 10: Profiles - Infrastructure Protection Screen Information

Column	Definition
State	Indicates if the filter is currently enabled, disabled, or invalid.
Name	Name of the filter. Click on the filter name link to view and configure filter details.
Control	Location of where the action set is defined for the attack filter.
Action Set	The action set that is performed when the filter is triggered.
2.5 Category	Category that the filter is in for release 2.5
2.2 Category	Category that the filter was previously in for release 2.2 and earlier f
Discrepancy	Indicates if there is a difference in settings between V 2.2 and V 2.5 configurations
Severity	Indicates the potential consequences of the traffic that matches the filter. See <a href="#">“Severity Level” on page 195.</a>

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

- **Copy** — copy selected rows or cell value
- **Edit** — Edit a selected filter
- **New Exception** — Create a new exception
- **View Action Set** — Display the action set for the filter
- **What is Discrepancy** — Provides information about handling differences in filter behavior due to different IPS versions
- **View Related Events** — Display any events relating to the filter
- **Find** — Search for a filter
- **Advanced Search** — Search for a filter with advanced criteria options



**Note** If you receive errors or have issues editing and saving filters and exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

You can perform the following tasks for all Infrastructure Protection filters:

- **General:**
  - [“Edit Infrastructure Protection Category Settings” on page 210](#)
  - [“Create Filter Exception” on page 211](#)
  - [“Delete Filter Exception” on page 211](#)
  -

### How To: Edit Infrastructure Protection Category Settings

The **Infrastructure Protection Category Settings** section allows you to set filter category settings.



**Note** When you select settings in this section, you globally change the category settings for all filters of that type.

1. On the **Profiles** Navigation pane, select **Profiles** —> **Infrastructure Protection**. The **Profiles - Infrastructure Protection** screen displays.
2. For DDoS filters, do the following:
  - Check the **Enabled** check box. If you the check box is not selected, the filters are disabled.
  - Select an **Action Set** for the filters.



**Note** Category Settings for DDoS filters do not affect Advanced DDoS filters.

3. For Network Equipment Protection filters, do the following:
  - Check the **Enabled** check box. If you the check box is not selected, the filters are disabled.
  - Select an **Action Set** for the filters.

4. For Traffic Normalization filters, do the following:
  - Check the **Enabled** check box. If you the check box is not selected, the filters are disabled.
  - Select an **Action Set** for the filters.
5. Click **Save**.

### How To: Create Filter Exception

You can create custom filter exceptions for Infrastructure Protection filters. When you create exceptions for a specific filter, you exclude the IP address from receiving the filter. The IP addresses you enter will not have the filter applied.



**Note** These exceptions apply only to the customized filter. The exception does not globally affect all filters. For information on global profile exceptions, see [“IPS Profiles Shared Settings” on page 166](#).

1. On the appropriate Infrastructure Protection screen, select a filter.
2. To create an exception, do one of the following:
  - Click **Create Exception**.
  - On the Menu Bar, click **File** —> **New** —> **Exception**.
  - View the selected filter and click **Create** in the **Exceptions** section.
  - Right-click the selected filter and choose **Create Exception**.

The **Profiles - Infrastructure Protection Filters - Create/Edit Exception** dialog box displays. The dialog box lists the name of the attack filter receiving the exception.

3. Enter a **Name** for the exception.
4. For the **Src Address**, enter an IP address. Select the format for the address: **CIDR**, **IP Mask**, or **Any IP**.
5. For the **Dest Address**, enter an IP address. Select the format for the address: **CIDR**, **IP Mask**, or **Any IP**.
6. Click **OK**. You can also click **Distribute** to distribute the change.



**Note** If you receive errors or have issues editing and saving filter exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

### How To: Delete Filter Exception

1. On the appropriate Infrastructure Protection screen, select and open a filter.
2. In the **Exceptions** section, select an exception to delete.
3. Click **Delete**.

## Advanced DDoS Filters

Advanced DDoS, or Advanced Distributed Denial of Service filters, enable you to create filters for detecting denial of service attacks. These filters provide protection against a wider range of attacks, including SYN floods, Established Connection floods, and Connections Per Second (CPS) floods.



**Note** Only E-Series devices offer the **Advanced DDoS Protection** filters, such as the TippingPoint 100E/200E/1200E/2400E/5000E.

For more information on purchasing E-Series systems, contact your TippingPoint Sales Representative.

The Advanced DDoS system provides the following types of protection:

- **SYN Proxy** — Protects against SYN floods of the system. An attacker floods a server with malicious connection requests (TCP SYNs) with spoofed source IP addresses, preventing 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’s settings.
- **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** — Protects 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.

When using Advanced DDoS Protection filters, you must place the IPS device in a Symmetric Network. The device must see both sides of the traffic.



**Note** Advanced DDoS Protection Filters function only in a Symmetric Network. You must disable Asymmetric Mode for your device.

Configuring Advanced DDoS filters for devices requires the following:

- **Creating and Managing Filters for 100E/200E/210E** — To create a filter for a TippingPoint 100E/200E/210E, you do the following:
  - *Set the filter parameters through the **Filter Controls** tab.*
  - *Configure the DDoS settings through the **100E/200E/210E Settings** tab.*
- **Creating and Managing Filters for 1200E/2400E/5000E** — To create filters for the TippingPoint 1200E/2400E/5000E, you do the following:
  - *Set the filter parameters through the **Filter Controls** tab.*
  - *Configure the DDoS settings through the **1200E/2400E/5000E Settings** tab.*
  - *Configure enhanced settings according to selected device through the **Devices - Adv. DDoS Configuration** screen. See [“E-Series: Advanced DDoS” on page 427](#).*

You can perform the following tasks:

- **TippingPoint 100E/200E/210E:**
  - [“Create/Edit an Advanced DDoS Filter for 100E/200E/210E Models” on page 213](#)
  - [“Create an Advanced DDoS Exception for 100E/200E/210E Models” on page 217](#)
- **TippingPoint 1200E/2400E/5000E:**
  - [“Create/Edit an Advanced DDoS Filter for 1200E/2400E/5000E Models” on page 216](#)
  - [“Create/Edit an Advanced DDoS Filter for 1200E/2400E/5000E Models” on page 216](#)

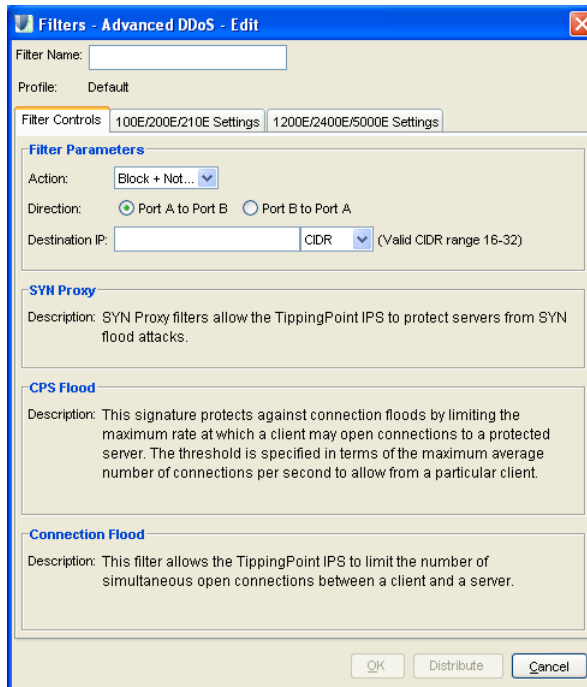
#### How To: Create/Edit an Advanced DDoS Filter for 100E/200E/210E Models

1. On the **Advanced DDoS** screen, click **New**. Or select a filter and click **Edit**.

The **Filter - Edit Filter** dialog box displays. It displays the **Filter Controls** tab by default. This tab provides information and filter parameters.

The following is the **Filter Controls** tab.

Figure 6 - 20: Filter Controls Tab



2. In the **Filter Parameters** section, do the following:
  - Select the **Action** for the filter.
  - Select a **Direction**: From Port A to Port B or From Port B to Port A.
  - Enter a **Destination IP** address and select a format from the drop-down list.



3. Select the **TippingPoint 100E/200E Settings** tab.

Figure 6 - 21: 100E/200E/210E Settings Tab

The screenshot shows the 'Filters - Advanced DDoS - Edit' window. At the top, there is a 'Filter Name' field and a 'Profile' dropdown set to 'Default'. Below this are two tabs: '100E/200E/210E Settings' (selected) and '1200E/2400E/5000E Settings'. The main area is divided into three sections: 'SYN Proxy', 'CPS Flood', and 'Connection Flood'. Each section has a 'State' checkbox (all are checked) and a 'Threshold' input field. The SYN Proxy threshold is 500, CPS Flood is 200.0, and Connection Flood is 25. Below these is an 'Exceptions' table with columns for Name, Source, and Destination. At the bottom of the dialog are 'Create', 'Edit', and 'Delete' buttons for the exceptions, and 'OK', 'Distribute', and 'Cancel' buttons for the main dialog.

4. In the **SYN Proxy** section, do the following:
  - Check the box **Enable** for **SYN Proxy**. Manually enabling this option provides traps for SYN floods, rather than using firewall blocks.
  - Enter the number of SYN requests allowed per second for the **Threshold**. The range is 1 to 10,000.
5. In the **CPS Flood** section, do the following:
  - Check the box **Enable** for **CPS Flood**.
  - Enter the number of maximum average connections allowed per second for the **Threshold**. The range is 1 to 4,096.
6. In the **Connection Flood** section, do the following:
  - Check the box **Enable** for **Connection Flood**.
  - Enter the number of allowed open connections for the **Threshold**. The range is 1 to 65,536.
7. To create an **Exception**, see [“Create an Advanced DDoS Exception for 100E/200E/210E Models” on page 217](#).

- Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

### How To: Create/Edit an Advanced DDoS Filter for 1200E/2400E/5000E Models

- On the **Advanced DDoS** screen, click **New**. Or select a filter and click **Edit**.

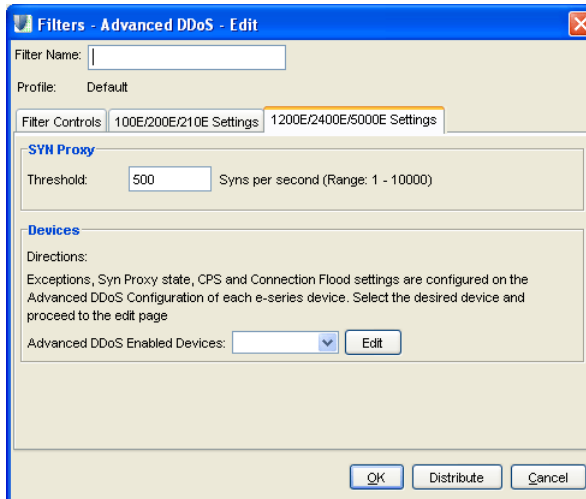
The appropriate **Filter - Advanced DDoS - Edit Filter** dialog box displays. It displays the **Filter Controls** tab by default. This tab provides information and filter parameters. The following is the **Filter Controls** tab.

Figure 6 - 22: Filter Controls Tab

- In the **Filter Parameters** section, do the following:
  - Select the **Action** for the filter.
  - Select a **Direction**: From Port A to Port B or From Port B to Port A.
  - Enter a **Destination IP** address and select a format from the drop-down list.

3. Select the **TippingPoint 1200E/2400E/5000E Settings** tab.

Figure 6 - 23: 1200E/2400E/5000E Settings



4. In the **SYN Proxy** section, enter a threshold amount of SYNs allowed per second (1 - 10,000).
5. Select a device to modify from the drop-down menu. Click Edit. The SMS redirects you to the Devices screen for the device. Further settings for DDoS are controlled there. See [“E-Series: Advanced DDoS” on page 427](#).
6. To create an **Exception**, see [“Create/Edit an Advanced DDoS Exception for 1200E/2400E/5000E Models” on page 219](#).
7. Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

#### How To: Create an Advanced DDoS Exception for 100E/200E/210E Models

1. You can create an exception when creating or editing an Advanced DDoS filter. On the **Filter - Advanced DDoS - Edit** dialog box, click the **Exceptions/Details** tab. This tab displays the description for the filter options and provides an option for creating exceptions.
2. On the **Advanced DDoS** screen, locate and select a filter.

3. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.

The **Filter - Advanced DDoS - Edit** dialog box displays. It displays the **Filter Controls** tab by default. This tab allows you to create customized category settings and exceptions for the specific filter.

4. On the **Filter - Advanced DDoS - Edit** dialog box, click the **Exceptions/Details** tab. This tab displays the description for the filter options and provides an option for creating exceptions.
5. Click **Create**. The **Filter - DDoS Create/Edit Exception** dialog box displays.
6. Enter a **Name**.
7. Enter a **Source Address** and select a format.
8. Click **OK**.

### How To: Edit an Advanced DDoS Exception for 100E/200E/210E Models

1. On the **Advanced DDoS** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.
3. +On the **Filter - Advanced DDoS - Edit** dialog box, click the **Exceptions/Details** tab. This tab displays the description for the filter options and provides an option for creating exceptions.
4. Select an exception. Click **Edit**. The **Filter - DDoS Create/Edit Exception** dialog box displays.
5. Edit the **Name**.
6. Edit the **Source Address** and select a format.
7. Click **OK**.

### How To: Delete an Advanced DDoS Exception for 100E/200E/210E Models

1. On the **Advanced DDoS** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.

The **Filter - Advanced DDoS - Edit** dialog box displays. It displays the **Filter Controls** tab by default. This tab allows you to create customized category settings and exceptions for the specific filter.

3. On the **Filter - Advanced DDoS - Edit** dialog box, click the **Exceptions/Details** tab. This tab displays the description for the filter options and provides an option for creating exceptions.
4. Select an exception.
5. Click **Delete**.

### How To: Create/Edit an Advanced DDoS Exception for 1200E/2400E/5000E Models

1. You can create and edit Advanced DDoS filters for the TippingPoint-5000E through the **Filter - Advanced DDoS - Edit** dialog box. Click the **TippingPoint5000E Settings** tab. This tab displays the description for the filter options and provides an option for creating exceptions.
2. Select a device from the drop-down menu and click **Edit**. The **Devices - Advanced DDoS** screen displays.



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

## Network Equipment Protection Filters

Network attacks can broadly or specifically seek access and data to corrupt on a network. Network equipment filters protect networked equipment from attacks that scan and search for hardware. Networked hardware receives requests and from operating systems and services on a network. This equipment includes peripherals such as printers and fax/modems as well as routers and integrated phone systems. These filters detect and block the malicious attacks that target equipment accessible through a network.

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 Attacks** — Display the related attacks with the filter in the Events screen
- **View Specific Attack** — Display a specific attack for the filter in the Events screen
- **Find** — Search for a filter
- **Advanced Search** — Search for a filter with advanced criteria options

You can perform the following tasks for all Network Equipment Protection filters:

- [“Edit a Network Equipment Filter” on page 220](#)
- [“Create Filter Exception” on page 211](#)
- [“Delete Filter Exception” on page 211](#)



**Note** If you receive errors or have issues editing and saving filters and exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

### How To: Edit a Network Equipment Filter

1. On the **Network Equipment Protection** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.

The appropriate **Filter - Intrusion Prevention Filters - Edits** dialog box displays. It displays the **Main** tab by default. This tab allows you to create customized category settings and exceptions for the specific filter.

3. To enter custom category settings, do the following:
  - Click **Use Filter Specific Settings**.
  - For **State**, click the **Enabled** check box. If you do not click this check box, the filter custom settings are disabled.
  - From the **Action** drop-down menu, select an action set.
4. Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Config State** section, select one of the following:
  - **Use adaptive configuration settings** — Applies the global adaptive filter settings
  - **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter
5. To create a custom filter exception, see [“Create Filter Exception” on page 203](#).

6. Click the **Details** tab. This tab displays the description for the filter.
7. Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

## Traffic Normalization Filters

Traffic Normalization filters block network traffic when the traffic is considered improper or malformed. These filters allow you to set alerts to trigger when the system recognizes this traffic. Traffic pattern anomaly filters alert when network traffic varies from normal. Traffic normalization filters enforce valid packet processing within the Threat Suppression Engine. They protect the engine by detecting invalid or abnormal packets. By protecting the engine, the filters scrub the network of possible issues.

As these filters inspect traffic for malformed packets, Recommended Setting for the action set is typically set to Block. TippingPoint does not recommend using a Permit action as this action could introduce vulnerabilities with malformed packets.

As these filters manage traffic, you may notice not all filters result in blocked streams. The following filters do not hold blocked datastreams:

- 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.

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 — Display the action set for the filter
- View Related Events — Display any events relating to the filter
- Find — Search for a filter
- Advanced Search — Search for a filter with advanced criteria options



**Note** You can create Traffic Normalization filters with the same name as existing filters, and in the same profile. The SMS gives each filter a unique ID, using that ID as reference in the system.

You can perform the following tasks for all Traffic Normalization filters:

- [“Edit Infrastructure Protection Category Settings” on page 210](#)
- [“Edit a Traffic Normalization Filter” on page 222](#)
- [“Create Filter Exception” on page 211](#)

### How To: Edit a Traffic Normalization Filter

1. On the **Profiles - Traffic Normalization** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.

The appropriate **Filter - Traffic Normalization - Edit Filter** dialog box displays.

3. In the **Setting** section, select **Use Category Settings** or **Use Filter Specific Settings**. If you select **Use Filter Specific Settings** to use a different action set for the filter, do the following:
  - Select the **Use Filter Specific Settings** radio button.
  - Check the **Enabled** check box.
  - Choose an **Action** from the drop-down list.



**Note** If you select Recommended as the action set, this sets the filter to the recommended setting for that filter.

If you assign a Permit action to a Traffic Normalization filter, packets matching the rule are logged and passed without further inspection. This process differs from normal packet processing and can introduce vulnerabilities. When you select a non-blocking action set or create an exception to a Normalization filter, you receive a notification from the system.

If you select a rate limit, it applies only to TCP, UDP, or ICMP traffic.

4. Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Config State** section, select one of the following:
  - **Use adaptive configuration settings** — Applies the global adaptive filter settings
  - **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter
5. Optionally, you can add exceptions to the filter. See [“Create Filter Exception” on page 211](#).
6. Click **OK**.



## 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 TippingPoint system 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 go 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 through the **Blocked Streams** tab of the device configuration of the TSE.

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.

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 [“Threshold State” on page 64](#).

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

- New — Create a new filter
- Edit — Edit a selected filter
- Delete — Delete a selected filter
- View Related Events — Display any events relating to the filter
- Find — Search for a filter
- Advanced Search — Search for a filter with advanced criteria options

You can perform the following tasks for all Traffic Threshold filters:

- [Create/Edit a Traffic Threshold Filter](#)
- [Delete a Traffic Threshold Filter](#)

### How To: Create/Edit a Traffic Threshold Filter

1. On the **Profiles - Traffic Threshold** screen, to create:

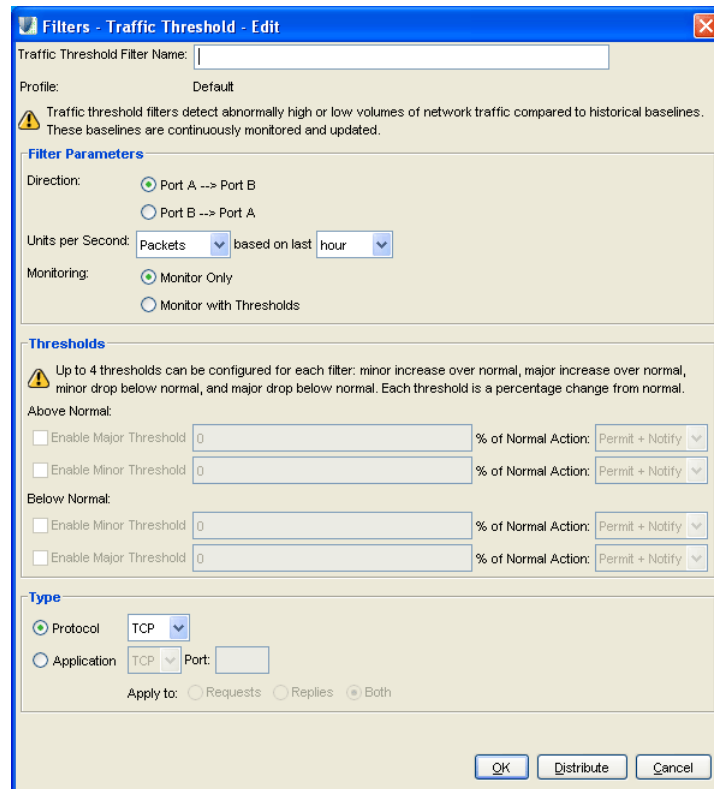
- Click **New**.
- Right-click the selected filter and choose **New**.

To edit, select a filter and:

- Click **Edit**.
- On them Menu bar, click **Edit -> Details...**
- Right-click the selected filter and choose **Edit**.

The **Filters - Traffic Threshold - Edit** dialog box displays.

Figure 6 - 24: Filters - Traffic Threshold - Edit Dialog Box



2. Enter the **Traffic Threshold Filter Name**. The profile for the filter displays below the name.

3. For **Filter Parameters**, modify 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 unity 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.

4. For **Thresholds**, you can modify up to 4 thresholds for each filter: minor increase over normal, major increase over normal, minor drop below normal, and major drop below normal. Each threshold is a percentage change from the “normal” baseline.
  - Click the box to **Enable Above Normal Major**. Enter a percentage amount of normal and select an action set.
  - Click the box to **Enable Above Normal Minor**. Enter a percentage amount of normal and select an action set.
  - Click the box to **Enable Below Normal Major**. Enter a percentage amount of normal and select an action set.
  - Click the box to **Enable Below Normal Minor**. Enter a percentage amount of normal and select an action set.
5. 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**.
6. Click **OK**.

#### How To: Delete a Traffic Threshold Filter

1. On the **Profiles - Traffic Threshold** screen, select a filter.
2. Do one of the following:
  - Click **Delete**.
  - On them Menu bar, click **Edit -> Delete**.
  - Right-click the selected filter and choose **Delete**.
 A deletion message may display. Click **OK** to delete.

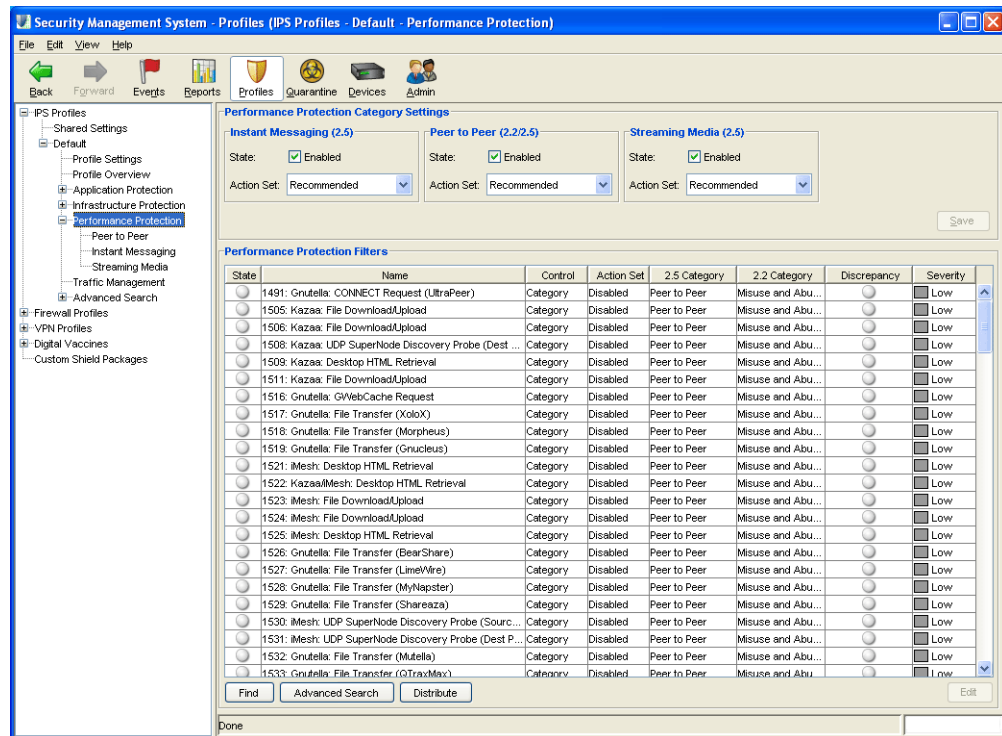
## Performance Protection Filters

Performance Protection is a set of filter categories that allow key applications to have prioritized access to bandwidth. These filters ensure mission critical applications have adequate performance during times of high congestion.

Performance Protection filters allow users to manage policy around non-productive or potentially illegal applications. Initially this includes Peer-to-Peer management, where the user may apply block or shape actions across the category or on an individual basis.

You can view filters of each type or all Performance Protection filters through the **Profiles - Performance Protection** screen:

Figure 6 - 25: Profiles - Performance Protection



These filters have the following settings:

Table 6 - 11: Profiles - Performance Protection Screen Information

Column	Definition
State	Indicates if the filter is currently enabled, disabled, or invalid.
Name	Name of the filter. Click on the filter name link to view and configure filter details.
Control	Location of where the action set is defined for the attack filter.

Table 6 - 11: Profiles - Performance Protection Screen Information

Column	Definition
Action Set	The action set that is performed when the filter is triggered.
2.5 Category	Category that the filter is in for release 2.5
2.2 Category	Category that the filter was previously in for release 2.2 and earlier f
Discrepancy	Indicates if there is a difference in settings between V 2.2 and V 2.5 configurations
Severity	Indicates the potential consequences of the traffic that matches the filter. See <a href="#">“Severity Level” on page 195.</a>

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

- **Copy** — copy selected rows or cell value
- **Edit** — Edit a selected filter
- **New Exception** — Create a new exception
- **View Action Set** — Display the action set for the filter
- **What is Discrepancy** — Provides information about handling differences in filter behavior due to different IPS versions
- **View Related Events** — Display any events relating to the filter
- **Find** — Search for a filter
- **Advanced Search** — Search for a filter with advanced criteria options



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543.](#)

Performance Protection filters allow the user to manage policy around non-productive or potentially illegal applications the user may apply block or shape actions across the category or on an individual basis.

Performance Protection profiles include the following category settings:

- [Peer to Peer](#)
- [Instant Messaging](#)
- [Streaming Media](#)

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

- Edit — Edit a selected filter
- View Action Set — Display the action set for the filter
- View Related Events — Display any events relating to the filter
- Find — Search for a filter
- Advanced Search — Search for a filter with advanced criteria options

You can perform the following tasks for Performance Protection filters:

- [“Edit a Performance Protection Filter” on page 229](#)
- [“Edit Performance Protection Category Settings” on page 228](#)
- [“Search/View a Filter” on page 191](#)
- [“Perform an Advanced Search” on page 192](#)

### How To: Edit Performance Protection Category Settings

1. On the **Profiles** Navigation pane, select **Profiles** —> **Performance Protection**. The **Profiles - Performance Protection** screen displays.

The **Performance Protection Category Settings** section allows you to set filter category settings.



**Note** When you select settings in this section, you globally change the category settings for all filters of that type.

2. For Performance Protection filters, do the following:
  - Check the **Enabled** check box. If the check box is not selected, the filters are disabled.
  - Select an **Action Set** for the filters.
3. Click **Save**.

### 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.

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:

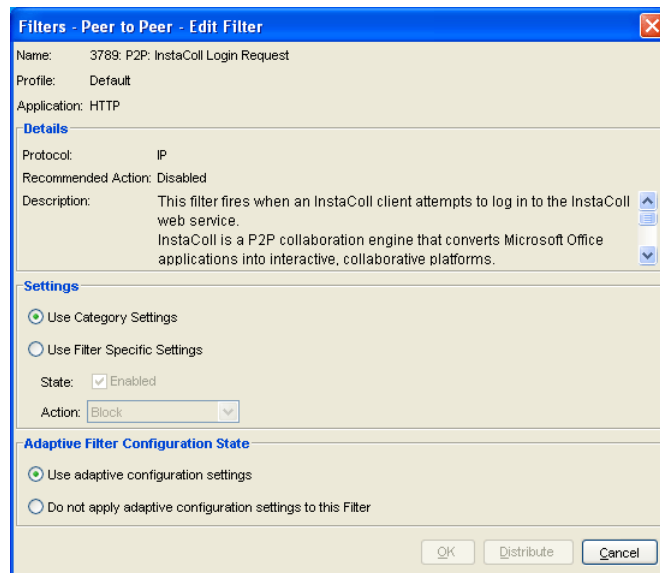
- Unicast — sends a separate copy of the media stream from the client to each client.
- Multicast — sends a single copy of the media stream over any given network connection and must be implemented in network routers and servers.

### How To: Edit a Performance Protection Filter

1. On the **Profiles - Performance Protection** screen, select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the filter and choose **Edit**.

The **Filters - Edit Filter** dialog box displays.

Figure 6 - 26: Filters - Edit Dialog Box



3. For **Settings**, select one of the following: **Use Category Settings** (the default or globally set category settings) or **Use Filter Specific Settings** (custom setting). For Use Filter Specific Settings, do the following:
  - For the **State**, click the **Enabled** check box. If you do not click the check box, the custom settings are disabled.
  - Select an **Action**, such as Block + Notify.

4. Optionally, you can set adaptive filter settings for flow control. In the **Adaptive Filter Configuration State** section, select one of the following:
  - **Use adaptive configuration settings** — Applies the global adaptive filter settings
  - **Do not apply adaptive configuration settings to this filter** — Removes any global adaptive filter settings for this filter
5. Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

## Traffic Management Filters

Traffic Management filters react to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values. As an example, you might define the following Traffic Management filters for your web servers in a lab that denies access to external users:

- Block traffic if the source is on an external subnet that arrives through port 80 and is destined for the IP address of your web server.
- Block traffic if the source is your web server, the source port is 80, and the destination is any external subnet.

The scope of these policies can include any or all of the follow:

- IP Based — Enables you to define a single IP or CIDR to block or shape traffic
- Protocol Based — Enables you to select from a list of predefined protocols to block, monitor or shape traffic. These Protocols include ICMP, UDP, TCP, and Other.

When you create Traffic Management filters, you can modify the sequence they fire in by selecting a filter and using the up and down buttons at the bottom of the screen.

**Figure 6 - 27: Up & Down Buttons**



The up and down buttons move the selected filter up and down in the sequence.

In general, more specific filters should come first. For example, a more specific IP filter might block traffic with fully qualified source and destination IP addresses and ports. More general ones, like those that apply to subnets, should follow.



**Note** This can be a complex task. Some resources that might help you with this process include **Building Internet Firewalls**, by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, 1995, and **Firewalls and Internet Security**, by William R. Cheswick and Steven M. Bellovin, Addison-Wesley Publishing Company, 1994.



Packets that match “allow” or “rate-limit” filters are inspected by other types of filters. In other words, the system does not allow attacks through because the packet matched an “allow” filter. You can also set the filters to trust traffic. *Trusted* filters instruct the IPS not to inspect the traffic, allowing the traffic to continue without comparing it with any other filter rules.

As an example, consider the following IP filters:

**Table 6 - 12: Example Traffic Management Settings**

Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
any	any	UDP	any	53	Allow
any	any	UDP	any	any	Block
any	any	ICMP	any	any	20 Mbps rate-limit
any	1.2.3.4	TCP	any	80	Allow
any	any	TCP	any	80	Block

These filters perform the following:

- Block all UDP traffic except DNS requests. DNS requests are inspected for attacks.
- Limit all ICMP traffic to 20Mbps.
- Block all HTTP traffic except for server 1.2.3.4.

These filters have the following settings:

**Table 6 - 13: Profiles - Traffic Management Screen Information**

Column	Definition
State	Indicates if the filter is currently enabled, disabled, or invalid
Name	Name of the filter. Click on the filter name link to view and configure filter details
Direction	The directional flow of traffic according to the segment Port A and B
Protocol	The action set that is performed when the filter is triggered
Source Address	The source IP address
Src Port	The source IP port
Dest Address	The destination IP address
Dest Port	The destination IP port

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

- New — Create a new filter
- Edit — Edit a selected filter
- Delete — Delete the selected filter
- Save Order — Saves the order of the filters

You can perform the following tasks for Traffic Management Filters:

- [“Create/Edit a Traffic Management Filter” on page 232](#)
- [“Delete a Traffic Management Filter” on page 234](#)
- [“Save the Traffic Management Filter Order” on page 234](#)
- [“Search/View a Filter” on page 191](#)
- [“Perform an Advanced Search” on page 192](#)



**Note** You can create Traffic Management filters with the same name as existing filters, and in the same profile. The SMS gives each filter a unique ID, using that ID as reference in the system.



**TIP** To rate shape traffic for bi-directionality, you must create two filters: one for A -> B and one for B -> A.

### How To: Create/Edit a Traffic Management Filter

1. On the **Profiles - Traffic Management** screen, do one of the following:
  - Click **New**.
  - Right-click on an entry and select **New**.

Or to edit, select a filter and:

- Click **Edit**.
- On the Menu Bar, select the **Edit** —> **Details**.
- Right-click on the filter and select **Edit**.

The **Traffic Management Filters - Create/Edit Filter** dialog box displays.

Figure 6 - 28: Traffic Management Filters - Create/Edit Filter Dialog Box

The screenshot shows a dialog box with the following fields and options:

- Name:** [Empty text box]
- Profile:** Default
- State:**  Enabled
- Apply only to IP Fragments (TOS Versions 2.5 and higher)
- Action:**  Block,  Allow (incoming traffic will be inspected using profile settings),  Trust (incoming traffic will be trusted and not inspected),  Rate Limit [r1]
- Protection Point:**  Port A to Port B,  Port B to Port A,  Create filters for both directions
- Protocol:** IP
- Source:** Address: [Empty], CIDR: [Empty], Port: ANY
- Destination:** Address: [Empty], CIDR: [Empty], Port: ANY
- ICMP Attributes:** Type: [Empty], Code: [Empty]

Buttons at the bottom: OK, Distribute, Cancel.


2. Enter a **Name** for the filter.
3. For **State**, select the **Enabled** check box. If the check box is not selected, the filter is disabled.



**Note** If you want to apply special handling for IP protocol packet fragments, check the appropriate box to create a filter for fragments only. Generally, this option is used on applications, such as streaming media.

**Note** If you use this option to create special handling for packet fragments, you must create another rule to handle non-fragmented packets.

4. Select the **Action** for the filter:
  - **Block** — Select to block traffic
  - **Allow** — Select to handle traffic according to the filter settings
  - **Trust** — Select to accept and not inspect incoming traffic
  - **Rate Limit** — Select the action set. Enter an amount.

5. Select the **Protection Point**:
  - **Port A to Port B** — To protect traffic flowing from Port A to Port B
  - **Port B to Port A** — To protect traffic flowing from Port B to Port AThe button for **Create filters for both directions** will do this for you.  
  
 **TIP** To rate shape traffic for bi-directionality, you must create two filters: one for A -> B and one for B -> A.
6. Select a **Protocol**: **IP**, **TCP**, **UDP**, or **ICMP**.
7. Enter a **Source**:
  - Enter an **IP Address** and select the format as **CIDR**, **IP Mask**, or **Any IP**.
  - Enter the **Port**. Default value is ANY.
8. Enter a **Destination**:
  - Enter an **IP Address** and select the format as **CIDR**, **IP Mask**, or **Any IP**.
  - Enter the **Port**. Default value is ANY.
9. If you selected the ICMP protocol, the filter displays the **ICMP Attributes**:
  - **Type**
  - **Code**
10. Click **OK**.

### How To: Delete a Traffic Management Filter

1. On the **Profiles - Traffic Management** screen, select a filter.
2. Click **Delete**.

### How To: Save the Traffic Management Filter Order

1. On the **Profiles - Traffic Management** screen, move filters into an order for use by the system.
2. Select a filter and click the down button to move it down in the listed order.
3. Select a filter and click the up button to move it up in the listed order.
4. To save the order, do one of the following:
  - Click **Save Order**.
  - Right-click and select **Save Order**.

## DDoS Filters (E-Series Devices)



**Note** Only devices running V 1.4.x TOS software can view and edit DDoS filters. E Series IPS models are purchased and installed with the **Advanced DDoS Protection** feature, replacing these filters. This option is available only on the E Series of devices, such as the TippingPoint 100E/200E/1200E/2400E/5000E.

All other IPS models (not E Series) running 2.x TOS do not have DDoS filter support.

For more information on purchasing E Series devices, contact your TippingPoint Sales Representative.

DDoS, or Distributed Denial of Service filters, detect denial of service attacks. These attacks flood a network with requests, including traditional SYN floods, DNS request floods against nameservers, and attempts to use protected systems as reflectors or amplifiers in attacks against third parties. These filters detect direct flood attacks and attacks hidden within larger packets and requests.

The SMS provides protection against SYN and DDoS attacks through these filters. SYN floods enact a series of requests with false SYN flags that constantly request a connection. 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.

DDoS attacks cause great harm to a network. These attacks have a multitude (in the range of thousands) of systems send TCP/ACK connections to multiple destinations. These destination ports range from 1 to 1024. The general protections and investigation methods do not identify these attacks: IP Source routing and TCP SYN proxy cannot detect these attacks. DDoS disrupts these two possible solutions for locating and blocking such attacks.

DDoS filters protect a network by watching and analyzing network traffic through past history, deeply investigating the IP connections, and monitoring the threshold of connections that could potentially be DDoS connections.

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 — Display the action set for the filter
- View Related Events — Display any events relating to the filter
- Find — Search for a filter
- Advanced Search — Search for a filter with advanced criteria options



**Note** If you receive errors or have issues editing and saving filters and exceptions due to exceeded limits, see [“SMS Error Messages” on page 543](#).

You can perform the following tasks for DDoS Filters:

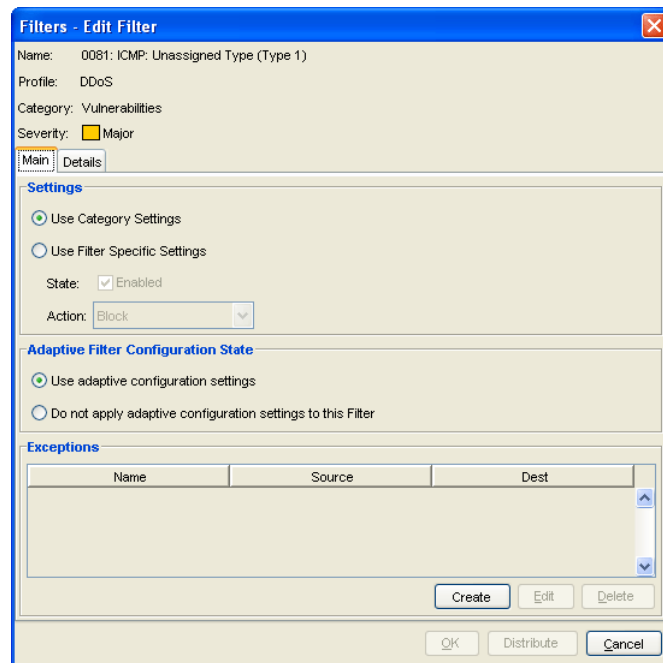
- [“Edit Infrastructure Protection Category Settings” on page 210](#)
- [“Edit a DDoS Filter” on page 236](#)
- [“Create Filter Exception” on page 211](#)
- [“Delete Filter Exception” on page 211](#)

#### How To: Edit a DDoS Filter

1. On the **DDoS** screen, locate and select a filter.
2. To view, do one of the following:
  - Click **Edit**.
  - On the Menu Bar, click **Edit** —> **Details**.
  - Double-click the filter.
  - Right-click the selected filter and choose **Edit**.

The appropriate **Filter - DDoS - Edit Filter** dialog box displays with the **Main** tab as the default. This tab allows you to create customized category settings and exceptions for the specific filter.

Figure 6 - 29: Filter - DDoS - Edit Filter Dialog Box (Main tab)



3. To enter custom category settings, do the following:
  - Click **Use Filter Specific Settings**.
  - For **State**, click the **Enabled** check box. If you do not click this check box, the filter custom settings are disabled.
  - From the **Action** drop-down menu, select an action set.

4. Enter a **Threshold** setting of SYN requests per second.
5. To create a custom filter exception, see [“Create Filter Exception” on page 203](#).
6. Click the **Details** tab. This tab displays the description for the filter.
7. Click **OK**.



**Note** If you receive errors or have issues editing and saving filters due to exceeded limits, see [“SMS Error Messages” on page 543](#).

## Firewall Profiles (X-Family Devices)

This section contains the following topics

- [“Managing Firewall Profiles” on page 237](#)
- [“Managing Firewall Profile Rules” on page 239](#)
- [“Firewall Shared Settings” on page 241](#)

The X-Family device polices traffic between the security zones according to a set of firewall rules. Using these rules, you can prioritize, permit, block, filter, authenticate, schedule and monitor traffic between security zones. You can define the order in which the firewall rules are applied, so that traffic is checked first against the higher priority rules.

The X-Family is pre-configured with a set of default firewall rules. The SMS can configure and distribute firewall rules to multiple X-Family devices. Firewall profiles are separate profiles from device profiles.

### Managing Firewall Profiles

The main **Profiles (Firewall Profiles)** screen provides a top level view of firewall inventory and firewall profile distribution. From this screen you can, import, distribute, view and manage firewall profiles. You can also create a new firewall profile using the Firewall Profile setup wizard. The Firewall setup wizard allows you to create a profile with the default set of rules which are applicable for devices managed by the device you choose as the foundation device.

This section has the following items:

- [“Creating New Firewall Profiles” on page 238](#)
- [“Distributing Firewall Profiles” on page 238](#)

## Creating New Firewall Profiles

### How To: Add a Firewall Profile

1. From the **Profiles** Navigation menu, select **Firewall Profiles**.
2. Click the **New** button.  
The setup wizard displays. 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.
3. On the **Profile Name and Description** screen, complete the following information:
  - Profile Name
  - Description
4. On the **Device Foundation** screen, choose a device to use as the foundation. The selected device is used as the basis for providing Security Zones, IP Address Groups, and Privilege Group For information on creating new security zones, see [“Network Configuration: Segments/Zones Tab” on page 395](#).
5. On the **Default Firewall** screen, make sure that the **Create Default Firewall Rules for this Profile** box is checked.
6. Click **Finish** to save your Firewall profile.

## Distributing Firewall Profiles

For user-defined profiles, the SMS allows users to distribute profiles to multiple devices. The firewall profile distribution can:

- update device’s shared settings such as services, service groups and schedules prior to policy rule distribution operation.
- save information about which devices have which profiles as of the last distribution.
- maintain default setting for rules and shared settings using the latest information available from shared device files.



**Note:** When distributing new profile rules to devices, the new profile rules will completely replace old rules on the device. Also, shared settings will automatically be reconciled before the new profile rules are distributed. Be aware that this reconciliation can add and/or modify shared settings on the device based on the SMS shared settings. This can potentially change values of existing services, service groups and/or schedules.

See also [“Distribute a Firewall Profile” on page 238](#).

### How To: Distribute a Firewall Profile

1. From the **Profiles** Navigation menu, expand **Firewall Profiles**.
2. Select a firewall profile from the inventory listing and click **Distribute**.



3. On the **Profile Distribution** screen, select individual devices or the **All Devices** to include every device.
4. Click **OK** to distribute the profile to the selected devices.

## Managing Firewall Profile Rules

Each firewall profile has a set of rules that are applied by the X-Family device. These rules are applied in the order they are displayed in the Firewall Rules table. The first rule that matches the category of the traffic in the request is applied first.

Specific features of the SMS Firewall rules include the following items:

- Allows one or more rules per profile as in LSM
- Can specify either a service or a service group
- Can specify a schedule (*default is always on*)
- Can depend on a SMS named address group where the members are defined on each device and can be different for each device
- Can depend on a SMS named address group where the members are globally defined and maintained. For more information, see [“Named Resources” on page 487](#).

Device default settings are available on the SMS for use in creating new rules and for populating initial values for shared settings.

After you create a firewall profile using the default settings, you may want to make specific changes in the rules. The **Firewall Rules** Table provides a convenient location to create, copy and edit firewall rules. After making these changes, you can also distribute the profile directly from the **Firewall Rules** screen.

You can perform the following tasks:

- [“Add a Firewall Rule” on page 239](#)
- [“Manage Firewall Rules” on page 240](#)
- [“Edit a Firewall Rule” on page 240](#)

### How To: Add a Firewall Rule

1. From the **Profiles** Navigation menu, expand **Firewall Profiles** and perform one of the following tasks:
  - In the inventory listing, double-click a firewall profile.
  - From the Navigation pane, select a firewall profile.
2. Click **Edit Rules**.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
3. Click the **New** button.  
The setup wizard displays. 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 **Action Definition** screen, complete the following information:
  - Action to take on a packet
  - Service that the rule applies to
  - Enable/Disable status If desired, you can enable on a schedule, such as typical working days and hours.
5. On the **Target Traffic** screen, choose which traffic path (Source and Destination Zones) to apply this firewall rule.
6. On the **Bandwidth Management** as an optional step, you can enable and configure bandwidth management to provide better control over network resources
7. On the **User Authentication** screen as an optional step, you can allow the rule to be applied only to authenticated users.
8. On the Other Settings screen, you can enable logging, set time for inactivity, and add any comments.
9. Click **Finish** to save your Firewall rule.

### How To: Manage Firewall Rules

1. From the **Profiles** Navigation menu, expand **Firewall Profiles** and perform one of the following:
  - In the inventory listing, double-click a firewall profile.
  - From the Navigation pane, select a firewall profile.
2. Click **Edit Rules**.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
3. Select a rule or rules and perform any of the following tasks:
  - Use the up- and down-arrows to change the order in which rules will be applied.
  - Click **Copy Rule(s)** to make a copy of a rule.
  - Click **Delete** to remove the rule for the firewall profile.

### How To: Edit a Firewall Rule

1. From the **Profiles** Navigation menu, expand **Firewall Profiles** and do one of the following tasks:
  - In the inventory listing, double-click a firewall profile.
  - From the Navigation pane, select a firewall profile.
2. Click **Edit Rules**.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
3. Select a rule from the list and click the **Edit** button.  
The setup wizard displays.
4. Make any needed changes and click **OK**. To navigate between screens, select the appropriate screen listing from the wizard navigation pane.

## Firewall Shared Settings

Shared settings contains the following tab options:

- [Services](#) — specific list of services for firewall rules only
- [Service Groups](#) — named list of services to allow a rule that can specify multiple services
- [Schedules](#) — time ranges for firewall rule schedule
- [Common Parameters](#)



**Note** To delete one or more custom shared settings that you created, such as service, service group or schedule, select one or more items and click the **Delete** button.

You can perform the following tasks:

- [“Add a Custom Service” on page 241](#)
- [“Edit a Custom Service” on page 242](#)
- [“Add a Service Group” on page 242](#)
- [“Edit a Custom Service” on page 242](#)
- [“Add a Schedule” on page 243](#)
- [“Set up a common definition for common parameters” on page 243](#)
- [“Associate a common name with a firewall profile” on page 244.](#)

### Services

From the Custom Firewall Services area, you can create and manage custom services. From the Default Firewall Services area, you can edit any default services.

See also [“Add a Custom Service” on page 241](#) and [“Edit a Custom Service” on page 242](#).

#### How To: Add a Custom Service

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Services** tab.
3. Click **New**.
4. On the **Add Service** screen, complete the following information:
  - Service Name
  - Protocol for the service
  - Destination Port Range
5. Click **OK**.

### How To: Edit a Custom Service

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Services** tab.
3. Select a custom or default service and click **Edit**.
4. On the **Edit Service** screen, make the desired edits of the following information:
  - Service Name
  - Protocol for the service
  - Destination Port Range
5. Click **OK**.

## Service Groups

From the Service Groups area, you can create new service groups and edit existing groups.

See also [“Add a Service Group” on page 242](#) and [“Edit a Custom Service” on page 242](#)

### How To: Add a Service Group

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Service Group** tab.
3. Click **New**.
4. On the **Add Service group** screen, use the arrow buttons to move the desired available services to the **Selected Services** area.
5. Click **OK**.

### How To: Edit a Custom Service

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Service Groups** tab.
3. Select a service group and click **Edit**.
4. On the **Edit Service Group** screen, use the arrow button to move services to the **Selected Services** area
5. Click **OK**.

## Schedules

From the **Schedules** area, you can add or edit a schedule for Firewall Rules.

See also [“Add a Schedule” on page 243](#) and [“Edit a Schedule” on page 243](#)

### How To: Add a Schedule

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Schedules** tab.
3. Click **New**.
4. On the **Firewall Rule Schedule** screen, specify a name for the schedule and click **Add**.
5. On the **Schedule - Time Interval** screen, define the time ranges to include and click **OK**.
6. On the **Firewall Rule Schedule** screen, click **OK** to save your schedule.

### How To: Edit a Schedule

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Select **Shared Settings** and the **Schedules** tab.
3. Click **Edit**.
4. On the **Firewall Rule Schedule** screen, make any desired changes to the schedule name.
5. To make changes to the schedule, select the listed schedule and click **Edit**.
6. On the **Schedule - Time Interval** screen, make any desired changes to the time ranges and click **OK**.
7. On the **Firewall Rule Schedule** screen, click **OK** to save your schedule.

## Common Parameters

You can define a set of common parameters with a common definition that can be used with a firewall profile to manage one or more devices. Areas that can be used with a firewall profile include the following items:

- privilege group — an association of users based on user access requirements
- security zones — a section of the network which is associated with a port or a network
- IP address group — an association of systems based on system IP addresses

For example, you can set up a privilege group that is attached to a firewall rule that allows for the removal of web content blocking for the users in the privilege group.

See also [“Set up a common definition for common parameters” on page 243](#) and [“Associate a common name with a firewall profile” on page 244](#).

### How To: Set up a common definition for common parameters

1. On the **Devices** screen Navigation pane, expand the entry for a TippingPoint X-Family device, and then select **Network Configuration**,
2. Define common parameters such as WAN, LAN, etc.

### How To: Associate a common name with a firewall profile

1. From the **Profiles** Navigation pane, select and expand **Firewall Profiles**.
2. Associate a specific device and its parameters with a firewall profile and its rules.



**Note:** To use a service group to distribute a common firewall profile to multiple devices, you must use the same name for the common service group on each device you plan to use with the firewall profile.

## VPN Profiles (X-Family Devices)

This section contains the following items:

- [“Managing VPN Profiles” on page 244](#)
- [“VPN Shared Settings” on page 245](#)

A Virtual Private Network (VPN) is a means of establishing a secure private network connection between devices across a public network, for example, the Internet. A VPN uses packet encryption to tunnel across the public connection from the Initiation Point to the Termination Point. The SMS can create VPN networks among the X-Family devices that it manages by creating and deploying a SMS VPN profile. The SMS VPN profile supports following VPN topologies:

- **point-to-point** — a tunnel exists between each pair of systems
- **hub and spoke** — a number of remote sites (spokes) are connected to a central site (hub),
- **full mesh** — a tunnel exists between every pair of VPN edge devices.



**Note** When setting up a VPN tunnel that terminates in the different security zone with LANs, make sure to set your firewall rules to allow the traffic to flow between the tunnel and the LAN.

### Managing VPN Profiles

The VPN profile takes care of all the VPN settings and IP routing for the VPN network by automatically generating the following items:

- security associations
- IP address groups (if needed)
- GRE virtual interfaces (if needed)
- static routes (if needed)

After setting up a VPN profile or profiles, you can then select a profile from the VPN Profile inventory and deploy the profile.

You can perform the following tasks:

- [“Set up a VPN Profile” on page 245](#)
- [“Deploy a VPN Profile” on page 245](#)
- [“Set up IPSec Security Association” on page 246](#)

### How To: Set up a VPN Profile

1. From the **Profiles** Navigation menu, expand **VPN Profiles**.
2. Click the **New** button.  
The setup wizard displays. 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.
3. Complete the following information:
  - VPN Profile Name
  - Topology Type (point-to-point, hub and spoke, or full mesh)
4. Select the devices to include in the VPN Profile and select the Terminating Security Zone. For information on creating new security zones, see [“Network Configuration: Segments/Zones Tab” on page 395](#).
5. Select the Tunnel Type (IPSec or GRE over IPSec). If you are using GRE over IPSec as your tunnel type, complete the Transport mode information.
6. Click **Finish** to save your VPN profile.

### How To: Deploy a VPN Profile

1. From the **Profiles** Navigation menu, expand **VPN Profiles**.
2. Select a VPN profile from the VPN Profile Inventory and click **Deploy**.  
A VPN deployment preview dialog appears that lists the information, warnings and error messages for each device in the profile.
3. If there are no errors, click **OK** to deploy the profile. If there are errors, you must fix any errors before you deploy the profile.

## VPN Shared Settings

Shared settings contains the following tab options:

- [“IKE Proposals Tab” on page 245](#)
- [“Security Zones Tab” on page 246](#)

### IKE Proposals Tab

The VPN profile uses IKE as keying mode. so you need to configure at least one IKE proposal to select the security attributes for VPN. the IKE proposal wizard has two screens to complete, IKE Phase 1 setup and IKE Phase 2 setup.

See also [“Set up IPSec Security Association” on page 246](#).

### How To: Set up IPSec Security Association

1. From the **Profiles** Navigation menu, expand **VPN Profiles** and select **Shared Settings**.
2. In the List pane, select the IKE Proposals tab and do one of the following tasks:
  - Select an existing IKE Proposal and click **Edit**.
  - Click **New** to create a new Security Association.
3. Complete each of the two setup screen. For additional information about the needed information, click the **more** link located in the top right-hand corner the wizard setup screen.
4. When all information is complete, click **Finish**.

### Security Zones Tab

From the security zone tab, you can designate the name for new security zone, edit or delete a security zone. Those security zones could be referred when you create a VPN profile. During VPN profile deployment, if there is no such security zone in a device, the new security zone will be created using the default configuration of the device.

You can use the SMS to add, edit, or delete security zones. A security zone is a section of the network which is associated with a port or VLAN. If you need to control the traffic between devices, the devices must be in separate security zones. Security zones enable you to logically segment your networks so that the SMS can apply firewall rules and IPS filters to control the traffic passing between the zones.

From the **Security Zones** tab, you can designate the name for a new security zone, edit the name of an exiting security zone, or delete a security zone. For information on configuring security zones, see [“Network Configuration: Segments/Zones Tab” on page 395](#).

## Digital Vaccine Management

This section contains the following topics:

- [“Digital Vaccine Screen” on page 247](#)
- [“Digital Vaccine Tasks” on page 249](#)

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

You can manually or automatically download and distribute these updates through the **Profiles - Digital Vaccines** screen. The screen allows you to download packages and distribute them to devices 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, deselect that option when prompted to download a new DV and also on the Digital Vaccine management screen in the Profiles area of the SMS. See [“Digital Vaccine Alert Window” on page 10](#).



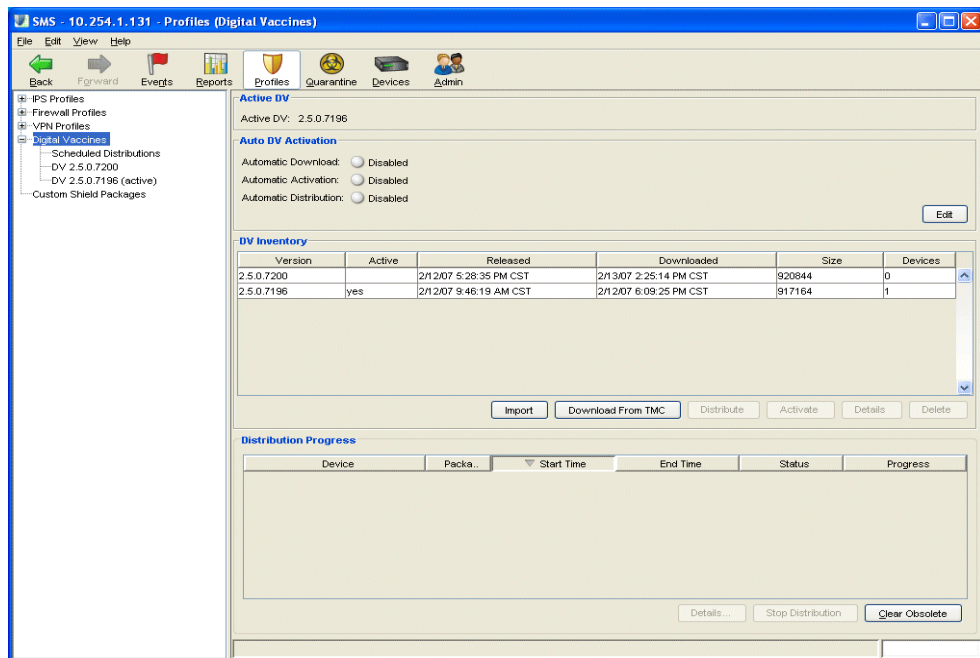
You can also have the SMS send you email notification of automatic Digital Vaccine downloads and distribution. To receive these messages via e-mail, you need to add your contact information to the Network Information settings for the SMS system. See [“Network Information” on page 470](#)

Only users with Super User and Administrator access can perform these operations.

## Digital Vaccine Screen

The following is the Digital Vaccine screen:

Figure 6 - 30: Digital Vaccine Screen



the Digital Vaccine screen has the following information:

- **DV Auto Activation** — provides version information about the active Digital Vaccine package and options for automatic downloads and distribution.
- **DV Inventory** — lists the Digital Vaccine packages that have been downloaded and are available for distribution
- **Distribution Progress** — provides information on distribution status of a Digital Vaccine package for a device

Table 6 - 14: DV Inventory Details

Column	Description
Version	The version of the Digital Vaccine package
Active	The active status of the Digital Vaccine package. You can download many packages that can be activated based on your system needs.
Released	The date and time the Digital Vaccine package was released
Downloaded	The date and time the Digital Vaccine package was downloaded from the TMC
Size	The file size of the Digital Vaccine package
Devices	The number of devices that have received the distributed Digital Vaccine package. If the number is zero (0), the package has not been distributed.

The process for downloading and managing these filters includes the following:

1. Download or import the latest filters from the TMC in the form of *Digital Vaccine packages*.

In the **Profiles - Digital Vaccines** screen, you can see 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 IPS devices 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 163](#).

You can right-click on entries in the DV Inventory and do the following:

- **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 package active
- **Details** — View the details of the package
- **Delete** — Removes 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 c You can also directly download the package file from the Threat Management Center through the SMS.



**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.

Only users with Super User and Administrator access can perform these operations.

## Digital Vaccine Tasks

DV Package management includes the following major task areas:

- [“Importing DV Packages” on page 249](#)
- [“Managing DV Packages” on page 251](#)
- [“Distributing DV Packages” on page 252](#)

### Importing DV Packages

When you import a Digital Vaccine package, the SMS accesses TMC 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 Client 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 New Digital Vaccine Packages” on page 250](#)
- [“Download a Digital Vaccine Package” on page 250](#)
- [“Import a Digital Vaccine Package” on page 250](#)

### How To: Auto-Download New Digital Vaccine Packages

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. To enable auto-download, select the **Automatic Download Enable** check box.
3. To disable auto-download, unselect the **Automatic Download Enable** check box.

If you enable the option, the system automatically checks for and downloads a new Digital Vaccine package from the TMC.

### How To: Download a Digital Vaccine Package

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. Do one of the following:
  - In the **DV Inventory** section, click **Download from TMC**.
  - On the Menu Bar, select the **File** —> **Download Digital Vaccine from TMC** menu item.
  - Right-click an entry and click **Download from TMC**.
3. Select a version to download.
4. 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.

### How To: Import a Digital Vaccine Package

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 navigation pane on the left, click **Digital Vaccines**. The page lists all available software images. The most recent version is at the top of the list.
3. Click the **More Info** button next to the most recent package.
4. In the Download File page, click the **Download Now** button. After a few seconds, the **File Download** dialog box is displayed.
5. 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.

6. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.

7. Do one of the following:
  - In the **DV Inventory** section, click **Import**.
  - On the Menu Bar, select the **File** —> **Import** —> **Digital Vaccine** menu item.
  - Right-click an entry and click **Import**.
8. Locate and select the file to import. Click **OK** to begin import.

The file imports and displays in the **DV Inventory** section and **Profiles** Navigation pane.

## Managing DV Packages

After importing these packages, you can activate, delete, and view the information for the packages.

You can now make this package active if desired, as well as view details, distribute, and remove the package.

You can perform the following tasks:

- [“Delete a Digital Vaccine Package” on page 251](#)
- [“Activate a Digital Vaccine Package” on page 251](#)
- [“View Details of a Digital Vaccine Package” on page 252](#)

### How To: Delete a Digital Vaccine Package

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. Select a package to delete.



**Note** You cannot delete active packages. If you attempt to delete an active package, an error message displays.

3. Do one of the following:
  - In the **DV Inventory** section, click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete** menu item.
  - Right-click an entry and click **Delete**.
4. A verification message displays. Click **Yes**.

### How To: Activate a Digital Vaccine Package

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. In the DV Inventory, select a package.

3. Do one of the following:
  - In the **DV Inventory** section, click **Activate**.
  - In the **DV Inventory** section, click **Details**. On the displayed screen, click **Activate**.
  - On the Menu Bar, select the **File** —> **Activate** —> **Digital Vaccine** menu item.
  - Right-click an entry and click **Activate**.

The package displays as active in the **DV Inventory** section.

### How To: View Details of a Digital Vaccine Package

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. In the **DV Inventory** section, select a package.
3. Do one of the following:
  - In the **DV Inventory** section, click **Details**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.
  - Right-click an entry and click **Details**.
4. 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.
5. The **Release Notes** tab provides the documentation for the DV package.
6. You can perform a distribution and activation for the DV package from this screen.

### Distributing DV Packages

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.

The following table outlines permissions for scheduled distributions:

**Table 6 - 15: Permissions for Scheduled Distributions**

Role	Actions	Access
Super User	can view, edit, and create scheduled distributions	<b>All Devices or Selected Groups</b> option
Admin user	can view, edit, and create scheduled distributions	any device to which Super Users have granted them access

You can perform the following tasks:

- [“Auto-Distribute New Packages” on page 253](#)
- [“Distribute New Packages” on page 253](#)
- [“Cancel a Distribution Process” on page 254](#)
- [“New Scheduled Distribution” on page 254](#)
- [“Edit Scheduled Distribution” on page 254](#)

#### How To: Auto-Distribute New Packages

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. To enable auto-distribution, select the **Automatic Distribution Enable** check box.
3. To disable auto-distribution, deselect the **Automatic Distribution Enable** check box.

If you enable the option, the system automatically distributes a newly imported or downloaded Digital Vaccine package.

#### How To: Distribute New Packages

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. In the **DV Inventory** section, select a package.
3. Do one of the following:
  - In the **DV Inventory** section, click **Distribute**.
  - On the Menu Bar, select the **File** —> **Distribute to Device** —> **Digital Vaccine** menu item.
  - Right-click on the entry and click **Distribute**.
4. In the distribution dialog, select the device or devices you want to receive the distribution.
5. The package distributes. As it runs, an entry displays with updating status in the **Distribution Progress** section.

### How To: Cancel a Distribution Process

1. In the **Profiles** Navigation pane, click **Digital Vaccines**. The **Profiles - Digital Vaccines** screen displays.
2. In the **Distribution Progress** section, select a distribution in-progress.
3. In the **Distribution Progress** section, click **Cancel Distribution**.

### How To: New Scheduled Distribution

1. In the **Profiles** Navigation pane, click **Digital Vaccines**, and then select **Scheduled Distributions**. The **Profiles (Digital Vaccines - Scheduled Distributions)** screen displays.
2. Click **New**.  
The setup wizard displays. 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.
3. On the **Generals Settings** screen, select a one time or recurring schedule. If you select a recurring schedule, complete the scheduled distribution time.
4. Click **Next**.
5. Choose which device or devices will receive the distribution package. If you want all the devices to receive the package, select the check box next for the **All Devices** folder.

### How To: Edit Scheduled Distribution

1. In the **Profiles** Navigation pane, click **Digital Vaccines**, and then select **Scheduled Distributions**. The **Profiles (Digital Vaccines - Scheduled Distributions)** screen displays.
2. Select an existing scheduled distribution from the List pane and Click **Edit**. The setup wizard displays.
3. Make desired changes and click **OK**.

## Custom Shield Package Management

This section contains the following topics:

- [“Creating and Activating Packages” on page 256](#)
- [“Managing Packages” on page 257](#)
- [“Distributing Packages” on page 259](#)

You may want to create your own custom filters for your network and system. TippingPoint created the Custom Shield Writer (CSW) for this purpose. These filters are saved into package files, imported into the SMS, and distributed to devices.


When you upload CSW packages, the SMS assigns each filter a new filter ID based on the ID you previously assigned it using the Custom Shield Writer. Each filter created by the CSW numbers the



filters with a starting C followed by numbers. The SMS removes the C character and adds one million to the filter number. For example, C001 in CSW becomes 1000001 in SMS.

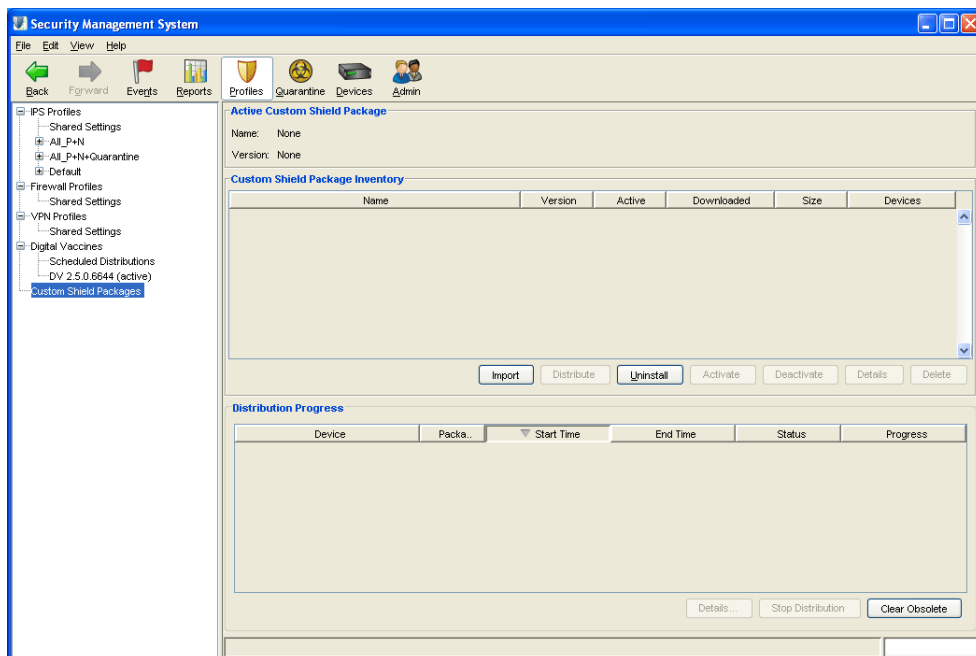
Only users with Super User and Administrator access can perform these operations.

Through the **Profiles - Custom Shield Packages** screen, you can import and distribute the filters to devices managed by the SMS.

 **Note** The latest version of Custom Shield Writer may not function the same way as previous versions. For the latest information, see the IPS Release Notes and the IP User Guide. For the most recent documentation updates, check the Threat Management Center (TMC) Web site, <https://tmc.tippingpoint.com>.

## Custom Shield Packages Screen

Figure 6 - 31: Profiles - Custom Shield Packages Screen



The **Profiles - Custom Shield Packages** screen includes the following information:

- **Active Custom Shield Package** — provides the name and version information about the active Custom Shield Package.
- **Custom Shield Package Inventory** — lists the Custom Shield packages that have been downloaded and are available for distribution
- **Distribution Progress** — provides information on distribution status of a Custom Shield package for a device:

Table 6 - 16: CSW Inventory Details

Column	Description
Name	Name of the Custom Shield package
Version	The version of the package
Active	The active status of the package. You can import many packages that can be activated based on your system needs.
Downloaded	The date and time the package was downloaded from the TMC
Size	The file size of the package
Devices	The number of devices that have received the distributed package. If the number is zero (0), the package has not been distributed.

## Creating and Activating Packages

Using the Custom Shield Writer, create and save custom filters to a package file. For the latest information, see the *TippingPoint IPS Release Notes* and the *TippingPoint IPS User's Guide*. For the most recent documentation updates, check the Threat Management Center (TMC) Web site, <https://tmc.tippingpoint.com>.

See also [“Import and Activate a Custom Package” on page 256](#).

### How To: Import and Activate a Custom Package

1. In the **Profiles - Custom Shield Packages** screen, you can see the list of packages installed and activated on your system.
2. Select the package. Click **Activate**.
3. Edit and customize the filters. You may need to enable certain filters according to the filter pillar type.
4. Distribute the Custom Shield package prior to distributing the profile. Select the package and click **Distribute**.
5. On the **Profiles** screen, select a profile to distribute. Distribute the profile to IPS devices or associated segment group.

As you make changes and additions, the SMS saves the changes to a profile. The profile includes all filter changes and recent additions of the Custom Shield package. For distribution information, see [“Distributing Profiles” on page 163](#).

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

- Import — Import a Custom Shield package from a file
- Distribute — Distribute the Custom Shield package to the devices
- Activate — Make the package active in the SMS and for the device. Deactivating the package removes it as the currently used package. To remove a package from a device, use the uninstall option.
- Details — View the details of the package
- Delete — Removes the package file from the system

## Managing Packages

Through the **Profiles - Custom Shield** screen and Navigation pane, you can manage Custom Shield packages. When you update the filters of a system, you can download or import the packages. To import a package, you must have a Custom Shield package file. You can create this file through the Custom Shield Writer application

Only users with Super User and Administrator access can perform these operations.

You can perform the following tasks:

- [“Import a Custom Shield Package” on page 257](#)
- [“Delete a Custom Shield Package” on page 258](#)
- [“Activate/Deactivate a Custom Shield Package” on page 258](#)
- [“View Details of a Custom Shield Package” on page 258](#)
- [“Uninstall a CSW Package” on page 259](#)

### How To: Import a Custom Shield Package

1. Create and save a Custom Shield package using the Custom Shield Writer.
2. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
3. Do one of the following:
  - In the **Csw Inventory** section, click **Import**.
  - On the Menu Bar, select the **File** —> **Import** —> **Custom Shield Packages** menu item.
  - Right-click on an entry and click **Import**.
4. Locate and select the package file you created.

The file imports and displays in the **DV Inventory** section and **Packages** Navigation pane. You can now manage, view details, distribute, and remove the package.

### How To: Delete a Custom Shield Package

1. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
2. Select a package to delete.



**Note** You cannot delete active packages. If you attempt to delete an active package, an error message displays.

3. Do one of the following:
  - In the **Csw Inventory** section, click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete** menu item.
  - Right-click an entry and click **Delete**.
4. A verification message displays. Click **Yes**.

### How To: Activate/Deactivate a Custom Shield Package

1. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
2. In the CSW Inventory, select a package.
3. To Activate the package (make the selected package the currently used package):
  - In the **Csw Inventory** section, click **Activate**.
  - In the **Csw Inventory** section, click **Details**. On the displayed screen, click **Activate**.
  - On the Menu Bar, select the **File** —> **Activate** —> **Custom Shield Packages** menu item.
  - Right-click an entry and click **Activate**.
4. To Deactivate the package (remove the current active package from the SMS):
  - In the **Csw Inventory** section, click **Deactivate**.
  - In the **Csw Inventory** section, click **Details**. On the displayed screen, click **Deactivate**.
  - On the Menu Bar, select the **File** —> **Deactivate** —> **Custom Shield Packages** menu item.
  - Right-click an entry and click **Deactivate**.

The package displays as active in the **Csw Inventory** section.

### How To: View Details of a Custom Shield Package

1. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
2. In the **Csw Inventory** section, select a package.

3. Do one of the following:
  - In the **Csw Inventory** section, click **Details**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.
  - Right-click an entry and click **Details**.

The **Profiles - Custom Shield Details** screen displays.

### How To: Uninstall a CSW Package

1. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
2. In the **CSW Inventory** section, select a package.
3. Click **Uninstall**. The package uninstalls filters associated with the selected CSW package. When you distribute profiles, the uninstalled filters are removed from the devices.

## Distributing Packages

When you distribute a Custom Shield 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 - Custom Shield Packages** 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.

You can perform the following tasks:

- [“Distribute New Packages” on page 259](#)
- [“Cancel a Distribution In-Progress” on page 166](#)

### How To: Distribute New Packages

1. In the **Profiles** Navigation pane, click **Custom Shield Packages**. The **Profiles - Custom Shield Packages** screen displays.
2. In the **Csw Inventory** section, select a package.
3. Do one of the following:
  - In the **Csw Inventory** section, click **Distribute**.
  - On the Menu Bar, select the **File** —> **Distribute to Device** —> **Custom Shield Packages** menu item.
  - Right-click an entry and click **Distribute**.
4. The package distributes. As it runs, an entry displays with updating status in the **Distribution Progress** section.



# 7 Quarantine

*The Quarantine screen provides a centralized interface for managing quarantine actions, policies, switches, and quarantined hosts.*

## Overview

This section includes the following topics:

- [“Quarantine: What’s New” on page 262](#)
- [“How To Tasks” on page 262](#)
- [“Navigation and Menu Options” on page 263](#)
- [“Configuring Quarantine” on page 265](#)
- [“Quarantined Hosts” on page 266](#)
- [“Actions” on page 269](#)
- [“Policies” on page 278](#)
- [“Network Devices” on page 283](#)
- [“Radius” on page 285](#)
- [“IP Correlation” on page 286](#)
- [“Managing Manual Quarantine Policy” on page 291](#)
- [“Managing Quarantine Through an External/3rd-Party Interface” on page 291](#)

Threats to network security require advanced features to manage and mitigate malicious traffic and hosts. Quarantine features provide mitigation security to block infected or malicious traffic, inform the user of possible threats, and place the host into remediation. The SMS places the host into a queue of quarantined hosts that you can review and manage accordingly.

SMS Quarantine is a service that reacts to its inputs in order to perform a set of actions. How it reacts and the set of actions taken is based on the Quarantine Policies that the user has configured. A policy contains a set of actions to be taken when the policy is triggered. A policy can be triggered in several

ways: thresholding, manual, web service, or escalation of an IPS Quarantine. Policies can be configured to include and/or exclude a set 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.

TippingPoint provides multiple methods for quarantining hosts. Filters include action sets with options to automatically redirect users and halt trigger traffic flows. Quarantine policies watch all traffic according to devices and filters to enact another layer of quarantine protection. And the SMS provides manual actions for adding hosts to the quarantine queue.

The Quarantine options in this section detail the actions and policies that perform expanded quarantine actions beyond filter action sets. Triggered policies can make an entry to the event log, email a message regarding the issue, and perform an SNMP trap. You can also create policies for switches, integrating with 3Com EMS systems.

**IMPORTANT! Make sure your system meets TMC port requirements. See [“Port Information” on page 557](#).**



**Note** The feature uses XML scripts for defining the available action types. In continuing releases, you can write scripts to define custom action types for your network topology.

## Quarantine: What's New

This section outlines the following major changes for the current SMS release:

- **Web Action** — allows you to specify the destination for the HTTP/HTTPS message.

## How To Tasks

### *Quarantined Hosts*

- [“How To: Search Quarantined Hosts” on page 268](#)
- [“How To: Unquarantine a Host” on page 268](#)
- [“How To: View Quarantine Events by Hosts” on page 269](#)

### *Actions*

- [“How To: Edit the Switch Disconnect Action” on page 270](#)
- [“How To: Implement the Switch Disconnect Action” on page 271](#)
- [“How To: Edit the IPS Default Quarantine Action” on page 271](#)
- [“How To: Create/Edit a Syslog Action” on page 272](#)
- [“How To: Implement a Syslog Action” on page 273](#)
- [“How To: Create/Edit an Email Action” on page 273](#)
- [“How To: Implement an Email Action” on page 273](#)
- [“How To: Create/Edit a NMS Trap Action” on page 274](#)



- [“How To: Create/Edit a Web Action” on page 275](#)
- [“How To: Implement a Web Action” on page 276](#)
- [“How To: Create/Edit a SNMP Trap Action” on page 276](#)
- [“How To: Create/Edit a Move Quarantined Host onto a VLAN action” on page 277](#)
- [“How To: Implement a Move Quarantined Host onto a VLAN Action” on page 277](#)

### ***Policies***

- [“How To: Edit Default Quarantine Policy” on page 280](#)
- [“How To: Manually Quarantine a Host” on page 281](#)
- [“How To: Create/Edit a new Policy” on page 282](#)

### ***Network Devices***

- [“How To: Add/Edit a Switch” on page 284](#)

### ***RADIUS***

- [“How To: Configure RADIUS” on page 286](#)

### ***IP Correlation***

- [“How To: Add/Edit Network Mapping” on page 288](#)
- [“How To: Add/Edit Web Services” on page 289](#)
- [“How To: Control Web Service Precedence” on page 289](#)
- [“How To: Perform a Test” on page 290](#)

## Navigation and Menu Options

The Quarantine screen includes the following panes and options:

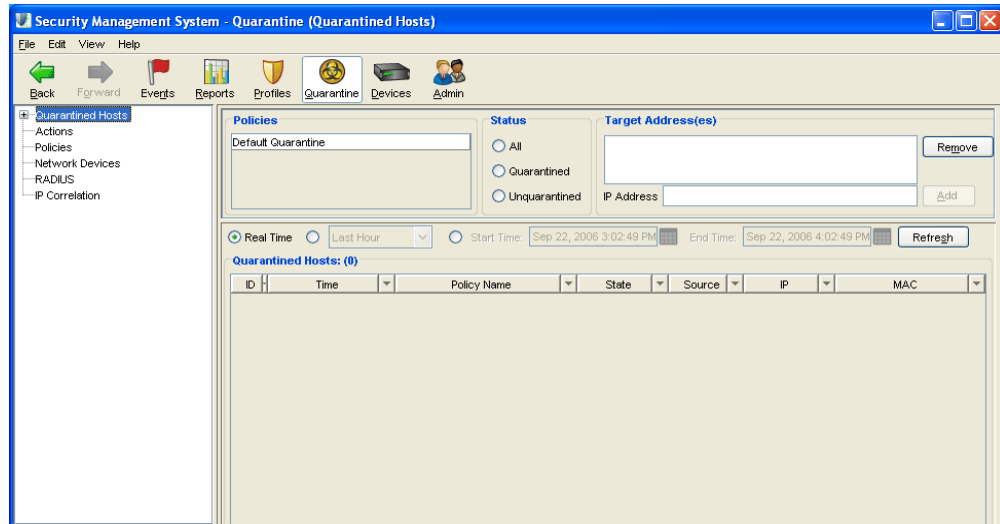
- [“Main Screen” on page 263](#)
- [“Navigational Pane” on page 264](#)
- [“Menu Bar Options” on page 265](#)

### **Main Screen**

To open the **Quarantine** screen, click the **Quarantine** button on the Toolbar. This screen is designed for managing and tuning your system's quarantine policies for mitigating malicious traffic.

The following is the **Quarantine** screen.

Figure 7 - 1: Quarantine Screen



## Navigational Pane

To access functions on the **Quarantine** screen, you can select options from the Navigation pane or Menu Bar. From the Navigation pane, the options include the following:

- **Quarantined Hosts** — Allows you to review and managed hosts that trigger quarantine policies. These hosts are effectively quarantined until manually removed or traffic no longer triggers policies.
- **Actions** — Allows you to create and maintain actions to be performed when a quarantine policy is triggered. You use these actions in quarantine policies.
- **Policies** — Allows you to create and maintain a manual quarantine policies and new policies for quarantine protection. Each policy includes quarantine actions and associated filters for detecting and blocking malicious traffic.
- **Network Devices** — Allows you to add Layer 2/Layer 3 switches and routers for use in IP Correlation and switch-level quarantine actions.
- **RADIUS** — Allows you to configure a RADIUS server for authentication. This server is used for switch-level quarantine actions.
- **IP Correlation** — Allows you to configure and test for SMS use.

Selected options display in the Main/List pane. For more information on that pane, see [“Main User Interface” on page 18.](#)

## Menu Bar Options

The available menu items for the Menu Bar differ according to the displayed screen and user access settings. Each screen provides options for the following:



**Note** The following list may change depending on the displayed screen or selected item in the main pane.

- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:
  - *New* — *Creates a new action, policy or network device with easy-to-use wizards.*
  - *Import* — *Imports an action or device script.*
  - **Create Manual Quarantine** — *Allows you to quarantine a host manually.*
  - **Logoff** — *Logs you out of the SMS*
  - **Exit** — *Closes the SMS*
- **Edit** — Provides edit options based on the currently selected and displayed screen
  - *Preferences* — *Displays the System Preferences dialog box. See [“System Preferences” on page 27.](#)*
- **View** — Displays the screens for the options listed in the Navigation Pane.
  - *Dashboard* (see [“SMS Dashboard” on page 24](#))
- **Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

## Configuring Quarantine

SMS Quarantine includes a number of configurable settings. Administrators of the SMS may set and configure the triggers and their thresholds, supply the SMS with the URL to where quarantined hosts are redirected, control the criteria by which a host is unquarantined, and so on.

When quarantine triggers, the SMS uses a quarantine policy to manage affected hosts and halted traffic streams. Each policy requires a set of actions and settings configured to best respond to malicious traffic and traffic using switches in the network topology.

**When configuring quarantine, you perform the following steps.**

1. Manage a device. The device must use V 2.2 TOS for IPS devices or V2.5 TOS for X-Series devices. See [“Managing a Device” on page 327.](#)
2. Define actions. See [“Quarantined Hosts” on page 266.](#)
3. Create a policy. See [“Policies” on page 278.](#)
4. Add or modify an IPS profile action set to use the quarantine policy. See [“Configure a Quarantine Action Set” on page 174.](#)
5. Add or modify an IPS profile to use the action set. See [“Create/Edit an Action Set” on page 172.](#)

**To configure quarantine for a switch, you perform the following steps.**

1. Manage a device. The device must use V 2.2 TOS. See [“Managing a Device” on page 327](#).
2. Configure RADIUS. See [“Configuring RADIUS” on page 285](#).
3. Add a switch. See [“Quarantined Hosts” on page 266](#).
4. Define actions. See [“Actions” on page 269](#).
5. Create a policy. See [“Policies” on page 278](#).
6. Add or modify an IPS profile action set to use the quarantine policy. See [“Configure a Quarantine Action Set” on page 174](#).

Add or modify an IPS profile to use the action set. See [“Create/Edit an Action Set” on page 172](#).

## Quarantined Hosts

This section contains the following topics:

- [“Monitoring Quarantined Hosts” on page 268](#)
- [“Quarantine Events” on page 269](#)

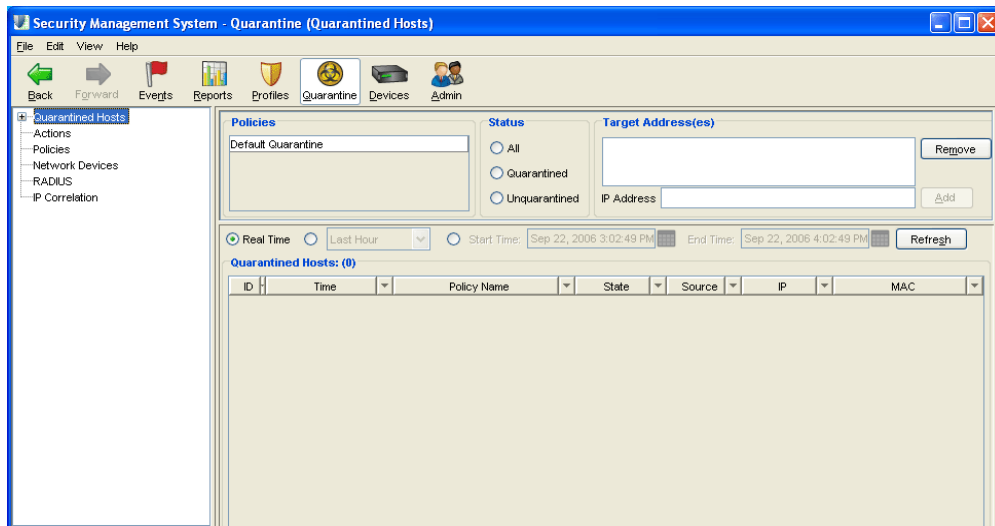
The system monitors traffic for malicious attacks based on SMS Quarantine policies. When traffic matches a filter with an associated quarantine policy, the actions are enacted against the host. The Quarantined Hosts table is where Quarantine actions for IPS and SMS actions are tracked. All quarantined hosts display on the Quarantined Hosts screen.

The quarantined Hosts screen is divided into two areas:

- **Search** — The top area contains search criteria options where you can perform queries to display, search, and unquarantined hosts.
- **Quarantine Hosts Table** — The bottom portion of the screen displays the Quarantined Hosts table, which is where Quarantine actions for IPS and SMS actions are tracked.

The following is the **Quarantined Hosts** screen:

Figure 7 - 2: Quarantined Hosts Screen



Search criteria include the following items

- **Policies** — Quarantine policies
- **Status** — Quarantine status
- **Targeted Addresses(es)** — Specific IP address, address range, netmask, or CIDR
- **Time Ranges** — real time, prescribed time intervals or user-selected time range

As you search for entries, displayed hosts may have one of the following quarantine states:

- **Initial** — the associated policy has just fired and updated the host list and will process to Quarantined.
- **Quarantined** — The host is quarantined. To remove the host from quarantine, right-click the entry and select the unquarantine option. The entry changes to the Unquarantine Requested state.
- **Unquarantined** — The host has been removed from quarantine. This entry will remain in the list until the database entries clear it or a year passes. Settings for the quarantine database are available through [“Database Administration” on page 454](#).

The source of the Quarantine event include the following items:

- **User** — A user-initiated action, whether it is a manual quarantine or an unquarantine request, on an existing host.
- **IPS** — The IPS has initiated a change in status on the policy. This is observed when dealing with SMS Quarantine policies that execute an IPS Quarantine action. The IPS has quarantined the host and put them into the listed status.
- **Policy** — A SMS policy threshold violation has resulted in the host becoming quarantined. An expire of the trigger results in the host becoming unquarantined.
- **SNMP Agent** — NMS trap listing

You can perform the following tasks:

- [“Search Quarantined Hosts” on page 268](#)
- [“Unquarantine a Host” on page 268](#)
- [“View Quarantine Events by Hosts” on page 269](#)

## Monitoring Quarantined Hosts

Carefully monitoring of quarantined hosts allows you to isolate and manage threats to your network. The Quarantine Hosts area provides a convenient area for monitoring the status of systems in your network including any policies that are associated with those systems.

You can perform the following tasks:

- [“Search Quarantined Hosts” on page 268](#)
- [“Unquarantine a Host” on page 268](#)

### How To: Search Quarantined Hosts

1. On the Quarantine navigation pane, click Quarantined Hosts.
2. From the Policies area, select one or more Quarantine policies.
3. For Status, select from the following: All, Quarantined, or Unquarantined.
4. For Target Address(es), enter and add an IP address to include in your search.
5. Select the Real Time option or select a Time Range, by a specific start and end time or by the last amount of time from the drop-down menu.
6. Click Refresh.

### How To: Unquarantine a Host

1. Search for a host. See [“Search Quarantined Hosts” on page 268](#).
2. Select a host entry in the list pane.
3. Right-click and select the unquarantine option or click **Unquarantine**.

## Quarantine Events

The Events section provides an area for monitoring Quarantine events for a specific host. This area tracks a specific host, when it enters quarantines, the type of action that was enforced and the associated details.

You can perform the following task:

- [“View Quarantine Events by Hosts” on page 269](#)

### How To: View Quarantine Events by Hosts

1. Search for a host. See [“Search Quarantined Hosts” on page 268](#).
2. Double-click a host entry in the list pane or select the entry and click **Details**.
3. Record the **Host ID** number.

## Actions

This section contains the following topics:

- [“Types of Actions” on page 269](#)
- [“Editing Default Actions” on page 270](#)
- [“Defining Actions” on page 272](#)

Actions are the instructions the system follows when a host's traffic triggers a quarantine policy.

The SMS provides a hard-coded IPS Quarantine action. This action performs traffic management as well as remediate 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.

## Types of Actions

Action Types include the following:

- [Default Actions](#)
- [Customized Actions](#)
- [Switch Actions](#)

## Default Actions

Every IPS contains a special *hidden* Quarantine action set that the SMS Quarantine application manages. The SMS also includes a default Switch Disconnect Action that is designed to work with Quarantine policies that apply to switches.

- **Switch Disconnect Action** — works dynamically based on IP correlation. You can edit the name for this action set, but cannot make any other changes.
- **IPS Quarantine Action** — describes how the IPS behaves when the SMS adds an IP to its list of quarantined IP addresses. You can edit this action, but cannot create a new IPS Quarantine action.

## Customized Actions

- **Syslog** — Sends a message to a syslog server when the policy is triggered.
- **Email** — Sends an email when the policy is triggered.
- **Web** — Performs an HTTP GET on a URL
- **SNMP Trap** — Enacts an SNMP Trap for the host traffic when the policy is triggered.

## Switch Actions

- **Switch Disconnect** — Instructs the switch to momentarily disable the port, which causes the host to reauthenticate. On reauthentication, access is rejected by the RADIUS server.
- **NMS Trap** — Integration with NMS to use an NMS Trap for quarantined hosts.
- **Move Quarantine Host onto a VLAN** — Moves a host triggered for quarantine onto a VLAN.



**Note** Switch policies can use all of the available action types including Default Actions, Customized Actions and Switch Actions.

## Editing Default Actions

For default actions, you can perform the following edit tasks:

- [“Edit the Switch Disconnect Action” on page 270](#)
- [“Implement the Switch Disconnect Action” on page 271](#)
- [“Edit the IPS Default Quarantine Action” on page 271](#)

### How To: Edit the Switch Disconnect Action

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, select the **Switch Disconnect** entry from the **Quarantine** action list and click **Edit**. The Quarantine Action setup wizard displays.
3. If you want to customize the **Action Name**, you can edit the name, but cannot make any other changes.
4. If you want to read special instructions for this action, select **Implementation** from the wizard navigation pane.
5. Click **OK**.



### How To: Implement the Switch Disconnect Action

1. This action must be listed in the **Actions** section of one or more Quarantine Policies. See [“Policies” on page 278](#).
2. Ingress switches must be identified in the **Network Devices** area of the Quarantine application. These are the switches that have quarantinable endstations plugged into them.
3. The SMS Quarantine RADIUS proxy must be configured and operating. The proxy is set up in the **RADIUS** section of the Quarantine application. See [“Radius” on page 285](#).
4. Every port on an ingress switch that should participate in a Quarantine activity must be configured to use RADA, 802.1x, or MAC authentication, and must be using the SMS RADIUS proxy as its authorization source.
5. Some means for performing IP Correlation must be configured. IP Correlation is the means by which attacking IP addresses discovered by an IPS are mapped the ingress switch and MAC address of the attacker. See [“IP Correlation” on page 286](#).

### How To: Edit the IPS Default Quarantine Action

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, select the **IPS Quarantine** entry from the **Quarantine** action list and click **Edit**. The Quarantine Action setup wizard displays.
3. If you want to customize the **Action Name**, you can edit the name, but cannot make any changes to the action type.
4. Select **IP Quarantine** from the wizard navigation pane.
5. For **Web Requests**, select the action to **Block** or **Redirect** to a web server. If you select **Redirect**, enter a web site to access.
6. For all **Other Traffic**, select **Block** or **Permit** for the response to host traffic.
7. For **Thresholds**, enter the **Hit Count** (1 to 10,000 hits) and **Period** (1 to 60 minutes).
8. To allow hosts to access specific sites, add a site to the **Quarantined Access** table:
9. Click **New** to create a new listing or select an existing listing and click **Edit**.
10. If desired, enter a **Name**.
11. Enter the **Address** and select **CIDR**, **IP Mask**, or **Any IP**.
12. Click **OK**.
13. If you want to test this action, click **Test**.
14. On the **Edit Quarantine Action (IPS Quarantine)** screen, click **OK**.

## Defining Actions

You can define the following actions with the Quarantine screen:

- [“Create/Edit a Syslog Action” on page 272](#)
- [“Implement a Syslog Action” on page 273](#)
- [“Create/Edit an Email Action” on page 273](#)
- [“Implement an Email Action” on page 273](#)
- [“Create/Edit a Web Action” on page 275](#)
- [“Implement a Web Action” on page 276](#)
- [“Create/Edit a NMS Trap Action” on page 274](#)
- [“Create/Edit a SNMP Trap Action” on page 276](#)
- [“Create/Edit a Move Quarantined Host onto a VLAN action” on page 277](#)
- [“Implement a Move Quarantined Host onto a VLAN Action” on page 277](#)

### How To: Create/Edit a Syslog Action



**Note** Before you set up a Syslog action, UDP Syslog agent must be running on the Syslog destination IP and port configured for this action.

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop-down menu, select **Syslog**.
6. Click **Next** or select **Syslog Settings** from the wizard navigation pane.
7. Specify the destination for the log message by completing the following information:
  - **IP Address of the Server** (UDP)
  - **Port** (default setting is 514)
  - **Facility**
8. If you want to test this action, click **Test**.
9. If you want to read special instructions for this action, click **Next** or select **Implementation** from the wizard navigation pane.
10. Click **Finish** or **OK** to complete your setup.

### How To: Implement a Syslog Action

1. This action must be listed in the **Actions** section of one or more Quarantine Policies. See [“Policies” on page 278](#).
2. UDP Syslog agent must be running on the Syslog destination IP and port configured for this action.
3. You can test this action to check for basic network connectivity between the SMS and the remote agent. See [“Create/Edit a Syslog Action” on page 272](#).

### How To: Create/Edit an Email Action



**Note** Before you set up a Syslog 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. See [“SMS Server Properties” on page 460](#).

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop-down menu, select **Email**
6. Click **Next** or select **Email Settings** from the wizard navigation pane.
7. Enter the following information:
8. **From** — Enter the email address where the notifying email originates (generally a SMS specific email alias).
9. **Reply To** — Enter the email address where replies are to be sent
10. For the **To** section, click the **Add** button and enter the email address or addresses where syslog email notices will be sent. To enter multiple email addresses, separate entries with a comma.
11. If you want to test this action, click **Test**.
12. If you want to read special instructions for this action, click **Next** or select **Implementation** from the wizard navigation pane.
13. Click **Finish** or **OK** to complete your setup.

### How To: Implement an Email Action

1. This action must be listed in the **Actions** section of one or more Quarantine Policies. See [“Policies” on page 278](#).
2. The system SMTP Server must be configured under the **Admin > Server Properties > Network** section of the SMS application. The system reply-to and from fields will be used if none are configured in this Email action. See [“SMS Server Properties” on page 460](#).

3. You can test this action to check for basic network connectivity between the SMS and the SMTP server. See [“Create/Edit a NMS Trap Action” on page 274](#).

#### How To: Create/Edit a NMS Trap Action



**Note** NMS (Network Management System) Trap sends out an SNMP Trap to an NMS as well as performing other quarantine 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

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop down menu, select **NMS Trap**.
6. Click **Next** or select **NMS Trap Destination** from the wizard navigation pane.
7. Specify the **NMS IP address** and **Destination Port**.
8. Click **Next** or select **Primary Action Settings** from the wizard navigation pane.
9. Select the **Primary Action type** from the drop-down list.
  - **RADIUS Reauthentication**
  - **VLAN isolation**
  - **Disable port**
10. Configure the setting for the action type you requested. If required, specify NAM Rule, Active Directory Group, Quarantine VLAN settings.
11. Select any of the following options that you want this action to perform:
  - **Perform VLAN check** — checks for VLAN preconditions before attempting this action.
  - **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.
12. Click **Next** or select **Secondary Action Settings** from the wizard navigation pane. Specify the second action to attempt should the first action fails. Refer to instructions outlined in steps 10 and 11.
13. Click **Next** or select **Final Action Settings** from the wizard navigation pane. Specify the final action to attempt should the first two actions fail. Refer to instructions outlined in steps 10 and 11.
14. If you want to test this action, click **Test**.
15. Click **Finish** or **OK** to complete your setup.

## How To: Create/Edit a Web Action

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop-down menu, select **Web**.
6. Click **Next** or select **Host Configuration** from the wizard navigation pane.
7. In the **Host Configuration** dialog, enter the following information to specify the destination for the HTTP/HTTPS message.

*If server is not specified, then the URL must be fully specified (for example, `http://xyzyzy.com/page`).*

### **Host Settings** section

- **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**.
- Enter **Username**.
- Enter **Password**.

8. Click **Next** or select **Proxy Settings** from the wizard navigation pane.
9. In the **Proxy Settings** dialog:

### **Proxy Host Settings** section

- To use Proxy, select the **Use Proxy Host** check box.
- Enter **Proxy Host**.
- Enter **Proxy Port** number.

### **Host Authentication** section

- For Host Authentication, select the **Use Authentication** check box.
- Enter **Username**.
- Enter **Password**.

10. If you want to test this action, click **Test**.
11. If you want to read special instructions for this action, click **Next** or select **Implementation** from the wizard navigation pane.
12. Click **Finish** or **OK** to complete your setup.

### How To: Implement a Web Action

1. This action must be listed in the **Actions** section of one or more Quarantine Policies. See [“Policies” on page 278](#).
2. An HTTP Server must be running on the HTTP destination IP and port configured for this action.
3. You can Test this action to check for basic network connectivity between the SMS and the remote server. See [“Create/Edit a Web Action” on page 275](#).

### How To: Create/Edit a SNMP Trap Action

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop-down menu, select **SNMP Trap**.
6. Click **Next** or select **Trap Destination** from the wizard navigation pane.
7. Specify the trap destination **Host** and **Port** settings.
8. If you want the SMS to send a trap on unquarantine, select that option. Otherwise, deselect the Trap option.
9. Click **Next** or select **SNMP Settings** from the wizard navigation pane.
10. Specify basic SNMP trap settings. The fields in the Authentication group are only available for SNMP v3.
  - **SNMP Version** — version of SNMP to use when sending this trap.
  - **Community** — group to which the destination host belongs. Value is only valid for SNMP v2.
  - **OID** — object identifier (OID) that defines this trap. Numeric format is required.
  - **Auth Protocol** — protocol to use for authentication. This value is only valid for SNMP v3.
  - **User Name** — user login name to use for authentication. Will default to 'private' for a v3 trap. Value is only used for SNMP v3.
  - **Password** — user login password to use for authentication. Value is only valid for SNMP v3.
  - **Privacy Password** — 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.
11. If you want to test this action, click **Test**.
12. If you want to read special instructions for this action, click **Next** or select **Implementation** from the wizard navigation pane.
13. Click **Finish** or **OK** to complete your setup.

### How To: Create/Edit a Move Quarantined Host onto a VLAN action

1. On the **Quarantine** navigation pane, click **Actions**.
2. In the **Actions** screen, click **New** to create a new Quarantine action or select an existing action entry and click **Edit**.
3. The **Quarantine Action** setup wizard displays.
4. Specify a name for the action.
5. From the **Action Type** drop-down menu, select **Move Quarantined Host onto a VLAN**.
6. Click **Next** or select **VLAN Name** from the wizard navigation pane.
7. Specify the VLAN that should be used for quarantine, typically an isolated VLAN with remediation services.
  - **VLAN Name** — named VLAN for use by network equipment that recognizes names. The actual interpretation of the name is configured on each device.
  - **VLAN ID** — numeric tag, assumed to be 802.1Q compatible that has a max value of 4095.
8. If you want to test this action, click **Test**.
9. If you want to read special instructions for this action, click **Next** or select **Implementation** from the wizard navigation pane.
10. Click **Finish** or **OK** to complete your setup.

### How To: Implement a Move Quarantined Host onto a VLAN Action

1. This action must be listed in the **Actions** section of one or more Quarantine Policies. See [“Policies” on page 278](#).
2. Ingress switches must be identified in the **Network Devices** area of the Quarantine application. These are the switches that have quarantinable endstations plugged into them.
3. The SMS Quarantine RADIUS proxy must be configured and operating. The proxy is set up in the **RADIUS** section of the Quarantine application. See [“Radius” on page 285](#).
4. Every port on an ingress switch that should participate in a Quarantine activity must be configured to use RADA, 802.1x, or MAC authentication, and must be using the SMS RADIUS proxy as its authorization source.
5. Some means for performing IP Correlation must be configured. IP Correlation is the means by which attacking IP addresses discovered by an IPS are mapped the ingress switch and MAC address of the attacker. See [“IP Correlation” on page 286](#).

# Policies

This section contains the following topics:

- [“Policy Setup Options” on page 278](#)
- [“Default Quarantine Policy” on page 280](#)
- [“Manual Quarantine” on page 281](#)
- [“Creating a Quarantine Policy” on page 282](#)

A quarantine policy defines the detection and response of the SMS when managing potential and determined threats against a network. Each policy may include segments from multiple managed devices, one of each type of action you created, and the IPS Quarantine action.

The system provides a **Default Quarantine Policy**. This policy enacts when you manually quarantine a host. See [“Quarantined Hosts” on page 266](#).

The method of configuring a Quarantine Policy on an IPS segment is based on Quarantine action. You create an action set with the SMS action equal to the quarantine 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 Quarantine.

## Policy Setup Options

The following policy setup options are available when setting up or editing a Quarantine policy:

- [Policy Initiation](#)
- [Policy Remediation Communication](#)
- [Inclusions and Exclusions](#)
- [IP Correlation and Thresholding](#)
- [Actions](#)

## Policy Initiation

An SMS Quarantine Policy controls how endstations move in and out of quarantine. A policy defines a number of Actions that occur when an endstation is quarantined. These actions can potentially interact with a variety of networking equipment, including NMS and ingress switches, to enforce a Quarantine.



The Policy also handles reversing these actions when Quarantine ends. Quarantine can be initiated by the following mechanisms:

- By correlating the event stream from a subset of managed IPSes, and quarantining when threshold criteria are met.
- Manually, by choosing **File > Create Manual Quarantine** and entering an IP address to be quarantined.
- 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 Quarantine.



**Note** SMS Policies that escalate the IPS Quarantine should be limited to one SMS Quarantine policy,



**Note** If there is already a host in SMS Quarantine and that host shares the same identity with an incoming IPS Quarantine escalation, the SMS does NOT escalate the IPS Quarantine into a new Quarantine event.

## Policy Remediation Communication

Quarantine typically is ended when the quarantined endstation is remediated. This act must be communicated to the SMS using the same set of mechanisms that are used for quarantine initiation - manually, or by an external NMS, etc. Optionally, a timeout can be configured to automatically end quarantine when a certain amount of time has passed since the last quarantine request for a given endstation.

## Inclusions and Exclusions

A Quarantine policy also contains a list of hosts/networks with the following classifications:

- **Allow Quarantine** — specifies the IP address ranges and subnets that are to be eligible for quarantine.
- **Never Quarantine** — specifies the IP address ranges and subnets that will ever be quarantined.

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 quarantine 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 IPSes and correlates them using the attacker's IP address. Hit counts are qualified and accumulated within a sliding time window (the Threshold

Period). Quarantine 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 is eligible for quarantine 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 endstation is Quarantined using this Policy, zero or more Actions are executed to affect the quarantine. 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.

## Default Quarantine Policy

### How To: Edit Default Quarantine Policy

1. On the **Quarantine** navigation pane, click **Policies**.
2. In the **Policies** screen, select the Default Quarantine entry from the Quarantine Policies list and click **Edit**. The **Quarantine Policy** setup wizard displays.
3. On the **Initiation and Timeout** screen, specify the mechanism to use to initiate the policy. See [“Policy Initiation” on page 278](#).
4. If you want to set the timeout option, select the **Enable Automatic Timeout** check box and enter a time in minutes. Setting this option automatically releases an endstation from Quarantined after the prescribed time limit even if remediation has not occurred.
5. Select **Inclusions and Exclusions** from the wizard navigation pane.
6. On the **Inclusions and Exclusions** screen, specify the hosts/networks to **Allow** or **Never Quarantine**. See [“Inclusions and Exclusions” on page 279](#).
7. Use the arrow buttons located at the end of each field to add an existing **Named Resource** or to create a new **Named Resource**.
8. Select **Actions** from the wizard navigation pane.
9. The **Actions** screen list the actions that are associated with the policy and the following information:
  - Priority —the order the actions should be performed
  - Action — name assigned to the action that you created. See [“Quarantine Events” on page 269](#).
  - Condition — trigger for running the action. This option is set when a new action is added to the Quarantine 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.

10. In the **Actions** screen, click **Add** to add a new Quarantine action or select an existing action entry and click **Edit**. The **Quarantine Action** screen displays.
11. Select an action to add from the drop down menu. You created these action in the Action screen for Quarantine. When adding additional actions, you can create dependences between the actions:
  - Select an action to add.
  - Select an option: success on or failure on.
  - Select the action to connect for dependency.

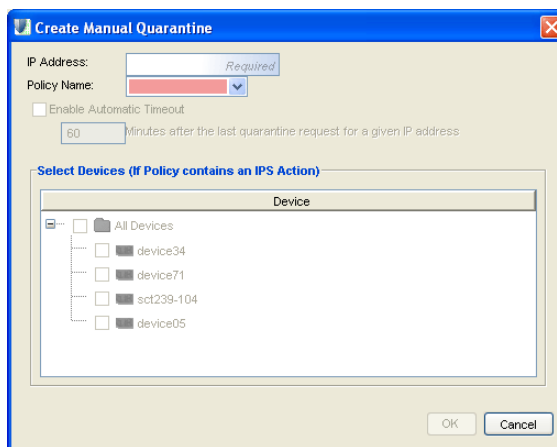
For example, the added action called Email Admin (email type) could have a dependency on the previously added action of Switch Down (switch disconnect type). In this situation, when the switch went down, the email action would send a message informing the network administrator.
12. Click **OK** to return to the setup wizard.
13. 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.
14. On the Quarantine Policy setup wizard, click **Finish** to save your settings.

## Manual Quarantine

### How To: Manually Quarantine a Host

1. On the **Quarantine** screen, select the **File -> Create Manual Quarantine** menu option. The **Create Manual Quarantine** dialog box opens.

Figure 7 - 3: Quarantine - Create Manual Quarantine Dialog Box



2. Enter an IP Address of a host to quarantine.
3. Select a Policy Name from the drop-down list. The SMS enacts this policy against the Quarantined Host.
4. If desired, select the **Enable Automatic Timeout** and specify the number of minutes the system will stay in quarantine. Setting this option automatically releases an endstation from Quarantined after the prescribed time limit even if remediation has not occurred.

5. In the Select Devices area, select **All devices** or individual devices if the policy you want to apply contains an IPS action.
6. Click **OK**.

## Creating a Quarantine Policy

### How To: Create/Edit a new Policy

Creating a Quarantine policy involves setting up various options that determine what actions are to be taken.

1. On the **Quarantine** navigation pane, click **Policies**.
2. In the Quarantines **Policies** screen, click **New** or select an existing policy entry from the Quarantine Policies list and click **Edit**. The **Quarantine Policy** setup wizard displays.
3. On the **Initiation and Timeout** screen,
  - Specify a Policy name
  - Specify the mechanism to use to initiate the policy. See [“Policy Initiation” on page 278](#).
  - If you want to set the timeout option, select the **Enable Automatic Timeout** check box and enter a time in minutes. Setting this option automatically releases an endstation from Quarantined after the prescribed time limit even if remediation has not occurred.
  - Click **Next** or select **Inclusions and Exclusions** from the wizard navigation pane.
4. On the **Inclusions and Exclusions** screen, specify the hosts/networks to **Allow** or **Never Quarantine**. See [“Inclusions and Exclusions” on page 279](#).
  - Use the arrow buttons located at the end of each field to add an existing **Named Resource** or to create a new **Named Resource**.
  - Click **Next** or select **Correlation and Thresholding** from wizard navigation pane.
5. For Correlation and Thresholding, enter settings for the following:
 

**Automatic Quarantine 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 quarantine 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.
6. Select **Actions** from the wizard navigation pane.

7. The **Actions** screen list the actions that are associated with the policy and the following information:
  - Priority —the order the actions should be performed
  - Action — name assigned to the action that you created. See [“Quarantine Events” on page 269](#).
  - Condition — trigger for running the action. This option is set when a new action is added to the Quarantine 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.
8. In the **Actions** screen, click **Add** to add a new Quarantine action or select an existing action entry and click **Edit**. The **Quarantine Action** screen displays.
9. Select an action to add from the drop down menu. You created these action in the Action screen for Quarantine. When adding additional actions, you can create dependences between the actions:
  - Select an action to add.
  - Select an option: success on or failure on.
  - 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.
10. Click **OK** to return to the setup wizard.
11. 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.
12. On the Quarantine Policy setup wizard, click **Finish** to save your settings.

## Network Devices

SMS Quarantine supports a number of hardware infrastructure elements. These elements work off of one or both of two separate authentication methods, RADA and 802.1x.

See also [“Adding a Switch” on page 283](#).

### Adding a Switch

Some network architectures employ switches for managing and maintaining traffic. Typical quarantine 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 endstations. Edge routers should have no other layer-three devices between them and endstations, and should be able to see the true MAC address of endstations.

The SMS currently supports the following switch models:

- Cisco 6500 (Cat OS 8.0 to 10.0)
- Generic Edge Router (SNMP v1/2c)
- 3Com4400 (5.0 to 6.0)
- 3Com 5500 (3.0 to 4.0),
- 3Com 7750 (1.0 to 10.0)

With each successive release, the list of supported switch models will expand.

You can perform the following tasks:

[“Add/Edit a Switch” on page 284.](#)

#### How To: Add/Edit a Switch

1. In the **Quarantine** navigation pane, click **Network Devices**.
2. Click **New**, or select an existing entry in the **Network Devices** list and click **Edit**. The **Quarantine Network Equipment Wizard** displays.
3. In 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 **Next** or select the **Configuration** or **Authentication** screen from the wizard navigation pane.
5. Depending upon the type of switch and required authentication, a **Configuration** or **Authentication** screen will display.
6. For the **Authentication** screen, follow the on-screen instructions and specify any or all of the following authentication information that applies to the switch:
  - Username and Password — Enter the user name and password needed to manage this device
  - Enable Password — Select if needed.
  - Read Community and Write Community — The default value for Read Community is public and Write Community is private. If these settings differ on the switch, change them here.
  - Prefer VLAN Symbolic Name over ID — If want to use VLAN symbolic Name over ID, select the checkbox.
  - Use this device for IP to MAC Correlation
7. If the switch requires configuration, a **Configuration** screen displays that contains configuration entries in addition to authentication entries. Follow the on-screen instructions.



**Note** The 3Com 7750 and 3Com 5500 switches support RFC1213 IP Correlation. To use IP Correlation with these switches, be sure to select the checkbox next to **Use this device for IP to MAC Correlation (ARP, via RFC 1213)** on the configuration screen for your particular 3Com switch.

8. If you want to test this action, click **Test**.
9. Click **Finish** or **OK**.

# Radius

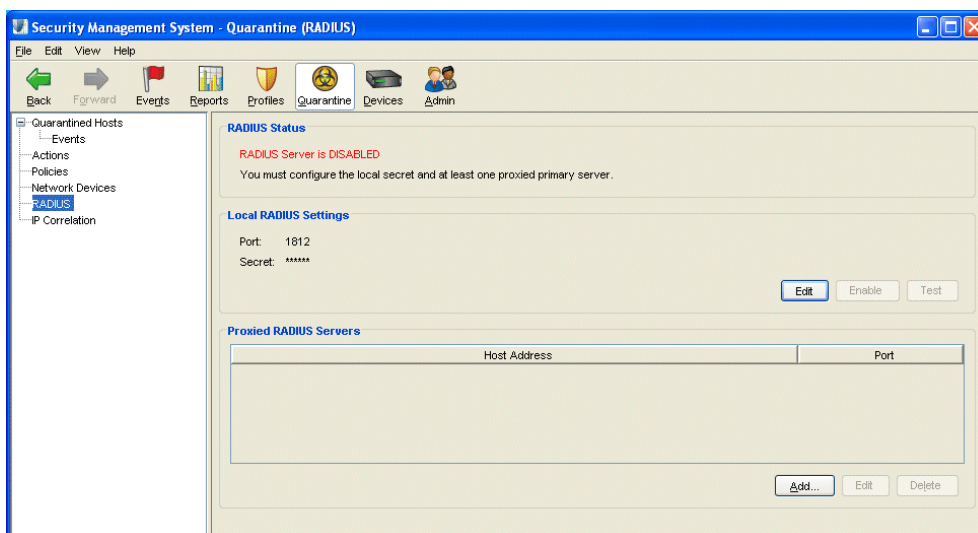
## Configuring RADIUS

RADIUS is an authentication application used for user accounts and access. When creating policies for switches, you should configure the RADIUS server. SMS requires settings entered when configuring the RADIUS software. For this configuration, you need the IP address, account, secrets, and primary/secondary server information.

After configuring RADIUS, you must point the RADIUS authentication to the SMS Server IP address.

The following is the **Quarantine - RADIUS** screen:

Figure 7 - 4: Quarantine - RADIUS Screen



### How To: Configure RADIUS

1. In the **Quarantine** navigation pane, click **RADIUS**.
2. In the **Local RADIUS Settings** area, click **Edit**.
3. In **Local RADIUS Settings** screen, enter the authentication port and secret, and then click **OK**. You configured the secret answer in your RADIUS software.
4. In the **Proxied RADIUS Servers** area, click **Add** to add a new server or select an existing server entry and click **Edit**.
5. In the **Proxied RADIUS Server** screen, enter the host IP address, authentication port, and secret and then click **OK**.



**Note** After configuring RADIUS, you must point the RADIUS authentication to the SMS Server IP address.

6. To enable the local setting, click **Enable**.
7. After RADIUS is configured and enabled, you can test your configuration by clicking **Test**.

## IP Correlation

This section contains the following topics:

- [Configuring IP Correlation](#)
- [IP Correlation Web Services](#)
- [Testing 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 quarantining hosts. This setup is required for SMS Quarantine to work with non-IPS infrastructure equipment such as switches and other network access points.

You can perform the following tasks:

- [Add/Edit Network Mapping](#)
- [Add/Edit Web Services](#)
- [Control Web Service Precedence](#)
- [Perform a Test](#)

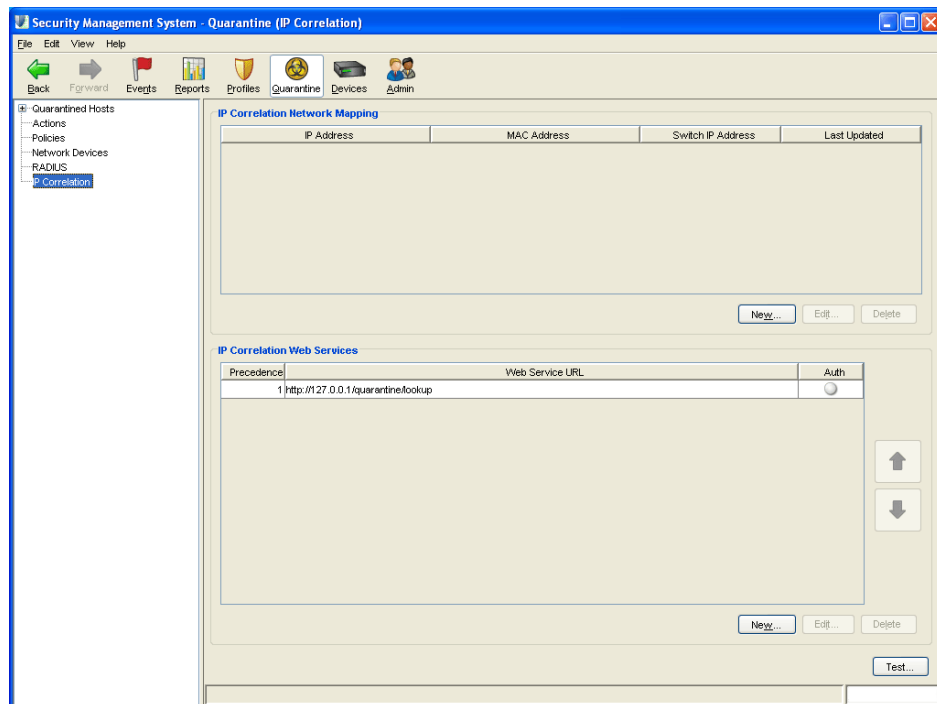


## Configuring IP Correlation

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 endstation to its IP address is a requirement for SMS Quarantine to properly control access on a host. The SMS watches events from an IPS and then using IP Correlation finds the endstation responsible for those events. the SMS uses this information to initiate Quarantine.

The following is the **Quarantine - IP Correlation** screen:

Figure 7 - 5: Quarantine - IP Correlation Screen



The SMS provides the following configuration options for IP Correlation:

- [Network Mapping Using the GUI](#)
- [Network Mapping - bulk Load via Service Mode](#)
- [IP Correlation Configuration - RFC1213](#)
- [IP Correlation Configuration - 3Com Network Director or 3Com Enterprise Management Suite](#)
- [IP Correlation Configuration - External Web API](#)

## Network Mapping Using the GUI

### How To: Add/Edit Network Mapping

Use the GUI to add network mappings one entry at a time.

1. In the **Quarantine** navigation pane, click **IP Correlation**. The **Quarantine - IP Correlation** screen displays.
2. In the **IP Correlation Network Mapping** area, click **New**, or select an existing entry in the in the list and click **Edit**. The **IP Correlation** dialog displays.
3. Specify the following information:
  - IP Address
  - MAC Address (in XX:XX:XX:XX:XX:XX format)



**Note** If you enter an existing MAC address, it will not validate.

4. Click **OK** to return to the **Quarantine - IP Correlation** screen.

### 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 db.

### IP Correlation Configuration - RFC1213

RFC1213 Network Identification lookup is configured under the **Quarantine -> 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 checkbox 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 endstation for the IP you are attempting to quarantine.

### 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

A specification was written that allows an advanced user to write their own external IP Correlation engine. IP Correlation Web Services allow an advanced user to direct the SMS to that interface using a Web API. To be called upon as a source for IP Correlation, the URL for this API must point to the web page interface where the user is hosting this lookup agent and must be entered into the IP Correlation Web Services table. See the Web API IP Correlation documentation for instructions on how to build an External Web API.

## 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 is checked by adjusting the precedence of each Web Service URL. 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 289](#)
- [“Control Web Service Precedence” on page 289](#)

### How To: Add/Edit Web Services

1. In the **Quarantine** navigation pane, click **IP Correlation**. The **Quarantine - 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 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** to return to the **Quarantine - IP Correlation** screen.

### How To: Control Web Service Precedence

1. In the **Quarantine** navigation pane, click **IP Correlation**. The **Quarantine - 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 the Web API IP Correlation documentation), but the above are the requirements for SMS Quarantine via an infrastructure action.

### How To: Perform a Test

1. In the **Quarantine** navigation pane, click **IP Correlation**. The **Quarantine - IP Correlation** screen displays.
2. Click **Test**. The **IP Correlation Test** dialog box opens.

Figure 7 - 6: IP Correlation Test Dialog Box

The screenshot shows a dialog box titled "IP Correlation Test". It contains a "Test Parameters" section with a "Correlation Method" dropdown set to "IPLOOKUP". There are two radio buttons: "IP Address" (selected) and "MAC Address" (unselected). Below these are two text input fields. A "Query" button is located to the right of the input fields. The "Results" section contains a table with two columns: "Attribute" and "Value". At the bottom of the dialog, there is a "Query Executed" field showing the URL "http://127.0.0.1/quarantine/lookup?METHOD=IPLOOKUP&IP=" and a "Close" button.

3. Select the **Correlation Method**
4. Select the type and enter an address: IP or MAC. Select appropriate to the method.
5. Click **Query**. The results of the query display in the results section.
6. Click **Close** to close the dialog and return to the **IP Correlation** screen.

# Managing Manual Quarantine Policy

The SMS supports manually quarantining hosts through the Quarantine screen. When you manually quarantine a host, the SMS enacts the Manual Quarantine policy on the traffic flow.

When you edit and enhance Manual Quarantine, you do the following:

1. Add policy actions. See [“Quarantined Hosts” on page 266](#).
2. Edit the Manual Quarantine policy. See [“Edit Default Quarantine Policy” on page 280](#).
3. After modifying the policy, you can begin to manually quarantine hosts. You need the IP address and any information regarding the devices you may want to specifically quarantine the host on. To quarantine a host manually, see [“Manually Quarantine a Host” on page 281](#).

You can perform manual quarantine by right-clicking IP addresses in generated event lists through the Events screen. You can also use the **File -> Create Manual Quarantine** menu option through the Quarantine screen. Hosts quarantined manually also display in the **Quarantined Hosts** screen.

## Managing Quarantine Through an External/3rd-Party Interface

For information on using an External/3rd-Party interface to manage Quarantine, see the Quarantine chapter of **TippingPoint SMS External Interface Guide** that is available on the Documentation CD or on the Documentation section of the Client web page.



# 8

## Devices

*The Devices screen graphically depicts TippingPoint devices, their segments, and the hosts and services on those segments. You can manage devices, update the TippingPoint operating system (TOS), and manage device/segment groups.*

### Overview

This section includes the following topics:

- [“Devices: What’s New” on page 294](#)
- [“How To Tasks” on page 298](#)
- [“Navigation and Menu Options” on page 302](#)
- [“Device Information” on page 304](#)
- [“Device Monitoring” on page 309](#)
- [“Device Management” on page 318](#)
- [“System Update” on page 328](#)
- [“TippingPoint OS” on page 332](#)
- [“Segment Groups” on page 337](#)

#### ***IPS Devices***

- [“IPS Devices: Device Configuration” on page 341](#)
- [“IPS Devices: Network Configuration” on page 366](#)
- [“IPS Devices: Event Monitoring” on page 371](#)

#### ***X-Family Devices***

- [“X-Family Devices: Device Configuration” on page 375](#)
- [“X-Family Devices: Network Configuration” on page 393](#)
- [“X-Family Devices: Security Configurations” on page 406](#)
- [“X-Family Devices: Event Monitoring” on page 423](#)

#### ***E-Series Devices***

- [“E-Series: Advanced DDoS” on page 427](#)

The **Devices** screen provides a dynamic view of your entire system. Through this screen, you can centrally monitor and manage the TippingPoint devices on your system. When you assume management of a device, you can control IPS networking configuration, filters and customizations, and distribution of filters and software.

Management of device includes adding it to the system, combining devices into related groups, unmanaging them temporarily, or deleting them from your system. You can also monitor the traffic processing, health, and hardware status on each device and its segments.



**Note** To manage devices, you must have Super User or Administrator authority. You can monitor devices with Administrator or Super User authority. Operators can view device information if granted permission by a Super User. Administrators can manage devices if granted permission by a Super User. For more information about user authority, see [“In the Upgrade License section, enter the New License Key, and then click Apply. User Administration” on page 445.](#)

This screen also enables you to download and install updates of the TippingPoint operating system (TOS). The TOS is the operating system used directed by devices. The LSM and SMS applications access the TOS to manage and maintain devices on your network.

## Devices: What's New

This section outlines the following major changes for the current SMS release:

- [Virtual Segments](#)
- [Bridge Mode for X-Family Devices](#)
- [Adding Offline X-Family Devices](#)
- [Viewing TOS Information For X-Family Devices](#)
- [Remote Syslog](#)
- [IPSec Security Association Setup](#)
- [DDoS Preferences](#)
- [Management Port Settings](#)
- [Interface Changes](#)

### Virtual Segments

Virtual segments were introduced in the SMS V 2.5 for X-Family devices. SMS V2.5.1 adds virtual segment support for the IPS devices. Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events. See [“IPS Devices: Network Configuration” on page 366.](#)

### Bridge Mode for X-Family Devices

A new bridge mode option is available for the X-Family devices. This option is available through the X-Family device **Network Configuration** —> **IP Interfaces** —> **IP Interface - External** screen.



### **Description**

X-Family devices used a proxy ARP mechanism in order to allow clients on different security zones, connected to the same virtual interface, to talk to one another. One major drawback of this is that it's impossible to run multiple IP subnets over a set of zones in a transparent virtual interface without configuring the X-Family device with appropriate routes for each subnet. This requirement causes major problems in deployments where the transparent mode device is spliced between 2 OSPF routers.

In the 2.5 and above releases, you can choose between using the old proxy ARP mechanism or a new bridge mode. In bridge mode, the X-Family devices implement a software bridge to transparently connect security zones assigned to the same virtual interface.

### **How It Works**

When in the bridge mode, the X-Family device learns MAC addresses on ports, and forwards traffic within the transparent virtual interface by destination MAC address to the appropriate port, or floods the packet if the address had not been previously learnt. In bridge mode, the X family device is truly transparent in that it no longer proxies for hosts and it no longer requires configuration of IP routes to bridge traffic.

The X family device does not forward spanning tree packets when in bridge mode. The X family device will still operate normally as a router and VPN terminator when in bridge mode. Currently the High Availability feature is unavailable if bridge mode is enabled.

## **Adding Offline X-Family Devices**

The SMS now supports embedded offline X-Family device configuration in the serial numbers file. See [“Adding Offline X-Family Devices” on page 320](#).

## **Viewing TOS Information For X-Family Devices**

For version 2.5.1 and above, the SMS displays an **X** before the TippingPoint Operating System (TOS) when viewing device information. See [“Devices Screen” on page 302](#).

## **Remote Syslog**

Five new log formats were added. New logs include:

- SMS 2.5 Syslog Format
- X-Family Firewall Block
- X-Family Firewall Session
- SMS System
- SMS Audit

For the 2.5 event format, four fields were added and two were removed. New log fields include:

- Source Zone Name
- Destination Zone Name
- Incoming Physical Port
- VLAN ID

Deleted fields include:

- Device Slot — no longer valid for 2.5 devices
- Device Segment — no longer valid for 2.5 devices

For information on setting up syslog, see [“Management Information” on page 460](#).

## IPSec Security Association Setup

In the **IPSec Security Association Setup** (IKE Phase 1 Setup) screen, the Automatically connect phase 2 field is new. Selecting this option allows phase 2 to be established even if no traffic is sent from that end of the tunnel. See [“IKE Proposals Tab” on page 415](#).

## DDoS Preferences

In the **Device Configuration (TSE Settings)** screen, the following fields are new:

- 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 [“DDoS Preferences” on page 428](#).

## Management Port Settings

The following port settings can now be changed using the Device Configuration Wizard:

- **Auto negotiation:** Enable/Disable
- **Line Speed:** 100 Mbps, 10 Mbps
- **Duplex Mode:** Full/half

See [“Changing Management Port Settings” on page 325](#).

## Interface Changes

For 2.5 and above, the following interface changes were made:

- [Device Groups](#)
- [Device Segments](#)
- [Device Filter Settings](#)
- [Device Configuration](#)
- [Device Configuration/Device Events](#)
- [Device Configuration/Reset Filters](#)

### Device Groups

- The Device configuration information is in new location.
- The **All Devices** > device > **Device Configuration** sub-menu was moved. The new location is **All Devices** > **Member Summary**. The sub-menu items are displayed as tabs for the following items:
  - *Management Information*
  - *Management Routes*
  - *Services*
  - *High Availability*
  - *Servers*
  - *Remote Syslog Servers*
  - *Time Settings*
  - *TSE Settings*
- New Configuration Summary, Events, and System Health views which show all of the device group members information in a tabular view.

### Device Segments

- Virtual Device segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events. For more information, see [“Network Configuration: Segments/Zones Tab” on page 395](#).
- Device Segments view was moved to **Network Configuration**. Segment editing is now in a segment editor dialog and no longer has a separate view.
- Device Ports Summary was moved from Segment Edit View to Network Configuration. Port editing is now in a port editor dialog.
- Segment Group Details Views have directional columns. All 2.5 device segments have two entries - one for each direction. You can change the name of a segment group member and add a description. For information on Pre-2.5 devices, see [“” on page 429](#).

### Device Filter Settings

The **Device Filter Settings** view was moved to the **Profile** section and is now Profile **Overview**.

### Device Configuration

**Device Configuration** was moved to a dialog. The information that was previously displayed in the **Device Configuration** area is now displayed in the **Configuration Summary** view.

## Device Configuration/Device Events

The TSE Events logs moved to the **All Devices Events** screen and the **Events** screen for each device.

## Device Configuration/Reset Filters

After resetting the IPS filters on an X-Family or IPS, a popup notifies the user when the reset has completed. The reset process may take several minutes. Any profile distributions attempted before the reset has completed will fail, because the device is still busy resetting the filters.



**Note** This notification is not implemented in pre-2.5 IPS's or X-Family devices. 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 has completed.

# How To Tasks

### *Device Information*

- [“How To: View configuration settings for All Devices” on page 306](#)
- [“How To: Edit configuration settings for an individual device” on page 306](#)

### *Device Monitoring*

- [“How To: View Events for All Devices” on page 313](#)
- [“How To: View Events for a Specific Devices” on page 313](#)
- [“How To: Search Events Lists” on page 313](#)
- [“How To: Reset Events Lists” on page 313](#)
- [“How To: Flush Events Lists” on page 314](#)
- [“How To: Set Health Thresholds” on page 317](#)
- [“How To: Configure Logging Mode Settings” on page 318](#)

### *Device Management*

- [“How To: Add an IPS Device” on page 319](#)
- [“How To: Add an Offline X-Family Device” on page 323](#)
- [“How To: Create a Device Group” on page 324](#)
- [“How To: Edit Device Group Membership” on page 324](#)
- [“How To: Create a Device Group” on page 325](#)
- [“How To: Edit Device Group Membership” on page 325](#)
- [“How To: Unmanage a Device” on page 326](#)
- [“How To: Manage a device” on page 327](#)
- [“How To: Delete a Device” on page 328](#)
- [“How To: Rebooting a Device” on page 328](#)

### ***System Update***

- [“How To: Rollback to a Previous Version” on page 330](#)
- [“How To: Delete a Previous Version” on page 330](#)
- [“How To: Create a New System Snapshot” on page 330](#)
- [“How To: Import Snapshot From File” on page 331](#)
- [“How To: Export Snapshot to File” on page 331](#)
- [“How To: Copy Snapshot to the Device” on page 331](#)
- [“How To: Copy Snapshot to the SMS” on page 331](#)
- [“How To: Rollback to Snapshot” on page 331](#)
- [“How To: Delete Snapshot” on page 332](#)

### ***TippingPoint OS***

- [“How To: Download the TOS Software” on page 335](#)
- [“How To: Import TOS Software from a File” on page 335](#)
- [“How To: Obtain a High Encryption Package” on page 336](#)
- [“How To: View TOS Details” on page 336](#)
- [“How To: Distribute the TOS” on page 337](#)
- [“How To: Delete a TOS Entry” on page 337](#)

### ***Segment Groups***

- [“How To: Create/Edit a Segment Group” on page 340](#)
- [“How To: Edit a Segment Group Member” on page 341](#)

### ***IPS Devices: Device Configuration***

- [“How To: Import a Device Profile” on page 341](#)
- [“How To: Configure the Management Port” on page 346](#)
- [“How To: Reset Filters” on page 346](#)
- [“How To: Configure Management Routes” on page 347](#)
- [“How To: Configure Services” on page 349](#)
- [“How To: Configure the AFC Settings” on page 351](#)
- [“How To: Configure Network HA” on page 353](#)
- [“How To: Configure Logging Mode Settings” on page 354](#)
- [“How To: Configure NMS Settings” on page 355](#)
- [“How To: Create/Edit Remote Syslog Servers” on page 357](#)
- [“How To: Configure Servers” on page 358](#)
- [“How To: Configure the Time Options” on page 362](#)
- [“How To: Configure TSE Settings” on page 364](#)

### ***IPS Devices: Network Configuration***

- [“How To: Edit IPS Segment Details” on page 368](#)
- [“How To: Create/Edit a Virtual Segment” on page 369](#)
- [“How To: Edit Port Details” on page 369](#)
- [“How To: Import IPS Profile” on page 370](#)

### ***IPS Devices: Event Monitoring***

- [“How To: View Log” on page 371](#)
- [“How To: Reset Logs” on page 371](#)

### ***X-Family Devices: Device Configuration***

- [“How To: Configure the Management Port” on page 377](#)
- [“How To: Reset Filters” on page 378](#)
- [“How To: Configure Services” on page 379](#)
- [“How To: Configure the AFC Settings” on page 380](#)
- [“How To: Configure Logging Mode Settings” on page 382](#)
- [“How To: Configure NMS” on page 383](#)
- [“How To: Create/Edit Remote Syslog Servers” on page 385](#)
- [“How To: Configure Servers” on page 386](#)
- [“How To: Configure the Time Options” on page 390](#)
- [“How To: Configure TSE Settings” on page 392](#)

### ***X-Family Devices: Network Configuration***

- [“How To: Create/Edit Security Zone” on page 397](#)
- [“How To: Edit IPS Segment Details” on page 398](#)
- [“How To: Edit Port Details” on page 398](#)
- [“How To: Import a Profile” on page 399](#)
- [“How To: Create/Edit a Named IP Addresses” on page 401](#)
- [“How To: Create/Edit a Named Group of IP Addresses” on page 401](#)
- [“How To: Edit DHCP Server Settings” on page 402](#)
- [“How To: Create New DHCP Static Mapping” on page 403](#)
- [“How To: View/Refresh Routing Table” on page 405](#)
- [“How To: Edit Unicast/Multicast Routing Settings” on page 405](#)
- [“How To: Create a New Static Route” on page 405](#)

### ***X-Family Devices: Security Configuration***

- [“How To: Add a Firewall Rule” on page 407](#)
- [“How To: Manage Firewall Rules” on page 407](#)
- [“How To: Edit a Firewall Rule” on page 408](#)
- [“How To: Add a Custom Service” on page 409](#)
- [“How To: Edit a Custom Service” on page 409](#)
- [“How To: Add a Service Group” on page 409](#)
- [“How To: Edit a Custom Service” on page 410](#)

- [“How To: Add a Schedule” on page 410](#)
- [“How To: Edit a Schedule” on page 410](#)
- [“How To: Add a Virtual Server” on page 411](#)
- [“How To: Edit a Virtual Server” on page 411](#)
- [“How To: Edit Web Filtering Global Settings” on page 412](#)
- [“How To: Edit 3Com Content Filter Settings” on page 412](#)
- [“How To: Enable/Disable Manual Web Filtering” on page 413](#)
- [“How To: Enable/Disable IPSec Global Setting” on page 414](#)
- [“How To: Add/Edit IPSec Global Association” on page 414](#)
- [“How To: Set Up IPSec Security Association \(IKE\)” on page 415](#)
- [“How To: Enable/Edit L2TP Configuration Settings” on page 416](#)
- [“How To: Enable/Edit PPTP Configuration Settings” on page 417](#)
- [“How To: Edit Radius Configuration” on page 419](#)
- [“How To: Add/Edit Local Users” on page 420](#)
- [“How To: Edit Local User Preferences” on page 420](#)
- [“How To: Create/Edit Privilege Groups” on page 421](#)
- [“How To: Import a Local Certificate” on page 421](#)
- [“How To: Import CA Certificate” on page 422](#)
- [“How To: Export CA Certificate” on page 422](#)
- [“How To: Import Local Signed Certificate” on page 422](#)
- [“How To: Create Certificate Request” on page 423](#)

### ***X-Family Devices: Events Monitoring***

- [“How To: View Log” on page 423](#)
- [“How To: Reset Logs” on page 424](#)

### ***E Series: Advanced DDoS***

- [“How To: Configure Advanced DDoS Filter Options” on page 428](#)
- [“How To: Set DDoS Preferences” on page 429](#)

# Navigation and Menu Options

This section has the following topics:

- [Devices Screen](#)
- [Graphics Pane](#)
- [Menu Bar Options](#)

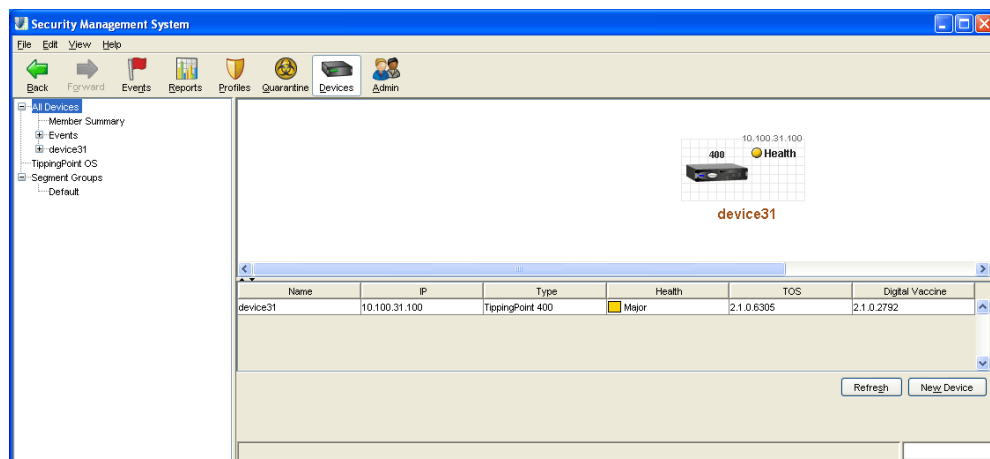
## Devices Screen

The **Devices** screen displays information for each device you are managing. By default, the **Devices** screen displays all devices and segment groups managed by your SMS. To open the **Devices** screen, click the **Devices** button on the SMS Toolbar.



**Note** A device icon or shelf-level graphic that appears with red crossbars is not managed currently by your SMS. See [“Unmanaging a Device” on page 326](#) for details.

Figure 8 - 1: Devices Screen



**Note:** For version 2.5.1 and above, the SMS displays an X before the TippingPoint Operating System (TOS) when viewing device information.



To access functions on the **Devices** screen, you can select options from the Navigation pane or Menu Bar. From the Navigation pane, the options include the following:

- [“Device Information” on page 304](#) — Details the All Devices screen that provides a jumping point for managing, monitoring, and configuring a device. Further options and sections include configuration, logs, and segments.
- [“Device Details” on page 306](#) — Details options for individual IPS and X-Family devices that the SMS manages.
- [“TippingPoint OS” on page 332](#) — Details the TOS screen for downloading, installing, and distributing updates of the TippingPoint operating system (TOS)
- [“Segment Groups” on page 337](#) — Details the Segment Groups screen that enables you to create groups of device segments for more control on distributing TOS, SMS, and profile updates.

The **Devices** screen includes the following sections and options:

- [“Graphics Pane” on page 303](#)
- [“Menu Bar Options” on page 303](#)

## Graphics Pane

The graphics pane in **Devices** displays images representing the managed and unmanaged devices in your system. Each image shows the name of the device or component, status indicators, networking information, and other appropriate details. Unmanaged devices appear with red crossbars.

By default, the graphics pane shows icons for each device and device group you are managing. Double-click a device icon to view a detailed view of the device chassis and its related status indicators.

## Menu Bar Options

The available menu items for the Menu Bar differ according to the displayed screen and user access settings. Each screen provides options for the following:



**Note** The following list may change depending on the displayed screen or selected item in the main pane.

- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:

- **New** — Creates a new item based on selection, such as:
  - a device
  - device group
  - segment group
- **Import**
  - IPS profile
  - IPS profile (VLAN)
  - TOS from file
- **Download TOS from TMC** — Downloads the latest TippingPoint operating system (TOS)
- **Distribute TOS to Device** — Distributes the TOS to a selected device
- **Reset Device** — Allows you to reset a selected device log, including all logs, system log, audit log, alert log, and block log as well as packet statistics and the connection table.
- **Logoff** — Logs you out of the SMS
- **Exit** — Closes the SMS
- **Edit** — Provides edit options based on the currently selected and displayed screen.
  - **Details** — Displays the details of a selected entry
  - **Delete** — Deletes a selected entry
  - **Membership** — Displays the segment group management screen
  - **Permissions** — Displays the user permissions to the screen options
  - **Manage Device** — Sets the selected device to be managed by SMS
  - **Unmanage Device** — Sets the selected device to not be managed by SMS
  - **Preferences** — Displays the System Preferences dialog box. See [“System Preferences” on page 27](#).
- **View** — Displays the screens for the options listed in the Navigation Pane.
  - **All Devices**
  - **TippingPoint OS**
  - **Segment Groups**
  - **Dashboard** (see [“SMS Dashboard” on page 24](#))
- **Help** — Opens and displays the *TippingPoint Security Management System Online Help*. These options also display context sensitive help for the displayed screen.

## Device Information

This section contains the following information:

- [All Devices](#) — displays images a information for all managed devices
- [Member Summary](#) — provides a snapshot of configuration settings for all managed devices
- [Device Details](#) — provides a consolidated view of device information and configuration settings.

You can perform the following tasks:

- [“View configuration settings for All Devices” on page 306](#)
- [“Edit configuration settings for an individual device” on page 306](#)

## All Devices

The **All Devices** screen displays images of the devices managed by the SMS. The List pane displays a table with entries for each device and associated device information such as IP Address, type of device, and health of the system. This screen also lists the installed versions of the TOS and DV for each managed device.

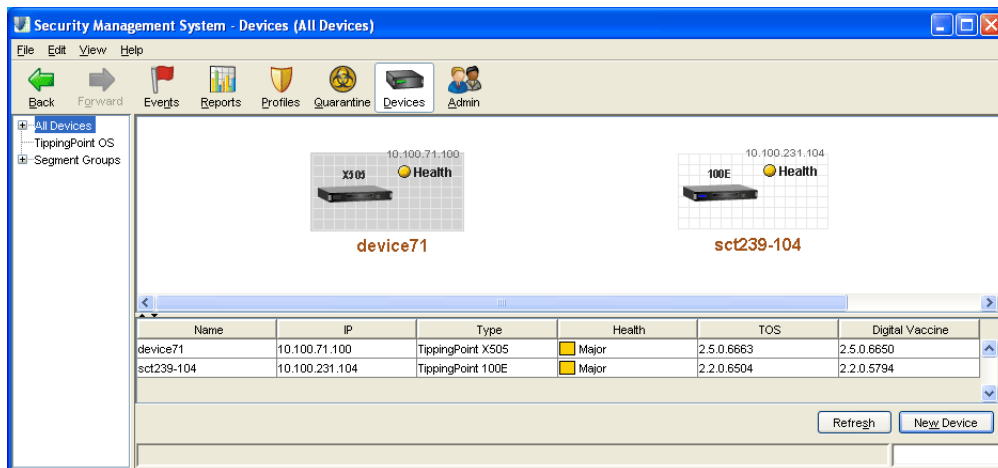
From this screen, you can:

- Refresh the list of devices and graphical image of the discovered and managed devices using the **Refresh** button.
- Add a new device using the **New Device** button. See [“Adding a Device” on page 319](#).
- Display full information on an individual device by double-clicking a device entry. See [“Device Details” on page 306](#)

See also [“Adding a Device” on page 319](#) and [“Adding Offline X-Family Devices” on page 320](#).

The following is the **All Devices** screen.

Table 8 - 1: All Devices Screen



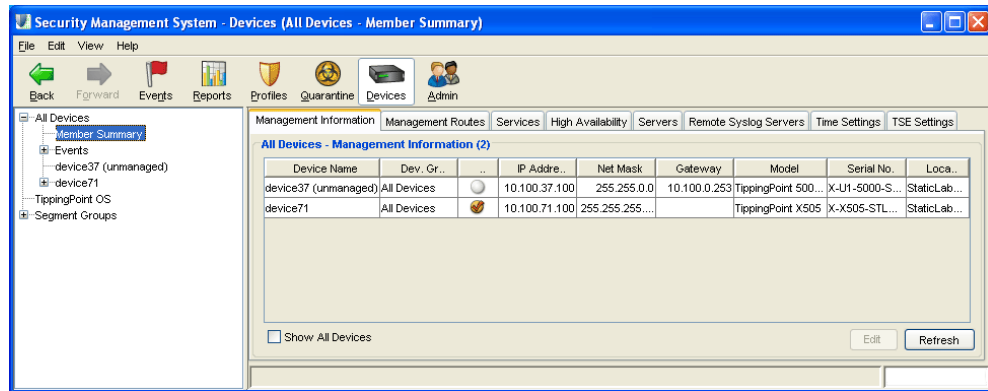
## Member Summary

For a snapshot of configuration settings for all managed devices, expand **All Devices** and select **Member Summary**.

The **Member Summary** screen lists the managed devices on the SMS and specific configuration information about those devices.

The following is the **Member Summary** screen.

Figure 8 - 2: Member Summary Screen



### How To: View configuration settings for All Devices

- Do one of the following:
  - On the **All Devices** screen, click **All Devices**.
  - On the Menu Bar, select the **view**—> **All Devices**.
- Select the appropriate tab for the configuration information you want to view.

### How To: Edit configuration settings for an individual device

- Select a device from the list pane and click Edit. The setup wizard displays.
- Make necessary changes to the appropriate configuration settings.

For information on using the Configuration Wizard and changing configuration settings for an individual device, see [“IPS Device Configuration Wizard” on page 342](#) and [“X-Family Device Configuration Wizard” on page 375](#)

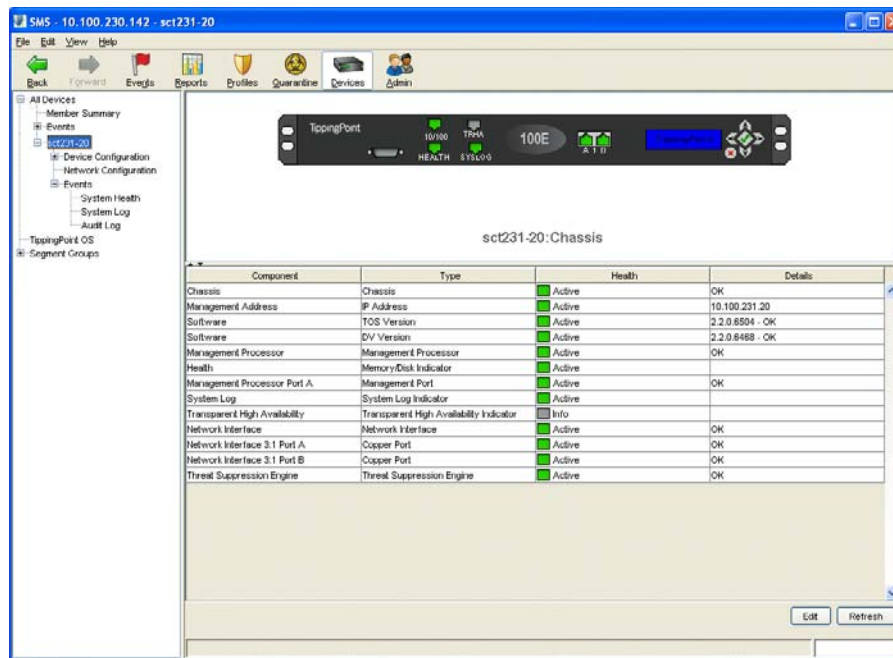
## Device Details

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
- Select an entry and select the **Edit** —> **Details** menu item.
- From the Navigation Pane, expand **All Devices**, expand **All Devices** and select a specific device from the list.

The following is the **Device Details** screen.


Figure 8 - 3: Device Details Screen




The Graph pane displays an image of the devices managed by the SMS. The List pane displays a table with entries for each managed device. The table details the following:

Table 8 - 2: Device Details

Column	Description
Component	The name of the component of the device
Type	The component type, such as chassis or copper port
Health	The health status of the device. See <a href="#">“Status Indicators” on page 308</a> .
Details	The description for the status, such as warnings or reasons for a status.

 **Note** If the Health indicator displays an error or issue, you can review the System Log for information on these health events. See [“Device Monitoring” on page 309](#).

 **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 543](#).

See the following sections:

- [Status Indicators](#)
- [Status Indicator Legends](#)

## 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 window facilitate device monitoring by displaying information about the traffic processing, health, and hardware behavior on each device and its segments.

Health status indicators provide information about the hardware components of a device.

## Status Indicator Legends

Status indicators usually appear as colored circles or squares next to a device, device group, segment or hardware component. However, in the detailed device chassis graphic, the following port graphics actually change their color as their status changes:

**Table 8 - 3: Chassis Component Legend**

Graphic	Component
	Copper ports
	Fiber ports

Status indicators appear in the following colors:

**Table 8 - 4: Status Indicator Legend**









Color	Status	Meaning
 white with grey stripes	Ignore	You have chosen to ignore the status of this element.
 red	Critical	You should respond immediately.
 yellow	Major	You should respond quickly.
 cyan	Minor	You should respond as time permits.
 grey	Informational	You might be interested in this event.
 white	Unknown	Status is unknown for this item.

Table 8 - 4: Status Indicator Legend (Continued)

Color	Status	Meaning
 green	Normal	No issues exist for this item.
 status color with grey stripes	Acknowledged	<p>You have acknowledged the status of this element. The color varies because acknowledging a status adds gray stripes to the current status indicator.</p> <p>When the status for the component changes, a status indicator set to Acknowledged changes to a color representing the new status.</p>

Additional device monitoring is available through the Events feature for a specific device, see [“IPS Devices: Event Monitoring” on page 371](#) and [“X-Family Devices: Event Monitoring” on page 423](#)

For information on system details for an individual device, see [“Device Details” on page 306](#).

## Device Monitoring

This section includes the following items:

- [“Events” on page 309](#)
- [“System Health” on page 314](#)

Additional device monitoring is available through the Events feature for a specific device, see [“IPS Devices: Event Monitoring” on page 371](#) and [“X-Family Devices: Event Monitoring” on page 423](#)

For information on system details for an individual device, see [“Device Details” on page 306](#).

## Events

The **All Devices - Event** screen provides a top view of event information for all managed devices.

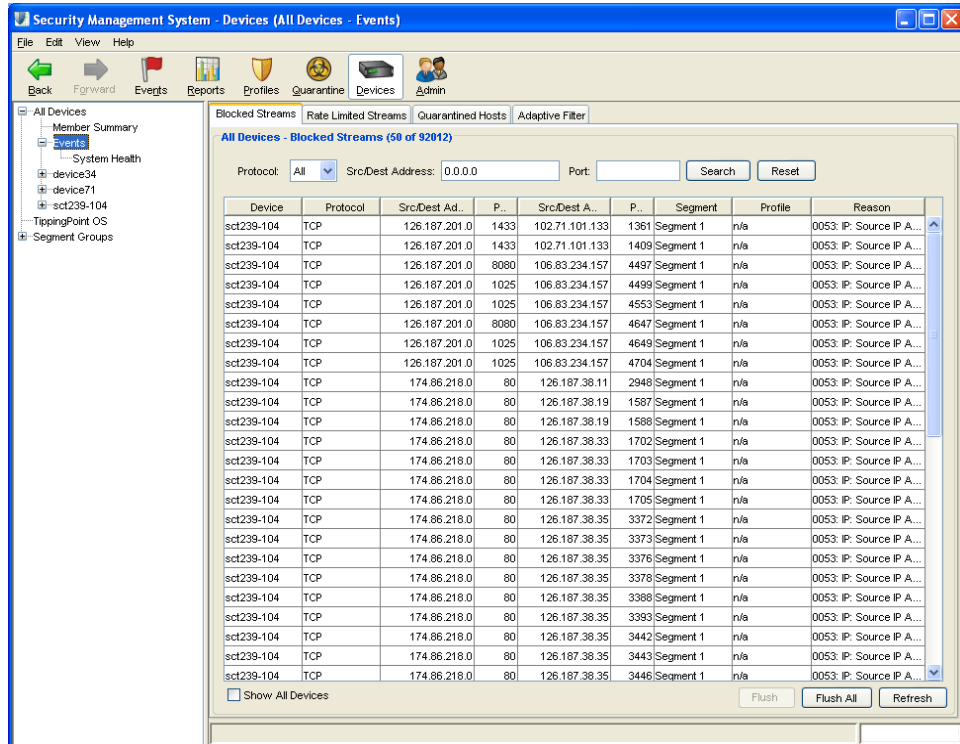
From the **All Devices - Events screen**, you can view information on the following items:

- Blocked Streams
- Rate Limited Streams
- Quarantined Hosts
- Adaptive Filter

To access the Events listings, use the Device 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 313](#) and [“View Events for a Specific Devices” on page 313](#).

The following is the **Device Events (All Devices)** screen.

Figure 8 - 4: Device Events (All Devices) Screen



This section contains the following items:

- [“Blocked and Rate Limited Streams Tabs” on page 310](#)
- [“Quarantine Hosts Tab” on page 311](#)
- [“Adaptive Filtering Tab” on page 312](#)
- [“Viewing and Searching Events” on page 312](#)

You can perform the following tasks:

- [“View Events for All Devices” on page 313](#)
- [“View Events for a Specific Devices” on page 313](#)
- [“Search Events Lists” on page 313](#)
- [“Flush Events Lists” on page 314](#)

## Blocked and Rate Limited Streams Tabs

The SMS provides a feature for displaying the blocked and rate limited streams of the connection table. To view, search, and flush the streams, you 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 and destination IP addresses and ports. The returned streams display in this table.

The streams display in the TSE Connection Table section of the screen. You can flush these connections from the connection table on this page. The **Flush All** option removes all blocked streams (including blocked streams not displayed) from the connection table. The effect is as though the blocked streams all timed out at the same time. You can also select blocked streams to be flushed. The **Flush Selected** option only removes the blocked streams selected from the list of displayed entries.

The Blocked Streams and Rate Limited Streams tabs provide the following information:

**Table 8 - 5: TSE Connection Table Details**

Option	Description
Device	device name
Protocol	protocol of the blocked or rate limited stream
Src/Dest Address	source IP address, destination IP address
Src /Dest Port	source port, destination port
Segment	IP address of the segment
Profile	name of the profile for the filter triggered
Reason	reason for the blocked stream

## Quarantine Hosts Tab

The **Quarantine** 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 Quarantine Hosts tab, you can search for specific host IP Address, unquarantine individual hosts or all hosts.

When a filter with a Quarantine option 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 may receive a message or be rerouted to a web page detailing the reason for the blocked traffic.

The Quarantine tab provides the following information:

Table 8 - 6: TSE Quarantine Table Details

Option	Description
Device	device name
Host Addr	quarantined IP address
Segment	segment the IP address is quarantined on
Profile	name of the profile for the filter triggered
Filter	name of the filter that triggered quarantine

### Adaptive Filtering Tab

The Adaptive **Filter** tab provides the following information:

Table 8 - 7: TSE Adaptive Filter Configuration Information

Option	Description
Device Name	device name
Filter Name	name of the filter that triggered
Segment	user-defined segment
Filter State	Indicates the filters state: <ul style="list-style-type: none"> <li>• Enabled — Displays <b>Enabled</b> if the filter is enabled and running</li> <li>• Disabled — Displays an empty value if the filter is disabled. To enable, edit the filter.</li> </ul>
Adaptive Config State	Indicates the adaptive state of the filter. If it displays <b>Enabled</b> , the filter has been disabled. The LSM disables a filter if the adaptive filter settings are triggered.

### Viewing and Searching Events

Table 8 - 8: Events Search Criteria

Status	Meaning
<b>Blocked Streams</b>	<ul style="list-style-type: none"> <li>• <b>Protocols:</b> All, TCP, UDP, ICMP</li> <li>• <b>Scr/Dest Address:</b> Source/Destination IP Address</li> <li>• <b>Port</b></li> </ul>
<b>Rate Limited Streams</b>	<ul style="list-style-type: none"> <li>• <b>Protocols:</b> All, TCP, UDP, ICMP</li> <li>• <b>Scr/Dest Address:</b> Source/Destination IP Address</li> <li>• <b>Port</b></li> </ul>
<b>Quarantined Hosts</b>	<ul style="list-style-type: none"> <li>• <b>Host Address</b></li> </ul>

### How To: View Events for All Devices

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select **Events** from the Navigation pane.
3. Select the tab associated with the event you want to view:
  - Blocked Streams
  - Rate Limited Streams
  - Quarantined Hosts
  - Adaptive Filter

See [“Search Events Lists” on page 313](#).

### How To: View Events for a Specific Devices

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.
  - Blocked Streams
  - Rate Limited Streams
  - Quarantined Hosts
  - Adaptive Filter

See [“Search Events Lists” on page 313](#).

### How To: Search Events Lists

1. [“View Events for All Devices” on page 313](#) or [“View Events for a Specific Devices” on page 313](#).
2. Select one of the following tabs:
  - Blocked Streams
  - Rate Limited Streams
  - Quarantined Hosts
3. Specify the appropriate search criteria. See [“Events Search Criteria” on page 312](#).
4. Click **Search**.

### How To: Reset Events Lists

1. [“View Events for All Devices” on page 313](#) or [“View Events for a Specific Devices” on page 313](#).
2. Select one of the following tabs:
  - Blocked Streams
  - Rate Limited Streams
  - Quarantined Hosts
3. Click **Reset**

### How To: Flush Events Lists

1. [“View Events for All Devices” on page 313](#) or [“View Events for a Specific Devices” on page 313](#).
2. Select one of the following tabs:
  - Blocked Streams
  - Rate Limited Streams
3. To flush all blocked or rate limited streams, click **Flush All**.
4. To flush selected streams, select entries and click **Flush Selected**.
5. Click **OK**.



**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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).



**Note** Not all Traffic Normalization filters result in blocked streams. For more information, see [“Traffic Normalization Filters” on page 221](#).

## System Health

The **Device System Health** screens provide information on the health, packets, and traffic of your system. Through the screen, you can:

- View system health information.
- Maintain the thresholds settings for the health of your hard disk usage, memory usage, and temperature.
- Reset packets and logs, including audit and system logs.
- Review traffic logs of the system.

The following is the **Device System Health** screen.

Figure 8 - 5: Device System Health Screen

The screenshot displays the 'Device System Health' screen for device 'sct231-20'. The interface is organized into three main sections:

- Packet Statistics:**
  - Device: sct231-20
  - Total Packets: 16,320,192,017
  - Blocked: 4,135,323 (Invalid) 3,944,312,858
  - Permitted: 68,264
- Health:**

Component	Value	Health	Details
Memory	72%	<span style="color: green;">■</span>	368 of 511 MB
Temperature	0 C	<span style="color: green;">■</span>	Range: 40 - 85 (Celsius)
Disk.boot	50%	<span style="color: green;">■</span>	50 of 100 MB
Disk.logt	0%	<span style="color: green;">■</span>	0 of 279 MB
Disk.usr	23%	<span style="color: green;">■</span>	14 of 59 MB
Disk.log	3%	<span style="color: green;">■</span>	2 of 59 MB
- Traffic:**

Interface	In-Octets	Out-Octets	In-Discards	Out-Discards	In-Errors	Out-Errors
Segment 1.B	0	0	0	0	0	0
Segment 1.A	0	0	0	0	0	0

The **Device System Health** screen includes the following sections:

- [Packet Statistics](#) —displays the number of packets processed by the device since boot time
- [Health](#) —displays information regarding device health and allows you to set associated threshold settings
- [Traffic](#) —tracks and compiles information on all traffic managed by the device

You can do the following tasks:

- [“Reset Logs” on page 318](#)
- [“Set Health Thresholds” on page 317](#)
- [“Configure Logging Mode Settings” on page 318](#)

### 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.

The section includes the following information:

- [Health](#)
- [Traffic](#):

Table 8 - 9: Packet Statistics Details

Heading	Description
Device	The name of the device
Total Packets	The total number of packets blocked and permitted
Blocked	The number of Blocked packets
(Invalid)	The number of invalid packets. This amount is part of the Blocked total.
Permitted	The number of permitted packets

### Health

The **Health** section displays the following information:

Table 8 - 10: Health Details

Column	Description
Component	<p>The components of the system:</p> <ul style="list-style-type: none"> <li>• Memory</li> <li>• Temperature</li> </ul> <p>The following also displays for 200/400/1200/2400/5000E:</p> <ul style="list-style-type: none"> <li>• Disk/boot</li> <li>• Disk/log</li> <li>• Disk/usr</li> <li>• Disk/opt</li> </ul> <p>The following also displays for 50/100E:</p> <ul style="list-style-type: none"> <li>• Disk/usb0</li> </ul>
Value	The percentage amount of the component used.
Health	<p>One of the following status indicators:</p> <ul style="list-style-type: none"> <li>• Green/Normal</li> <li>• Yellow/Major</li> <li>• Red/Critical</li> </ul>
Details	The amount used of the total available megabytes (MB)



**Note** For details about disk and memory usage, refer to the *TippingPoint Local Security Manager User's 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 543](#).

## Traffic

The **Traffic** log section tracks and compiles information on all traffic managed by the device. This log includes information according to segment of the device. It details the interface for managing the traffic, the type of traffic, and the count and rate. To refresh the display, click **Refresh**. To display Device Traffic reports, click **Traffic Reports**. See [“Device Traffic Reports” on page 124](#).

The screen displays the following information:

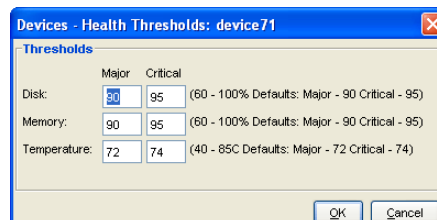
**Table 8 - 11: Traffic Details**

Column	Description
Interface	The segment and port through which the traffic passed
In: Octets	The total number of octets transmitted to the interface
Out: Octets	The total number of octets transmitted from the interface
In: Discards	The number of inbound packets discarded due to resource limitations
Out: Discards	The number of outbound packets discarded due to resource limitations
In: Errors	The number of inbound packets that were discarded due to errors
Out: Errors	The number of outbound packets that were discarded due to errors

## How To: Set Health Thresholds

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device and expand the options.
3. Select **System Health**.
4. In the **Health** section, click **Settings**.

The **Devices - Health Thresholds** dialog box displays.



5. For **Disk**, 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**.

#### How To: Reset Logs

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device and expand the options.
3. Select **Health/Performance** and the **Health/Performance** tab.
4. Do one of the following:
  - In the **Packet Statistics** section, click **Reset**.
  - Display a log screen and click **Reset**.
  - On the Menu Bar, select the **File** —> **Reset Device Logs** menu item and select the log you want to reset: system, audit, alert, block, or all.
5. To reset all logs, you can select the **All Logs** option. On the Menu Bar, select the **File** —> **Reset Device Logs** —> **All Logs** menu item.



**Note** The reset all option does not reset the audit log.

#### How To: Configure Logging Mode Settings

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device and expand the options.
3. Select **System Health** and then locate the **Logging Mode Settings** section.
4. To enable or disable continual alerting of permitted or blocked packets, click the **Enabled** check box. If enabled, the system continuously sends alerts for permits and blocks of traffic. If disabled, you can continue to configure settings for thresholds and disabled time periods.
5. To configure the threshold for disabling alerting, enter a percentage for **Packet loss threshold**. If the packet loss breaches the threshold, the system disables alerting according to the amount of configured time.
6. To set the amount of time to **Disable notifications**, enter an amount of seconds. After the time period passes, alerting enables until the threshold is exceeded again.
7. Click **Apply**.

## Device Management

To manage a device from the SMS, you must add it using the New Device add feature. After you add a new device, 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.



You can perform the following management options:

- [“Adding a Device” on page 319](#)
- [“Adding Offline X-Family Devices” on page 320](#)
- [“Creating a Device Group” on page 324](#)
- [“Creating a Segment Group” on page 324](#)
- [“Changing Management Port Settings” on page 325](#)
- [“Unmanaging a Device” on page 326](#)
- [“Managing a Device” on page 327](#)
- [“Deleting a Device” on page 327](#)
- [“Rebooting a Device” on page 328](#)



**Note** By default, the SMS can manage up to five devices. If you need to manage more, you must purchase a license upgrade from TippingPoint. For more information about upgrading your license, see [“Administration” on page 431](#).



**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 543](#).

## Adding a Device

When you add a device to the SMS, you can manage and unmanage the device without having to remove it. Before you can manage a device, you must enable the device to accept SMS control. See the *TippingPoint Local Security Manager User’s Guide*.

You add the device through the **All Devices** screen. As you add each device, the SMS displays the device by the name in the Navigation pane. You can then access and manage the device settings through the **Devices** screen.



**Note** When a device is added, it is under the exclusive control of the SMS. The Local Security Manager (LSM) becomes a read-only, web interface.

When you click the **Add** button to finish the instructions, blinking green status indicators and messages are displayed in the status bar at the bottom of the screen. If the device is added successfully, you see the message **Done**.

### How To: Add an IPS Device

1. Do one of the following:
  - On the **All Devices** screen, click **New Device**.
  - On the Menu Bar, select the **File** —> **New** —> **Device**.
 The **Devices - New Device** dialog box displays.

2. Enter the **IP Address** of the device.
3. Enter the **Username** for a SuperUser account defined on the IPS.
4. Enter the **Password** associated with the SuperUser account.
5. Select a device group to add the device to from the **Member of Device Group** drop-down. You can select All Devices or a specific Device Group. To create a group, see
6. Optionally, check the **Synchronize Device Time with SMS**.
7. Use the **Online Device** option if you want to configure the device and/or clone an existing device.
8. Click **OK**. When the request is successful, the device name displays in the **Devices** screen.
9. Repeat the previous steps to add multiple devices.
10. When you are finished adding multiple devices, close the **Device - New Device** dialog box by clicking the **Cancel** button.
11. To verify that your device or devices were added to the SMS and are functioning properly,
  - Navigate to the **All Devices** screen and verify that the device or devices are listed.
  - Verify that the Health status indicator is green. When you add a device, the system saves historical data for the device.

## Adding Offline X-Family Devices

The SMS offline configuration option provides a convenient method for pre-adding one or more X-Family devices to the SMS before the devices are actually online in the network.



**Note:** If an X-Family device is in Fully Transparent mode (i.e. it has only one virtual interface - the external one) Offline Device Acquisition does not work.

If you want the SMS to automatically acquire to devices using the SMS, you must add a VPN configuration file to the SMS offline setup. When each device comes online, it establishes a secure connection to the SMS using a VPN tunnel.

This section contains the following topics:

- [“Adding a Single Device” on page 321](#)
- [“Adding Multiple Devices” on page 321](#)
- [“Deploying X-Family Devices Remotely” on page 321](#)

## Adding a Single Device

To add one device at a time, you must enter a **Username**, **Password** and a valid serial number for the X-Family device.

## Adding Multiple Devices

If you are adding multiple devices, you can use a serial numbers file. A serial numbers file is a text file that resides on your network and contains one valid serial number per line. Offline configuration of X-Family devices can be set up per device using a single serial number file. See and [“Add an Offline X-Family Device” on page 323](#).



**Note:** A VPN Configuration file cannot be used with this method because each remote device needs a unique VPN configuration file.

## Deploying X-Family Devices Remotely

To automate device acquisition, you must use a configuration file to set up a VPN tunnel. A configuration file is a text file that resides on your network and contains one device CLI command per line. For instructions and setup information, [see Appendix E, “X-Family Remote Deployment” page 547](#).



**Note** If you use a VPN tunnel for device acquisition, this tunnel can also be used for other data. Any additional VPN tunnels that are set up on the device must not interfere with this tunnel (by editing the underlying IKE proposal or by using the same local and remote subnets).

The following setup requirements apply:

- **X-Family Device Setup** —SMS configuration must be enabled with the X-Family CLI `setup` command or the `conf t sms` command. See [“VPN Terminator Setup” on page 553](#).
- **VPN Terminator Setup** — VPN Terminator (to which SMS is connected) must meet specific configuration requirements. See [“VPN Terminator Setup” on page 553](#).
- **SMS Setup**— X-Family devices must be added offline using serial numbers. Setup must also include a VPN configuration file to establish the required VPN between the X-Family and the SMS. [“Device Management” on page 554](#).

Remote X-Family devices that are accessed via the internet are managed through an IPSec (or GRE/IPSec) tunnel between the HQ where the SMS is located and the remote X-Family device. The tunnel, which may also be used for regular data traffic, provides a secure connection for the device to notify the SMS that it is coming online to retrieve any initial (offline) configuration setup from the SMS.

The initial provisioning VPN configuration for the device is mapped to a series of CLI commands that will be sent to the device via the secure connection to perform minimum configuration setup to allow SMS to communicate with the device for SMS device management.

### X-Family Devices

The SMS Configuration dialog enables or disables management of the device by a Security Management System (SMS). If you enable SMS-based configuration on your X-Family device, you are prompted to enter the IP address of the SMS device that you want to manage the X-Family device. The device will download the SMS configuration from the specified device. For more information, see the TippingPoint X-Family documentation.

### SMS

To setup SMS and automate the X-Family device setup, perform the following tasks:

1. Using the offline option, pre-add one or more X-Family devices and designate the VPN configuration file to use.

You can also use a serial numbers file that contains the serial number for an X-Family device followed by the associated VPN configuration. A serial numbers files can contain multiple X-Family devices. See [“Add an Offline X-Family Device” on page 323](#).



**Note:** After an offline device is added, it cannot be edited. If there are incorrect information specified for the offline device, the offline device will need to be deleted and re-added to the SMS.

2. Manage the X-Family device by bringing the devices online. See [“Managing a Device” on page 327](#).

When each device comes online, it contacts the SMS to download the configuration file to establish the required VPN for SMS management.



**Note:** After the configuration file is downloaded to the device, errors in the configuration file can only be corrected using LSM or by deleting and re-adding the offline device with the correct configuration file. You must then re-run the device setup command to initiate the secure connection again.

The SMS client notification dialog displays messages regarding the status of the secure connection between the device and the SMS. Types of information includes when the device:

- comes online
- contacts the SMS
- starts processing the configuration file,
- has a configuration error

## How To: Add an Offline X-Family Device

- Do one of the following:
  - On the **All Devices** screen, click **New Device**.
  - On the Menu Bar, select the **File** —> **New** —> **Device**.
 The **Devices - New Device** dialog box displays.

- Enter the **Username** for a SuperUser account defined on the IPS.
- Enter the **Password** associated with the SuperUser account.
- Select a device group to add the device to from the **Member of Device Group** drop-down. You can select **All Devices** or a specific Device Group. To create a group, see
- Optionally, check the **Synchronize Device Time with SMS**.
- Select the **Offline X-Family Device** option.
- For the serial number, do one of the following:
  - Select the **Serial Number** option
    - Enter the serial number for the X-Family device.
    - Select the **Use a configuration file** option.
    - Browse to the file location and select the VPN configuration file.
  - Select the **Serial Numbers File** option.
    - Browse to the file location.
    - Select the serial numbers file that contains individual listings of the X-Family devices and their associated VPN configuration.



**Note:** A VPN configuration file is a text file that resides on your network and contains a series of CLI commands for setting up a VPN. For examples and the most current configuration file information, see the **SMS Release Notes**.



**Note:** A serial numbers file is a text file that resides on your network and contains a valid serial number followed by a series of CLI commands for setting up a VPN. You must use `#serial` for each serial number listing and `#config` for the associated CLI commands for setting up a VPN. For examples and the most current configuration file information, see the *SMS Release Notes*.

8. Click **OK**.

### Creating a Device Group

To enhance management of devices, the SMS provides device groups. These groups create a hierarchal organization to device management in the navigation pane for the Devices screen. Unlike segment groups, device groups do not affect action sets, distributions, reports, or other features for modifying and managing devices.

You can also create device groups within device groups, extending network device management. Each group can hold an unlimited amount of devices as needed.

#### How To: Create a Device Group

1. On the **All Devices** screen, select the **File** —> **New** —> **Device Group** menu item from the Menu Bar. The **Devices - New Device Group** dialog box displays.
2. Enter the **Name** for the device group.
3. To create a device group within a device group, select a device group from the drop-down menu.
4. Click **Add**.

#### How To: Edit Device Group Membership

1. On the **All Devices** screen, select a device group from the view.
2. On the Menu Bar, select the **Edit** —> **Membership** menu item. The **Device Group - Edit Membership** dialog box displays.
3. Enter a new **Device Group Name** for the device group.
4. To add a device to a group, select a device in the **Non-Member Group** pane and click the direction button to the **Device Group Members** pane.
5. To remove a device to a group, select a device in the **Device Group Members** pane and click the direction button to the **Non-Member Group** pane.
6. Click **OK** when complete.

### Creating a Segment Group

To enhance management of devices, the SMS provides segment groups. These groups create a hierarchal organization to device management in the navigation pane for the Devices screen. Unlike segment groups, device groups do not affect action sets, distributions, reports, or other features for modifying and managing devices.

You can also create device groups within device groups, extending network device management. Each group can hold an unlimited amount of devices as needed.

#### How To: Create a Device Group

1. On the **All Devices** screen, select the **File** —> **New** —> **Device Group** menu item from the Menu Bar. The **Devices - New Device Group** dialog box displays.
2. Enter the **Name** for the device group.
3. To create a device group within a device group, select a device group from the drop-down menu.
4. Click **Add**.

#### How To: Edit Device Group Membership

1. On the **All Devices** screen, select a device group from the view.
2. On the Menu Bar, select the **Edit** —> **Membership** menu item. The **Device Group - Edit Membership** dialog box displays.
3. Enter a new **Device Group Name** for the device group.
4. To add a device to a group, select a device in the **Non-Member Group** pane and click the direction button to the **Device Group Members** pane.
5. To remove a device to a group, select a device in the **Device Group Members** pane and click the direction button to the **Non-Member Group** pane.
6. Click **Ok** when complete.

## Changing Management Port Settings

The following management port settings can be changed using the Device Configuration Wizard.

- **Auto negotiation:** Enable/Disable
- **Line Speed:** 100 Mbps, 10 Mbps
- **Duplex**

#### *Change Management Port Settings*

1. To access the Device Configuration Wizard do one of the following:
  - On the **All Devices** screen, select a device and click **Edit**.
  - Select a device, select the management port listing from the component list, and then click **Edit**.
2. From the Device Configuration Wizard panel menu, select **Management Information**.

3. In the **Host Management Information** section, make the desired changes. Available options include:
  - **Auto negotiation:** Enable/Disable
  - **Line Speed:** 100 Mbps, 10 Mbps
  - **Duplex Mode:** Full/half



**Note:** If you change auto negotiation, line speed, or duplex settings for the management port, you may lose connectivity between the SMS and the device. Network monitoring by the device will remain unaffected.



**Note:** For pre-2.5 devices, you can view the management port setting, but cannot make any changes.

## Unmanaging a Device

At any time, you may need to unmanage a device. An unmanaged device returns control to modify filters, updates, and configuration settings through the Local Security Manager (LSM) and device itself. 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.

You must have Administrator access on the SMS to unmanage a device.

When the process is complete, the graphics for unmanaged devices appear in the **Devices** window with red crossbars over them. In **Configuration**, you can view the configuration information for unmanaged devices, but you cannot edit it.

After unmanaging the device, you can resume control of the device by managing the device. See [“Managing a Device” on page 327](#) for more information.



**Note** When you unmanage a device, it no longer counts against your SMS license allotment. See [“Administration” on page 431](#) for details.

### How To: Unmanage a Device

1. On the **All Devices** screen, select a managed device from the List pane.
2. On the Menu Bar, select the **Edit** —> **Unmanage Device** menu item. The **Unmanage Device** dialog box displays.

The dialog box informs you that unmanaging the device removes control to update or distribute packages to the selected device.
3. Click **Unmanage**.



## Managing a Device

When you manage a device, you control all aspects of configuration, updates, and filters through the SMS application. SMS management overrides the use and configuration control of the Local Security Manager (LSM). If you want to manage a device, the device must accept SMS control. See the *TipplingPoint Local Security Manager User's Guide* for more information.



**Note** You must have Administrator access on the SMS to manage a device.

When you manage a device, you are resuming control of a device you have unmanaged. Once you manage a device, you can unmanage the device. When you unmanage the device, the LSM can configure and enter filter changes to the device. See [“Unmanaging a Device” on page 326](#) for details.



**Note** When you manage a device, it counts against your SMS license allotment. See [“Administration” on page 431](#) for details.

### How To: Manage a device

1. Open the **All Devices** screen.
2. Select a device from the List pane. The device displays in the Graph pane with a red X over it. This mark represents that the SMS does not manage the device.
3. On the Menu Bar, select the **Edit** —> **Manage Device** option. A dialog box displays allowing you to enter data for the device. The IP address of the device is provided.
4. Enter the **Username** for a Super User account defined on the IPS.
5. Enter the **Password** associated with the Super User account.
6. Click **OK**. The device displays as normal, without the red X mark. You can now configure and manage the device using the SMS.

## Deleting a 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 is maintained unless you choose to delete it as well.



**Note** You cannot delete a device while it is receiving or distributing a software or security package or completing a configuration operation.



**Note** You must have Administrator authority on the SMS to delete a device.

When the process is complete, the device name is no longer displayed in any SMS window.

### How To: Delete a Device

1. On the **All Devices** screen, select a device from the List pane.
2. On the Menu Bar, select the **Edit** —>**Delete** menu item. The **Delete Device** dialog box displays. This dialog includes a warning reminds that you cannot manage a deleted device and that most of the information about it is purged from the SMS database.
3. Click **Delete**. The device is no longer is available for monitoring, managing, or editing in the SMS.

## Rebooting a Device

You may need to reboot a device to perform actions or to refresh the device. These actions include software update procedures and power supply replacement procedures. When you reboot a system through the SMS, you perform a warm boot. The device shuts down and restarts immediately. This type of reboot is not a power cycle. When you perform a power cycle, you disconnect the power from the device and wait ten (10) seconds prior to turning the device on.

You can reboot the device through the **Devices - Device Configuration** screen.

### How To: Rebooting a Device

1. Through the **Devices** Navigation pane, expand and select a device's Device Configuration screen.
2. On the **Device Configuration** screen, select the Management Port tab.
3. Click **Reboot**. The device reboots.

## System Update

On the **Device Configuration - Software Versions** screen, you can manage software versions and snapshots for a specific device. The SMS maintains a history of versions installed for your device. Through the **Previous TOS Versions** section, you may rollback to a previous version of the device software.

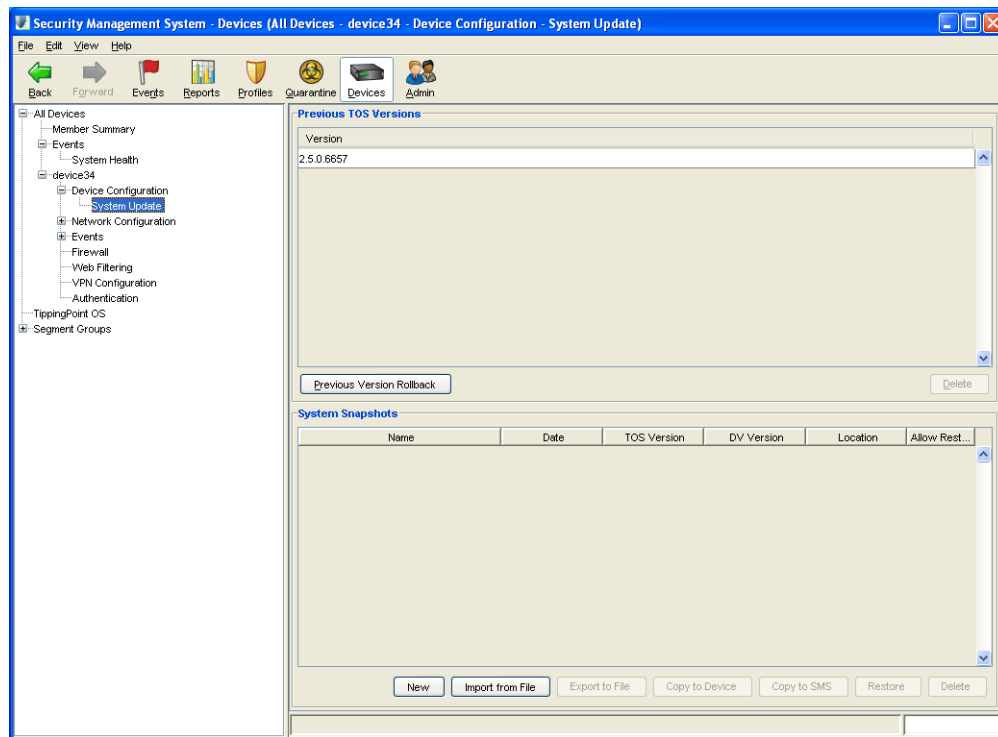


**Note** Prior to rolling back to a software version, make sure to review the release notes for any specific notations and warnings regarding a version's functionality.

Through the **System Snapshot** section, you can manage the snapshots taken of device filters and settings. You can create these snapshots through the **Profiles** screen.

The following is the **Device Configuration - Software Versions** screen:

**Figure 8 - 6: Device Configuration - Software Versions**



The two tables list the software versions and snapshots. Each entry includes the following information:

**Table 8 - 12: Software Versions Table Information**

Column	Description
Version	The version of the TOS
Name	The name of the snapshot
Date	The date of the snapshot
TOS Version	The version of the TOS running when the snapshot was made
DV Version	The version of the Digital Vaccine package when the snapshot was made
Location	Location of the rollback file
Allow Restore	Indicates if you can restore

See the following:

- [“Rollback to a Previous Version” on page 330](#)
- [“Delete a Previous Version” on page 330](#)
- [“Create a New System Snapshot” on page 330](#)
- [“Import Snapshot From File” on page 331](#)
- [“Copy Snapshot to the Device” on page 331](#)
- [“Copy Snapshot to the SMS” on page 331](#)
- [“Rollback to Snapshot” on page 331](#)
- [“Delete Snapshot” on page 332](#)

### How To: Rollback to a Previous Version

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. From the **Previous TOS Versions** table, select a software version entry.
3. 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 a version's functionality.

### How To: Delete a Previous Version

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. Select a software version entry.
3. Click **Delete**.
4. A confirmation message displays. Select the appropriate action to delete the entry.

### How To: Create a New System Snapshot

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. From the System Snapshots area, click **New**.
3. A new snapshot image is created of the device and the entry displays in the table.



**Note** The snapshot procedure may take time. Give sufficient time for the procedure to complete.

### How To: Import Snapshot From File

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. From the System Snapshots area, click **Import From File**. A file browsing window displays.
3. Browse to and select the local file. Click **OK**.
4. The system uploads the snapshot to the list of entries.

### How To: Export Snapshot to File

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. In the **System Snapshot** table, select a snapshot to export.
3. Click **Export To File**. A file browsing window displays.
4. Select a location for the file export.
5. The system exports the snapshot to a file.

### How To: Copy Snapshot to the Device

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. In the **System Snapshot** table, select a snapshot to copy.
3. Click **Copy To Device**.
4. The system copies the snapshot to the device.

### How To: Copy Snapshot to the SMS

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. In the **System Snapshot** table, select a snapshot to copy.
3. Click **Copy To SMS**.
4. The system copies the snapshot to the SMS.

### How To: Rollback to Snapshot

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. In the **System Snapshot** table, select a snapshot to rollback to and click **Restore**. When you roll-back, the snapshot overwrites all settings for a profile to the device with the snapshot settings.

3. The system may prompt with a warning or further steps.



**Note** The snapshot procedure may take time. Give sufficient time for the procedure to complete.

#### How To: Delete Snapshot

1. On the **Device Configuration** screen, click the **System Update** option. The **Device Configuration - System Update** screen displays.
2. In the **System Snapshot** table, select a snapshot to delete.
3. Click **Delete**. A confirmation message may display. Select the appropriate option to delete the snapshot.

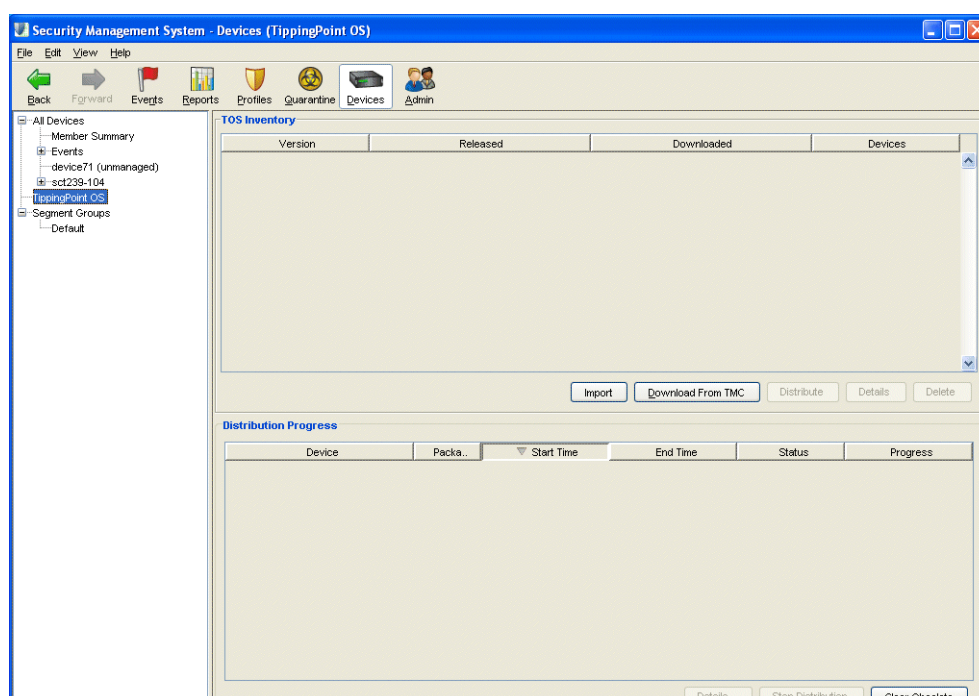
## TippingPoint OS

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. For information on updating Digital Vaccine and Custom Shield packages, see [Chapter 6, “Profiles”](#).

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 **Devices (TippingPoint OS)** screen.

The following is the **Devices (TippingPoint OS)** screen:

**Figure 8 - 7: Devices (TippingPoint OS) Screen**



The following information displays:

**Table 8 - 13: TOS Inventory Details**

Column	Description
Version	The version number of the TOS
Released	The date and time of the released version of the TOS
Downloaded	The date and time of the download to the SMS
Devices	The device models supported by the release

**Table 8 - 14: Distribution Process Details**

Column	Description
Device	The name of the device updating to the TOS
Version	The version number of the TOS
Start Time	The start date and time of the distribution
State	The state of the 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 may 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 335](#)
- [“Import TOS Software from a File” on page 335](#)
- [“Managing TOS Distribution” on page 336](#)
- [“View TOS Details” on page 336](#)
- [“Distribute the TOS” on page 337](#)
- [“Delete a TOS Entry” on page 337](#)

## 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.

Only users with Super User access can perform these operations.

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 335](#)
- [“Import TOS Software from a File” on page 335](#)

After importing and downloading the file(s), you need to distribute and manage the files. See the following:

- [“Managing TOS Distribution” on page 336](#)
- [“View TOS Details” on page 336](#)
- [“Distribute the TOS” on page 337](#)
- [“Delete a TOS Entry” on page 337](#)



### How To: Download the TOS Software

1. Open the **Devices - TippingPoint OS** screen.
2. Do one of the following:
  - Click **Download from TMC**.
  - On the Menu Bar, select the **File** —> **Download TOS Software** menu item.
3. The SMS contacts the Threat Management Center, checks the versions, and begins the download of any available updates for the TOS software.  
The file displays in the **TOS Inventory** section.

### How To: 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 navigation pane on the left, click **IPS Software Updates**. The page lists all available software images. The most recent version is at the top of the list.
3. Click the **More Info** button next to the most recent package.
4. In the Download File page, click the **Download Now** button. After a few seconds, the **File Download** dialog box is displayed.
5. 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.

6. In the SMS Client, open the **Devices - TippingPoint TOS** screen.
7. Do one of the following:
  - Click **Import**.
  - On the Menu Bar, select the **Edit** —> **Import TOS Software from File** menu item.
8. A dialog box opens. Locate the file.  
The file displays in the **TOS Inventory** section.

## High Encryption for X-Family Devices

X-Family devices contain encryption functionality that is controlled for export by the U. S. Department of Commerce. by default, all new X-Family platforms are supplied with 56-bit DES encryption only. To enable high encryption functionality (3DES, 128-AES, 192-AES, 256 AES) you must log on to your TMC account and complete an export compliance form.

After submission of the form, end-users who meet the U.S export criteria will be sent an email that contains a URL to download a high encryption service pack. This service pack is installed in the similar manner as any other TippingPoint Operating System (TOS) image. See [“Importing and Downloading the TOS” on page 334](#). After the service pack is installed, high encryption functionality is permanently enabled on the X-Family device.

### How To: Obtain a High Encryption Package

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. Click the appropriate link to complete the export compliance form, which is displayed in a new browser window.

## 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 displays in the **Distribution Progress** section 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. Only users with Administrative and Super User access can perform these operations.



**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.

You can do the following:

- [“View TOS Details” on page 336](#)
- [“Distribute the TOS” on page 337](#)
- [“Delete a TOS Entry” on page 337](#)

### How To: View TOS Details

1. On the **Devices** Navigation pane, click **TippingPoint OS**. The **Devices - TippingPoint OS** screen displays.
2. In the **TOS Inventory**, select a TippingPoint OS entry.

3. Do one of the following:
  - Click **Details**.
  - On the Menu Bar, select the **Edit** —> **Details** menu item.

The **TOS - Details** screen displays. The screen provides information on the TippingPoint OS software update.

#### How To: Distribute the TOS

1. On the **Devices** Navigation pane, click **TippingPoint OS**. The **Devices - TippingPoint OS** screen displays.
2. In the **TOS Inventory**, select a TippingPoint OS entry.
3. Do one of the following:
  - Click **Distribute**.
  - On the Menu Bar, select the **File** —> **Distribute TOS to Device** menu item.

The distribution process displays in the **Distribution Progress** section.

#### How To: Delete a TOS Entry

1. On the **Devices** Navigation pane, click **TippingPoint OS**. The **Devices - TippingPoint OS** screen displays.
2. In the **TOS Inventory**, select a TippingPoint OS entry.
3. Do one of the following:
  - Click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete** menu item.

A verification message displays.

4. Click **Yes**.

## 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 may 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.

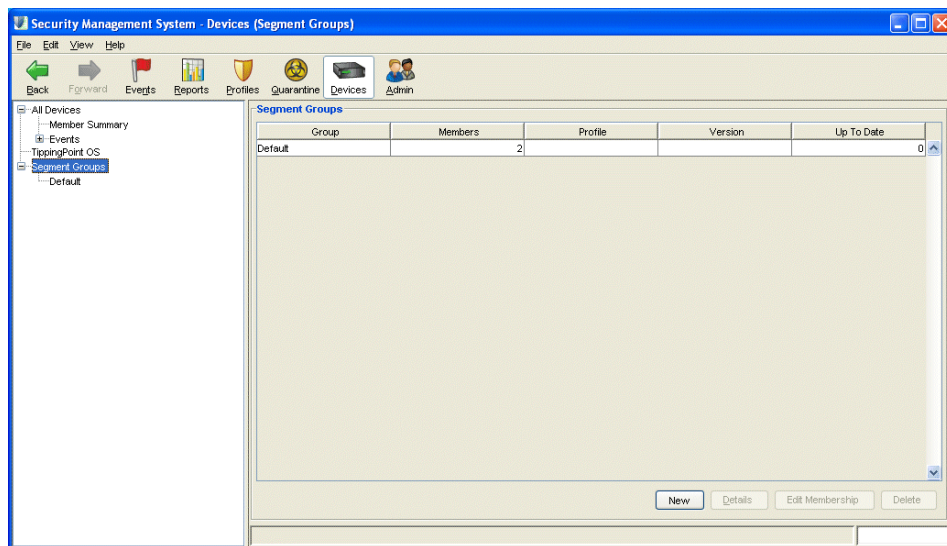


**Note** A segment can only be a member of one group and have only one distributed profile at any given time. You cannot add a segment to multiple groups.

However, you can have many profiles point to the same segment. When you distribute a profile the segment replaces the currently used profile.

The following is the **Devices - Segment Groups** screen:

**Figure 8 - 8: Devices - Segment Groups Screen**




The Segment Groups lists the segment groups with the following information:

**Table 8 - 15: Segment Group Information**

Column	Description
Group	Name of the segment group
Members	The total number of segment members
Profile	The name of the associated profile of filters
Version	The listed version of the profile
Up To Date	The total number of group members using the current profile

## Managing Segment Groups

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.

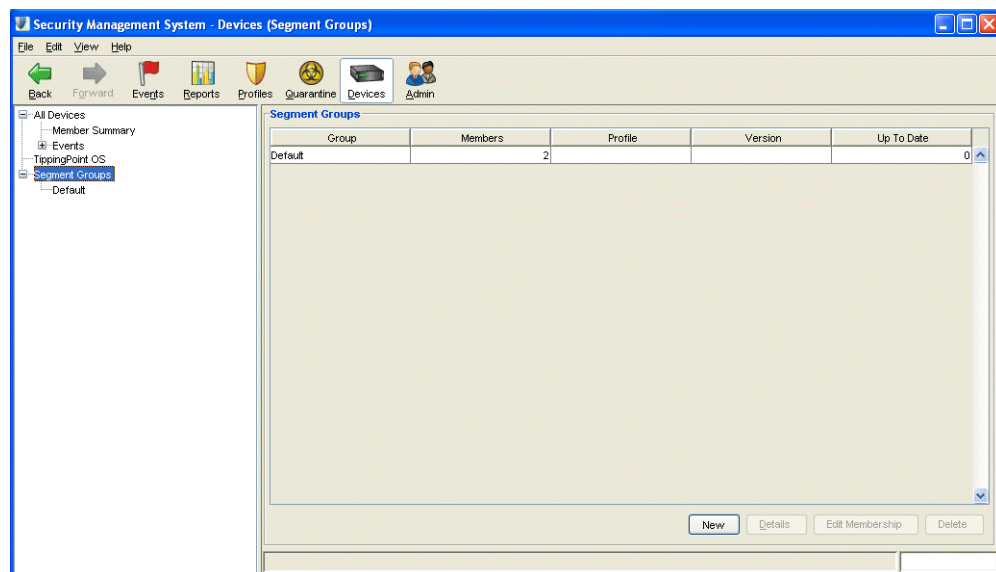
However, you can have many profiles point to the same segment. When you distribute a profile the segment replaces the currently used profile.

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

The following is the **Devices (Segment Groups)** screen.

**Figure 8 - 9: Devices (Segment Groups) Screen**



The Devices (Segment Groups) screen displays the following information:

**Table 8 - 16: Segment Group Details**

Column	Description
Device Group	User-assigned name to a group of devices

Table 8 - 16: Segment Group Details

Column	Description
Device	Device whose segments are members of the group
Segment	Segment member of the group
Description	Description of device group
Direction	Traffic direction for the segment
Profile	Profile of filters associated with the group
Version	Listed version of the profile associated with the group

You can do the following:

- [“Create/Edit a Segment Group” on page 340](#)
- [“Edit a Segment Group Member” on page 341](#)

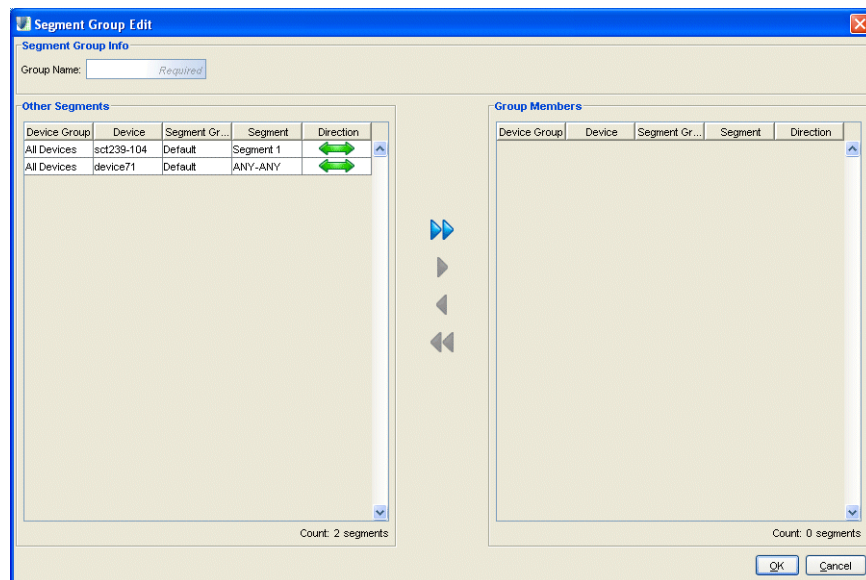
**How To: Create/Edit a Segment Group**

1. On the **Devices (Segment Groups)** screen, click **New** to create a new segment group or select an entry from the group list and click **Edit Membership**.

The **Segment Group Edit** dialog displays.

The following is the **Segment Group Edit** dialogs.

Figure 8 - 10: Segment Group Edit Dialog Box



2. In the **Group Name** field, specify a name for the group.

3. In the **Member Management** pane, select a device. You can select multiple devices by clicking and dragging your cursor over the names and using the **Shift** and **Ctrl** keys.
4. Click the right arrow button to move the selected device to the right members pane.
5. 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.
6. Click **OK**.

The segment group displays in the **Devices** Navigation pane and **Devices - Segment Group** screen.

#### How To: Edit a Segment Group Member

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 click **Edit**. The **Edit Segment Group Member** dialog displays.
3. Modify the **Segment Name**.
4. Click **OK**.

## Importing Device Profiles

After you have added and started managing a device, you may 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.

#### How To: Import a Device Profile

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 click **Import Profile**.

# IPS Devices: Device Configuration

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.



**Note** To view information about IPS configuration, you must have Operator authority. To edit device, or segment configuration, you must have Administrator authority. To do all of the above and import security packages from a device, you must have Super User authority. For more information about user authority, see [“Administration” on page 431](#).





**CAUTION** If an error occurs, the copper cable translator may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## IPS Device Configuration Wizard

The **Device Configuration Wizard** provides a convenient method for setting up the following device-specific items:

- [“Management Information” on page 344](#) — set the type of network connection the SMS uses for device communication. IPS devices have a dedicated Management Port and X-Family devices communicate using in-band management
- [“Management Routes for IPS Devices” on page 347](#) — sets routing options that enable your to communicate with network subnets other than the subnet where the Management Port is located.
- [“Services \(IPS Devices\)” on page 348](#) — configures settings for system services. You can enable one or more remote services for secure connections.
- [“AFC Settings” on page 350](#) — provides Adaptive Filtering configuration to protect against the potential adverse impact of a defective filter.
- [“HA High Availability \(IPS Devices\)” on page 351](#) — applies failure detection logic against the system
- [“Logging Mode Settings” on page 353](#) — allows users to configure setting for alerts
- [“Remote Syslog” on page 355](#)— can be used as another channel to report filter triggers.
- [“Servers \(IPS Devices\)” on page 357](#) — allows users to configure email settings for email alerts and IP address resolution. Enables applications to monitor the device.
- [“Time Settings” on page 359](#) — provides options for keeping time internally using CMOS clock or SNTP Server to check and synchronize time.
- [“TSE Settings \(IPS Devices\)” on page 363](#) — allows users to configure global settings for the Threat Suppression Engine (TSE)



The following is the **IPS Device Configuration Wizard**.

Figure 8 - 11: IPS Device Configuration Wizard

When you assume management of a device at the SMS, you can view all the activity on that machine. You can also define or edit its configuration. When you add a device that has not been configured, you must define all the parameters shown in the Configuration window. If the device has been configured, you can edit that information. You must have the Administrator role to configure a device.

To save any changes made to any pane in this window, you must click **OK**. The SMS sends the new configuration to the device immediately. The **Devices** screen lists all of the devices managed by the SMS in the **Devices** Navigation pane. You can modify all of the settings for each device through the associated tabbed screens available through the **Device Configuration** screen.



**Note** To modify all devices, you must make changes to each device and click **OK** to enter the modifications and send them to the associated device. 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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## Management Information

On the **Device Configuration (Management Information)** screen, you can 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 IPS. 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.

Through this screen, you can configure the management port, reboot, and reset filters. When you reset filters, you reset them to their recommended state. You should use this option when needed to reset filters due to issues or settings. The recommended settings for a filter may differ according filter-to-filter, including its state (enabled/disabled), notification contacts, exceptions, and action sets. this screen also provides a link to the LSM for the device.

The following is the **IPS Device Configuration (Management Information)** screen.

Figure 8 - 12: IPS Device Configuration (Management Information) Screen

The **IPS Device Configuration (Management Information)** screen provides the following settings:

Table 8 - 17: Management Port Information

Option	Description	Valid Input
Location	A description of the location of the TippingPoint device	A maximum of 32 characters describing where the TippingPoint device is located.
Hostname	The host name of your TippingPoint. It should be the same host name as the one listed for the TippingPoint device's IP address in your network DNS lookup.	A valid host name on your network segment, a maximum of 32 characters.
Model	The number of the device model, such as 2400	—
Serial Number	The serial number of the device	—
IP Address	The IP address that you will use to make a network connection to your TippingPoint device.	A valid IP address on the network segment the TippingPoint 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 TippingPoint device is attached to.	A valid network mask for the network segment on which your TippingPoint device resides in dotted decimal IP address (255.255.255.255) notation.
Default Gateway	The gateway through which the TippingPoint device communicates with external network entities, and through which external network entities communicate with the TippingPoint device. You can enter a number of gateways for <b>Gateway and Routing</b> .	A network device that contains routing tables that list the TippingPoint 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	Enable/disable auto negotiation
TOS	TippingPoint Operating System (TOS)	Settings related to this item have moved to <a href="#">"System Update" on page 328.</a>
DV	Digital Vaccine (DV) version numbers	Settings related to this item have moved to <a href="#">"System Update" on page 328.</a>

### How To: Configure the Management Port

1. From the Navigation menu, expand a specific device entry, select **Device Configuration** and then click **Edit** on the details screen.
2. On the **Device Configuration Wizard** screen, click the **Management Information** option.
3. Specify the **Name** and **Location** for the device.
4. In the **Host Management Port** section, enter the **Network Mask**.
5. In the **Gateway and Routing** section, do the following:
  - Click the **Enabled** check box.
  - Enter the **Default Gateway IP**.
  - Enter the **Destination IP, Subnet Mask, and Gateway IP**.
6. Click **OK**.

### How To: Reset Filters

1. On the **Device Configuration Wizard** screen, click the **Management Information** option.
2. To reset all filters, click **Reset Filters**. You see the following message as confirmation:

This command will reset all filters back to their recommended state. It will also delete all user-created action sets, rate limiters, traffic thresholds, etc. Would you like to continue?
3. Click **OK** to reset all filters.

After resetting the IPS filters on an X-Family or IPS, a popup notifies the user when the reset has completed. The reset process may take several minutes. Any profile distributions attempted before the reset has completed will fail, because the device is still busy resetting the filters.



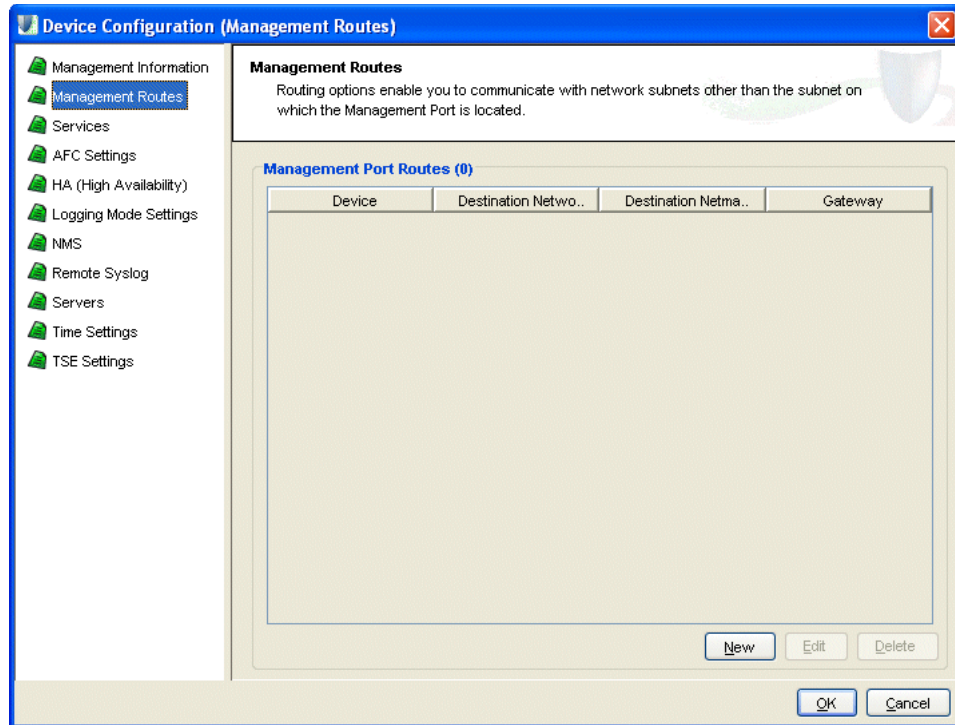
**Note** This notification is not implemented in pre-2.5 IPS's or X-Family devices. For those devices, the filter reset message displays immediately at the beginning of the reset process. For pre-2.5 devices, you can check the device System Log to determine when a filter reset has completed.

## Management Routes for IPS Devices

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.

The following is the **IPS Device Configuration (Management Routes)** screen.

Figure 8 - 13: IPS Device Configuration (Management Routes) Screen



### How To: Configure Management Routes

1. On the **Device Configuration** Wizard screen, select **Management Routes** from the navigation pane.
2. Click **New** to create a new management route or select an entry from the **Management Port Routes** list and click **Edit**.
3. In the Management dialog, specify the following information:
  - **Destination Network**
  - **Destination Netmask**
  - **Gateway**
4. Click **OK** to return to the Device Configuration Wizard.
5. Click **OK** on the Device Configuration Wizard screen to save your settings.

## Services (IPS Devices)

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 may 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. SSH and telnet require Super User access.



**Note** HTTPS service is an integral service for the SMS, always enabled and available.

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.

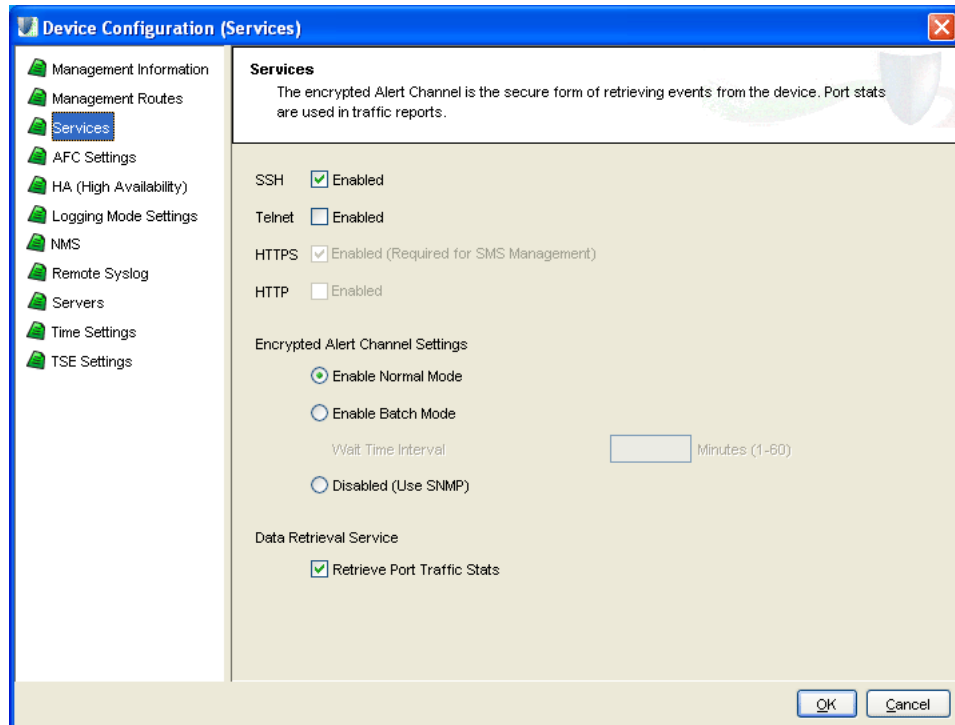
For devices using V 2.1 or higher TOS, the system can use an encrypted channel for sending messages between the device and SMS. The encrypted channel polls the device according to the mode's polling interval.

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 following is the **IPS Device Configuration (Services)** screen.

Figure 8 - 14: IPS Device Configuration (Services) Screen



The **Device Configuration (Services)** screen includes the following information:

Table 8 - 18: Services Information

Column	Description
SSH	Secure connection for using the CLI. Requires Super User access.
Telnet	Unsecure connection for using the CLI. Requires Super User access.
Encrypted Alert Channel Settings	Compiles and sends alerts. Encrypted for security. You can disable this service to use SNMP.

### How To: Configure Services

1. On the **Device Configuration** Wizard screen, select **Services** from the navigation pane. The **Device Configuration (Services)** screen displays.
2. To enable the SSH service, select the **SSH Enabled** check box. This service ensures a secure connection for the CLI.
3. To enable the Telnet service, select the **Telnet Enabled** check box. This service provides an unsecure connection for the CLI.



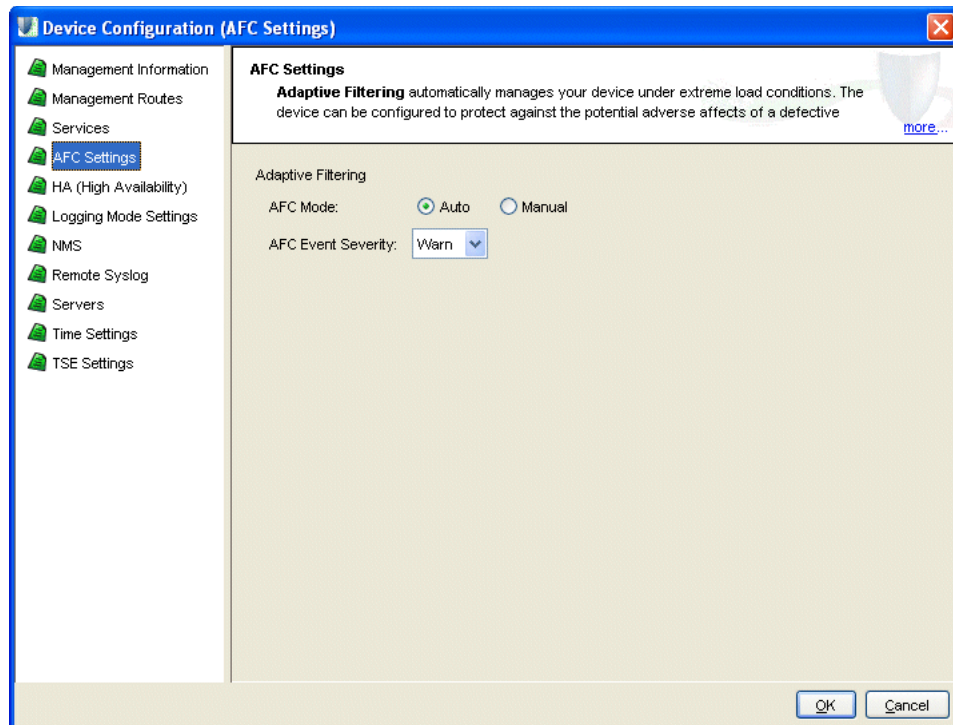
4. To enable the HTTPS service, select the **HTTPS Enabled** check box. This ensures a secure communication with the SMS and device.
5. For V 2.1 and higher TOS devices, you can configure settings for **Encrypted Alert Channel Settings**, which compile and send alerts not using SNMP. Select one of the following settings:
  - **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
6. Optionally, you can also set a **Data Retrieval** option. Select the check box to **Retrieve Port Traffic Stats**. The SMS retrieves and displays the traffic stats by port per device.
7. Click **OK**

## AFC Settings

Adaptive Filtering automatically manages your device under extreme load conditions. The device can be configured to protect against the potential adverse affects of a defective filter. On rare occurrences, the system may experience extreme load conditions that may cause the device to enter High Availability due to traffic congestion caused by filter failure.

The following is the **IPS Device Configuration (AFC Settings)** screen.

Figure 8 - 15: IPS Device Configuration (AFC Settings) Screen





## How To: Configure the AFC Settings

To prevent the device from entering HA, the device disables the filter causing the possible congestion of traffic.

1. On the **Device Configuration Wizard** screen, select **AFC Settings** from the navigation pane. The **Device Configuration (Services)** screen displays.
2. For **AFC Mode**, choose **Auto** or **Manual AFC Mode**.
3. For **Event Severity**, choose **Info**, **Warn**, **Error**, or **Critical** from the drop-down list.
4. Click **OK**.

## HA High Availability (IPS Devices)

On the **Device Configuration Wizard - HA (High Availability)** screen, you can configure settings for Intrinsic Network High Availability (INHA) and Transparent Network High Availability (TNHA). Intrinsic Network High Availability is the ability of multiple SMS and LSM applications and their IPS 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 may 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 signalling 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 fail-overs occur.

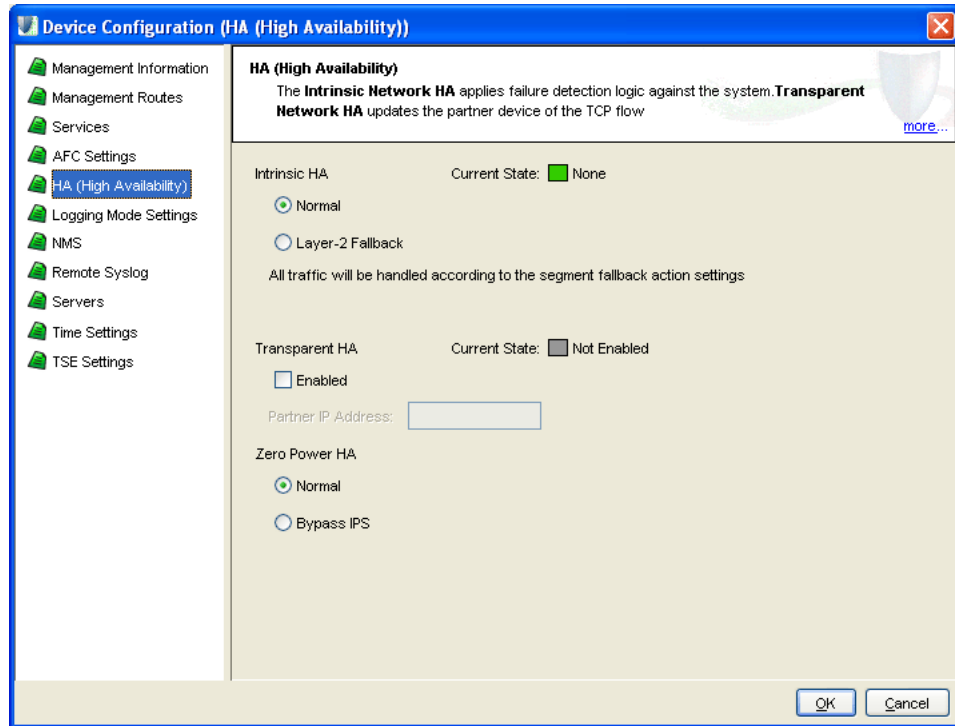
Transparent Network HA performs the same service; however, it differs by constantly updating devices of the TCP flow information. For these networks and devices, the fail-over port/device does not have to rebuild the information flow tables based on the information sent from the failing port/device. 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 Config (HA (High Availability))** screen, you can configure the following:

- **Intrinsic HA** — Directs the flow of network traffic between devices and ports when the current device fails-over.
- **Transparent HA** — Provides the same traffic management as INHA without the time and performance spent building a connection table from scratch. TNHA actively updates the connection tables between the devices for possible fail-over.
- **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.

The following is the **IPS Device Config (HA (High Availability))** screen.

Figure 8 - 16: IPS Device Config (HA (High Availability)) Screen



The **Device Config (HA (High Availability))** screen includes the following information:

Table 8 - 19: Network HA Information

Column	Description
Normal	The normal mode for the TNHA
Layer2 Fallback	The source IP address of the blocked stream
TNHA enablement	Indicates the source port of the blocked stream
Partner IP Address	The destination IP address of the blocked stream
Dest Port	Indicates the destination port of the blocked stream

## How To: Configure Network HA

1. On the **Device Configuration** Wizard screen, select **Network HA** from the navigation pane. The **Device Config (HA (High Availability))** page displays.
2. For the **Intrinsic HA**, select one of the following:
  - **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.
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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## Logging Mode Settings

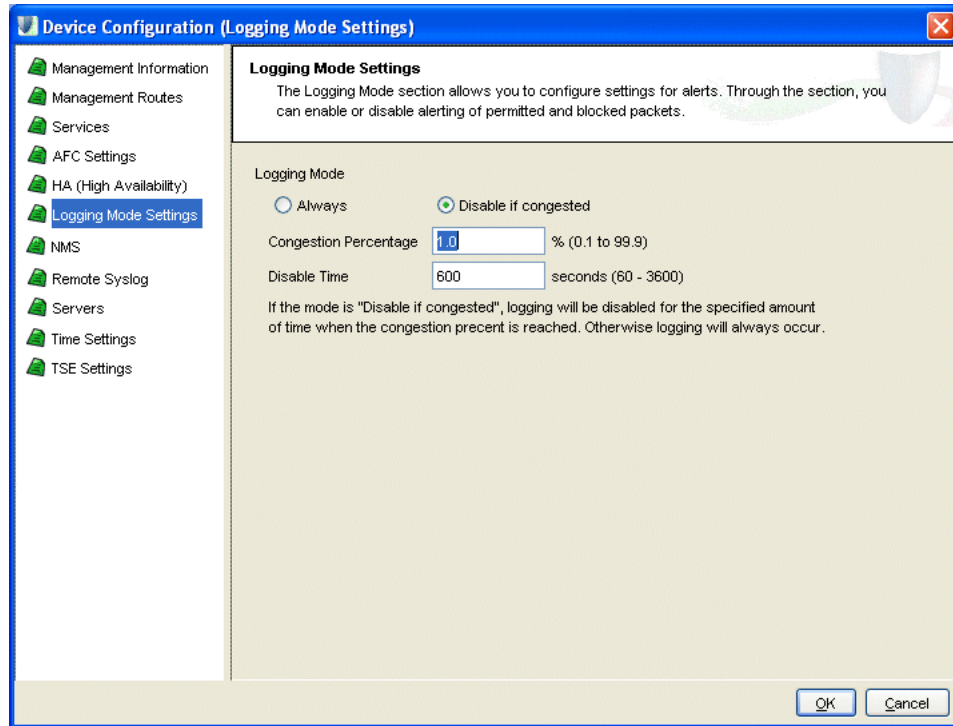
The Logging Mode section allows you to configure settings for alerts. On the **Device Config (Logging Mode Settings)** screen, you can enable or disable alerting of permitted and blocked packets. You have the option of setting the Logging Mode to **Always** or **Disable if congested**.

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 for logging to be disabled.
- **Disable Time** — amount of time in seconds (between 60 and 3600 seconds) that logging will be disabled after congestion percentage is met

The following is the **IPS Device Configuration (Logging Mode)** screen.

Figure 8 - 17: IPS Device Configuration (Logging Mode) Screen



### How To: Configure Logging Mode Settings

The Logging Mode section allows you to configure settings for alerts. Through the section, you can enable or disable alerting of permitted and blocked packets.

1. On the **Device Configuration** Wizard screen, select **Logging Mode Settings** from the navigation pane. The **Device Configuration (Logging Mode Settings)** page displays.
2. Specify the Logging Mode as **Always** or **Disable if congested**.
3. If you select **Disable if congested**, specify the following options:
  - **Congestion Percentage** — percent of congestion that triggers disable time. If the packet loss breaches the threshold, the system disables alerting according to the amount of configured time.
  - **Disable Time** — amount of time that logging will be disabled after the congestion percentage is reached. After the time period passes, alerting enables until the threshold is exceeded again.
4. Click **OK**.

### NMS for IPS Devices

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 HP OpenView™. On the **Device**

**Configuration (NMS)** screen, you can enable applications to monitor your IPS device. You can create new trap destination, edit or delete existing trap destination settings.

### How To: Configure NMS Settings

1. On the **Device Configuration Wizard** screen, 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 the **New** for a new configuration or select an existing NMS listing and click **Edit** to change an existing configuration.
4. Enter the **Trap IP Address** and the **Trap Port** (port 162 is the default port).
5. Click **OK to return to the Device Configuration Wizard screen**.
6. Click **OK** to save your settings.



**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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## 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.

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 (|). For more information about email and other contacts, see [Chapter 6, “Profiles”](#).

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 may 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.

**Table 8 - 20: Remote Syslog Field 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)
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

## How To: Create/Edit Remote Syslog Servers

1. On the **Device Configuration Wizard** screen, select **Remote Syslog** from the navigation pane. The **Device Configuration (Remote Syslog)** screen displays.
2. Click the **New** for a new configuration or select an existing listing and click **Edit** to change an existing configuration.
3. Specify an **IP Address** and **Port** for the remote server.
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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## Servers (IPS Devices)

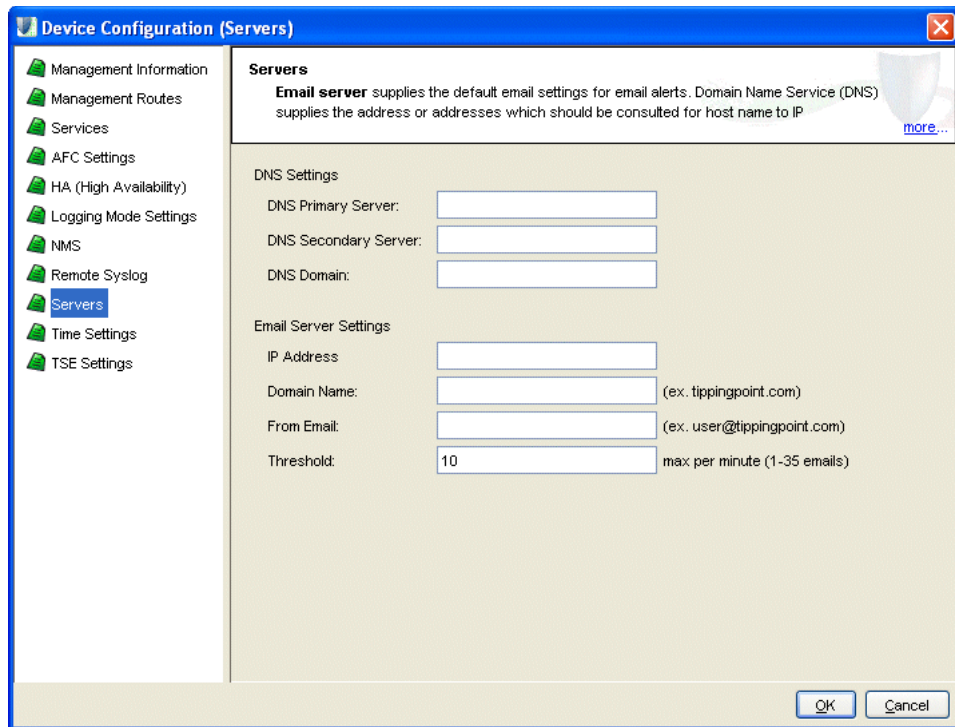
From the **Device Configuration (Servers)** screen, you can configure settings for DNS servers and Email Servers servers. Domain Name Service (DNS) supplies the address or addresses which should be consulted for host name to IP address resolution. Email server supplies the default email settings for email alerts.



**Note:** You must be sure that the IPS can reach the SMTP server that will be handling the email notifications. You may have to add a management route so that the IPS can communicate with the SMTP server.

The following is the **IPS Device Configuration (Servers)** screen.

Figure 8 - 18: IPS Device Configuration (Servers) Screen



### How To: Configure Servers

1. On the **Device Configuration** Wizard screen, select **Servers** from the navigation pane. The **Device Configuration (Servers)** screen displays.
2. In the **DNS Settings** section, specify the **Primary** and **Secondary Domain Server** IP addresses, and then enter the **DNS Domain**.
3. In the **Email Server Settings** section, 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 maximin emails per minute from 1 to 35 emails.



4. 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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## Time Settings

On the **Device Config (Time Settings)** screen, you can configure the settings for 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.

You must choose one of the following radio buttons:

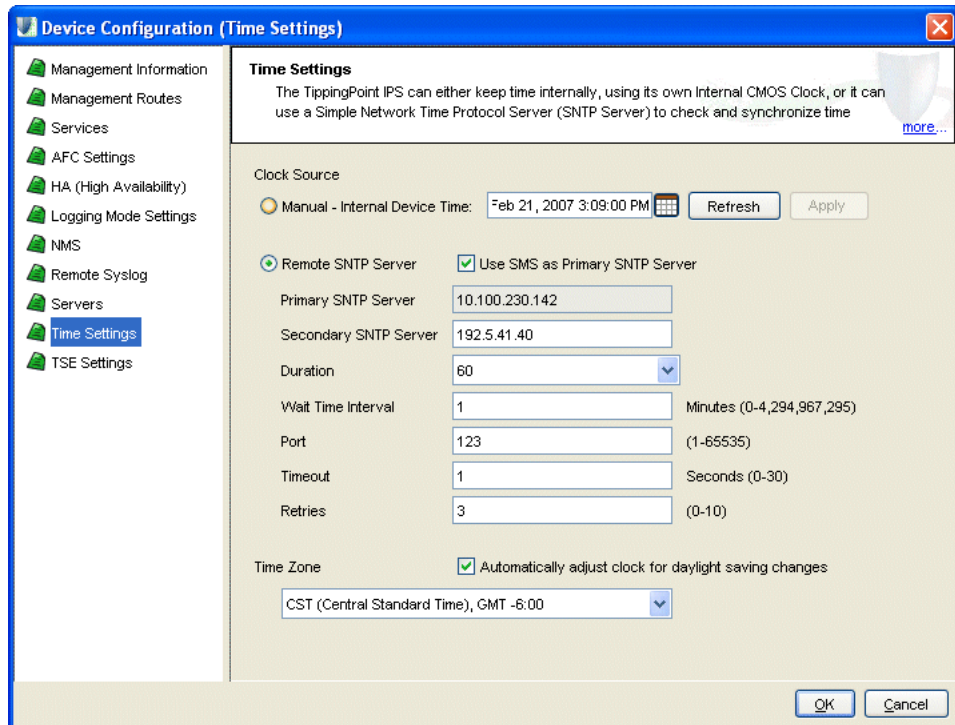
- **Internal Device Time**—sets the IPS to use its internal CMOS clock. You must then set the internal time for this device from the Local Security Manager (LSM).
- **Remote SNTP Server**—sets the IPS to use an Internet Simple Network Time Protocol (SNTP) server. You must define the **Primary SNTP Server Address**. Optionally, you can define a second server.



**Note** TippingPoint recommends that you use the SMS as your primary SNTP server. The SMS IP address is displayed at the bottom of the timekeeping panel.

The following is the **IPS Device Configuration (Time Settings)** screen.

**Figure 8 - 19: IPS Device Configuration (Time Settings) Screen**



The **Device Configuration - Time Options** screen includes the following information:

**Table 8 - 21: Time Option Information**

Column	Description
Manual/Internal Device Time	The internal time for the device. You can set this time manually.
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.
Time Zone	Indicates the time zone for the device, including an option for daylight savings time

From the Time zone drop-down menu, you can choose from the following time zones:

Table 8 - 22: Time Zone Definitions

Time Zone Code	Offset from UTC (hours)	Daylight Savings Time	Time Zone Long 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
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

Table 8 - 22: Time Zone Definitions

Time Zone Code	Offset from UTC (hours)	Daylight Savings Time	Time Zone Long Name
GMT-4	-4	OFF	Time zone GMT-4
GMT-3	-3	OFF	Time zone GMT-3
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 TippingPoint 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.

### How To: Configure the Time Options

1. On the **Device Configuration Wizard** screen, 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
  - **Remote SNTP Server** — Sets the IPS to use an Internet Simple Network Time Protocol (SNTP) server

3. If you select **Remote SNTP Server**, do the following:
  - To **Use the SMS as the Primary SNTP Server**, click the check box.
  - Enter the **Primary SNTP Server Address**.
  - Enter the **Secondary SNTP Server Address**.
  - Enter a **Duration** amount in minutes.
  - Enter an **Offset** amount in seconds.
  - Enter a **Port**.
  - Enter a **Timeout** amount in seconds.
  - Enter the amount of **Retries**.
4. In the **Time Zone** section, select a time zone from the drop-down menu.
5. To enable daylight saving time, select the **Automatically adjust clock for daylight saving changes** check box.
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.

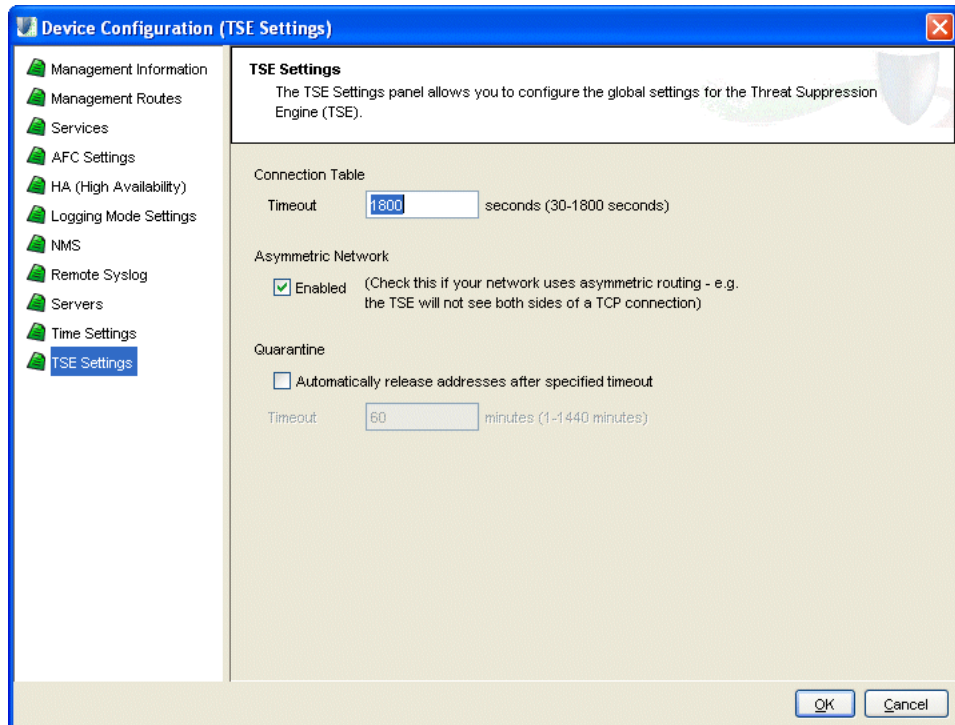
If an error occurs, the copper cable translator may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## TSE Settings (IPS Devices)

On the **Device Configuration (TSE Settings)** screen allows you to configure the global settings for the Threat Suppression Engine (TSE).

The following is the **IPS Device Configuration (TSE Settings)** screen.

Figure 8 - 20: IPS Device Configuration (TSE Settings) Screen



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 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.
- **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.

For information on monitoring TSE events, see: [“Device Monitoring” on page 309](#).

### How To: Configure TSE Settings

For information on configuring DDoS settings for E-Series devices, see [“Set DDoS Preferences” on page 429](#)

1. On the **Device Configuration** Wizard screen, select **TSE Settings** from the navigation pane. The **Device Configuration (TSE Settings)** screen displays.
2. Enter the **Connection Table Timeout**. This value is 30-1800 seconds.
3. If your network used asymmetric routing, select the check box for the **Asymmetric Network** to enable.
4. If you want to automatically release IP addresses from Quarantine after a specified amount of time, select the associated check box and then specify the **Timeout** value in minutes.
5. Click **OK**.

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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

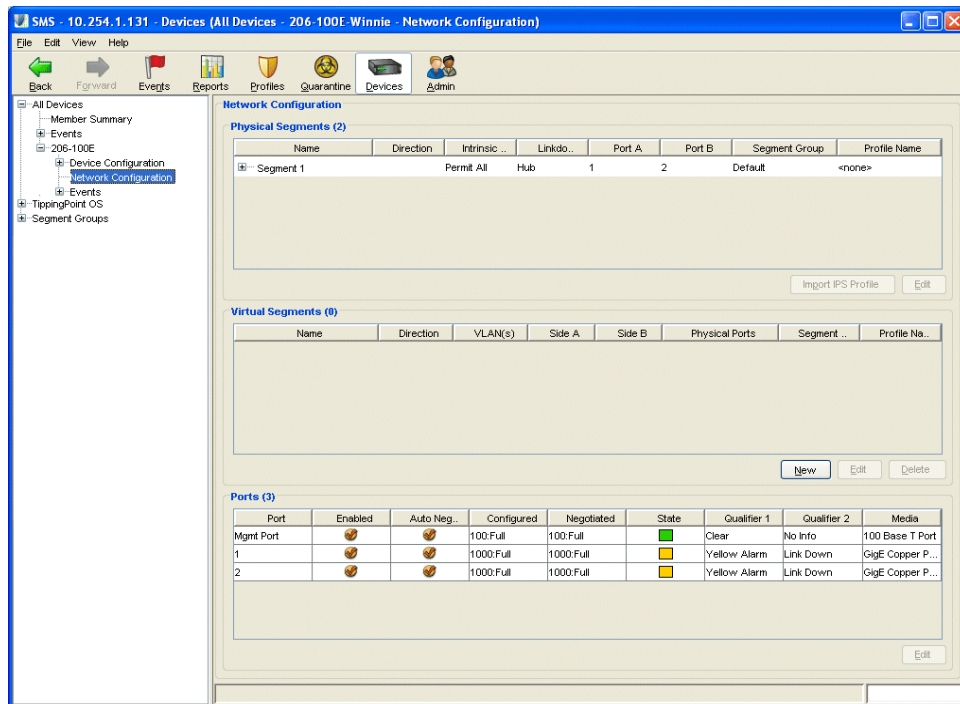


**Note** If you unmanage a device and then remanage the device, the Quarantine settings are reset to the default value.

# IPS Devices: Network Configuration

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**.

Figure 8 - 21: Devices - Network Configuration Screen for IPS Devices (V 2.5 and above)



## 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. Sets up a partition for traffic between two physical ports. 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 segment and segment groups.

## Virtual Segments

Two virtual ports make up a virtual segment. The SMS can create policies for a virtual segment in a similar manner as it does for a physical segment. Virtual segments build on the concept of physical segments by adding the ability to use existing VLAN IDs and associated rules to further tag types of



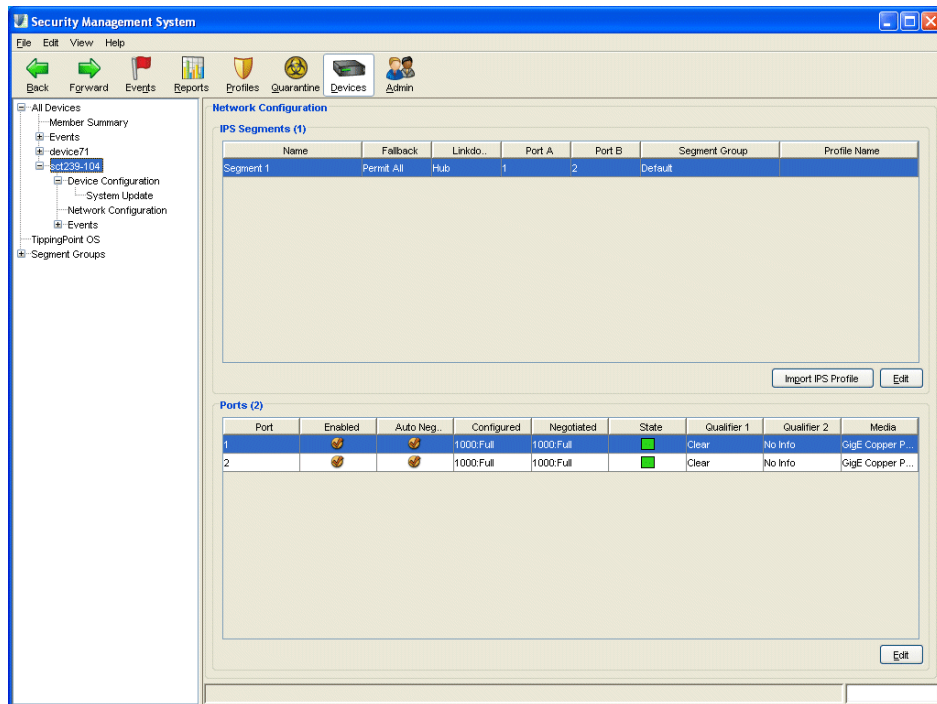
traffic. You can then apply specific filters to the virtual segment traffic or track the virtual segment traffic through SMS Events.



**Note** Virtual segments are used with V 2.5 and above device. For V 2.5+ and above, physical segments can be used but cannot be not created. Security zones are used with X-Family devices. Prior to V 2.5, IPS network configuration supported only IPS segments and ports.

For more information, see [“IPS Devices: Network Configuration” on page 366](#) and [“Network Configuration: Segments/Zones Tab” on page 395](#).

Figure 8 - 22: Devices - Network Configuration Screen for IPS Devices (prior to V 2.5)



## Link-Down Synchronization

Link-Down Synchronization, also called Sympathetic HA, 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 setting 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 does 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.

Once 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.

#### How To: Edit IPS Segment 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**.
4. In the **Physical Segments** table, select an entry and 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 Fallback mode:
  - **Block All**
  - **Permit All**
8. 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 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.
9. Click **OK**.

### How To: Create/Edit a Virtual Segment

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. From the **Virtual Segments** table, click the **New** button or select an entry from the list and click **Edit**. The setup wizard displays.
5. Specify a **Name** for the Virtual Segment and VLAN ID.
6. Click **Next** or select **Port Selection** from the wizard navigation pane.
  - Select which port pairs you want traffic with the VLAN ID(s) to be inspected on.
  - To create a Virtual Segment that applies to the entire device, select the **All Physical Ports** checkbox.
7. Click **Next** or select **Direction Labels** from the wizard navigation pane.
  - Enter a label for Side A — port 1 of the segment
  - Enter a label for Side B — located on the left of segment when viewing the device.

The sides can be named to represent meaningful traffic flow for your particular network, such as Finance, Core, etc.

8. Click **Next** or select **Segment Groups** from the wizard navigation pane.



**Note:** 2.5.1 and later IPS devices support segment group membership by direction.

- If you want to track traffic by direction or apply different profiles, place each direction in different segment groups.
9. Click **Finish** or **OK**.

### How To: 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**.
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 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.

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.

To resolve this issue, use the following procedure:

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 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.

#### How To: 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 select **Network Configuration**.
2. Select segment from the **IPS Segments** table, and then do one of the following tasks:
  - Click **Import IPS Profile**.
  - On the Menu Bar, select the **File** —> **Import Profile from Device** menu item.
3. The SMS imports the filters from the device into the SMS. The SMS names the profile using the segment's 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 [“IPS Profiles \(All Devices\)” on page 157](#) for more information on distributing profiles.

## IPS Devices: Event Monitoring

Through the **Events** screen for an individual device, you can monitor the following system-specific information:

- [IPS Device Events: System Log](#)
- [IPS Device Events: Audit Log](#)



For additional information on monitoring your IPS device, see [“Device Monitoring” on page 309](#).

You can do the following:

- [View Log](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

### How To: View Log

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device and expand the options.
3. Select a log option:
  - **Audit Log** — Displays the audit log. See [“IPS Device Events: Audit Log” on page 373](#).
  - **System Log** — Displays the system log. See [“IPS Device Events: System Log” on page 372](#).

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:
  - Select a **Start Time**. Click the calendar icon  and select the start and end times for the range. See [“Date and Time Controls” on page 37](#).
  - Select an **End Time**. Click the calendar icon  and select the start and end times for the range. See [“Date and Time Controls” on page 37](#).
  - Click **Refresh**.

### How To: Reset Logs

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device.
3. Click **Device Health and Stats**.

4. Do one of the following:
  - Display a log screen and click **Reset**.
  - On the Menu Bar, select the **File** —> **Reset Device Logs** menu item and select the log you want to reset: system, audit, alert, block, or all.
  - To reset all logs, you can select the **All Logs** option. On the Menu Bar, select the **File** —> **Reset Device Logs** —> **All Logs** menu item.

 **Note** Resetting all logs does not reset the audit log.

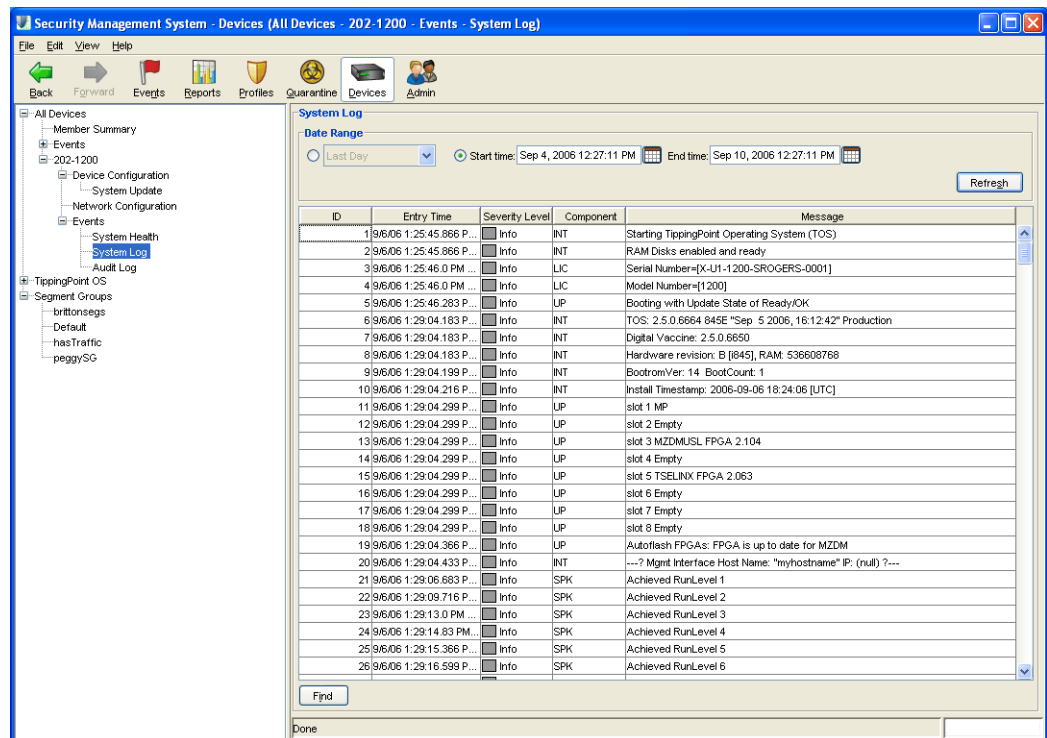
## IPS Device Events: System Log

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” on page 314](#) for more information.

The following is the **Devices - System Log** screen.

Figure 8 - 23: Devices - System Log Screen



ID	Entry Time	Severity Level	Component	Message
1	9/6/06 1:25:45.866 P...	Info	INT	Starting TippingPoint Operating System (TOS)
2	9/6/06 1:25:45.866 P...	Info	INT	RAM Disks enabled and ready
3	9/6/06 1:25:46.0 PM ...	Info	LIC	Serial Number={X-UI-1200-SROGERS-0001}
4	9/6/06 1:25:46.0 PM ...	Info	LIC	Model Number={1200}
5	9/6/06 1:25:46.283 P...	Info	UP	Booting with Update State of Ready/OK
6	9/6/06 1:29:04.183 P...	Info	INT	TOS: 2.5.0.6664 845E "Sep 5 2006, 16:12:42" Production
7	9/6/06 1:29:04.183 P...	Info	INT	Digital Vaccine: 2.5.0.6650
8	9/6/06 1:29:04.183 P...	Info	INT	Hardware revision: B [645], RAM: 536608768
9	9/6/06 1:29:04.199 P...	Info	INT	BootromVer: 14 BootCount: 1
10	9/6/06 1:29:04.216 P...	Info	INT	Install Timestamp: 2006-09-06 18:24:06 [UTC]
11	9/6/06 1:29:04.299 P...	Info	UP	slot 1 MP
12	9/6/06 1:29:04.299 P...	Info	UP	slot 2 Empty
13	9/6/06 1:29:04.299 P...	Info	UP	slot 3 MZDMUSL FPGA 2.104
14	9/6/06 1:29:04.299 P...	Info	UP	slot 4 Empty
15	9/6/06 1:29:04.299 P...	Info	UP	slot 5 TSELINX FPGA 2.063
16	9/6/06 1:29:04.299 P...	Info	UP	slot 6 Empty
17	9/6/06 1:29:04.299 P...	Info	UP	slot 7 Empty
18	9/6/06 1:29:04.299 P...	Info	UP	slot 8 Empty
19	9/6/06 1:29:04.366 P...	Info	UP	Autoflash FGAs: FPGA is up to date for MZDM
20	9/6/06 1:29:04.433 P...	Info	INT	...7 Mgmt Interface Host Name: "myhostname" IP: (null) ?---
21	9/6/06 1:29:06.683 P...	Info	SPK	Achieved RunLevel 1
22	9/6/06 1:29:09.716 P...	Info	SPK	Achieved RunLevel 2
23	9/6/06 1:29:13.0 PM ...	Info	SPK	Achieved RunLevel 3
24	9/6/06 1:29:14.83 PM...	Info	SPK	Achieved RunLevel 4
25	9/6/06 1:29:15.366 P...	Info	SPK	Achieved RunLevel 5
26	9/6/06 1:29:16.599 P...	Info	SPK	Achieved RunLevel 6

The following table details the system log details:

**Table 8 - 23: 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](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

## IPS Device Events: Audit Log

The audit log keeps track of device user activity that may have security implications. This activity includes user attempts (successful and unsuccessful) to do the following:

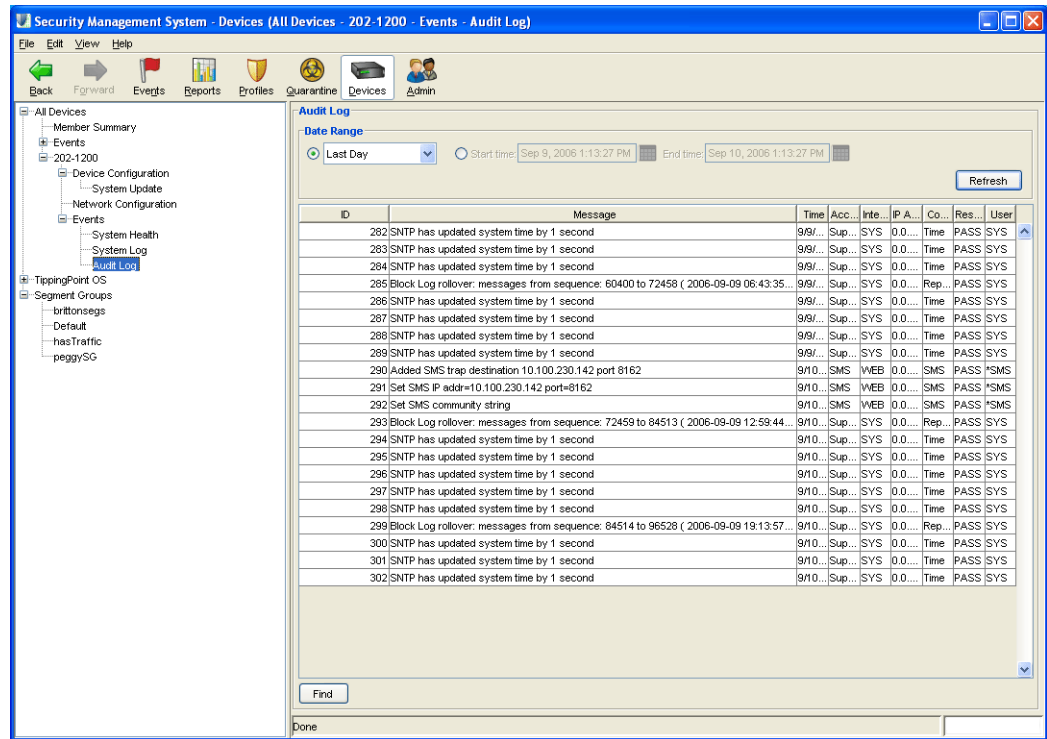
- Change user information
- Change device configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings



**Note** Only Super User level users can view, reset, and download the audit log.

The following is the **Devices - Audit Log** screen.

Figure 8 - 24: Devices - Audit Log Screen



The following table details the audit log details:

Table 8 - 24: 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, Super User, 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](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

When you view the log, the user listed for the logged events may include SMS, LSM, and CLI. These entries are entered by those applications into the audit log, as a Super User level of access.

## X-Family Devices: Device Configuration

The **Device Configuration Wizard** provides a convenient method for setting up the following device-specific items:

- [“Management Information” on page 376](#) — set the type of network connection the SMS uses for device communication. IPS devices have a dedicated Management Port and X-Family devices communicate using in-band management
- [“Services for X-Family Devices” on page 378](#) — configures settings for system services. You can enable one or more remote services for secure connections.
- [“AFC Settings” on page 380](#) — provides Adaptive Filtering configuration to protect against the potential adverse impact of a defective filter.
- [“Virtual Firewall HA for X-Family Devices” on page 381](#)
- [“Logging Mode Settings” on page 382](#) — allows users to configure setting for alerts
- [“NMS” on page 383](#)— can be used as another channel to report filter triggers.
- [“Servers” on page 386](#) — allows users to configure email settings for email alerts and IP address resolution.
- [“Time Settings” on page 387](#) — provides options for keeping time internally using CMOS clock or SNTP Server to check and synchronize time.
- [“TSE Settings” on page 391](#) — allows users to configure global settings for the Threat Suppression Engine (TSE)

### X-Family Device Configuration Wizard

When you assume management of a device at the SMS, you can view all the activity on that machine. You can also define or edit its configuration. When you add a device that has not been configured, you must define all the parameters shown in the Configuration window. If the device has been configured, you can edit that information. You must have the Administrator role to configure a device.

To save any changes made to any pane in this window, you must click **OK**. The SMS sends the new configuration to the device immediately. The **Devices** screen lists all of the devices managed by the

SMS in the **Devices** Navigation pane. You can modify all of the settings for each device through the associated tabbed screens available through the **Device Configuration** screen.



**Note** To modify all devices, you must make changes to each device and click **OK** to enter the modifications and send them to the associated device. 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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## Management Information

On the **Device Configuration (Management Information)** screen, you can 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 IPS. 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.

Through this screen, you can configure the management port, reboot, and reset filters. When you reset filters, you reset them to their recommended state. You should use this option when needed to reset filters due to issues or settings. The recommended settings for a filter may differ according filter-to-filter, including its state (enabled/disabled), notification contacts, exceptions, and action sets. This screen also provides a link to the LSM for the device.

Figure 8 - 25: Device Configuration (Management Information) Screen for X-Family Devices

The screenshot displays the 'Device Configuration (Management Information)' window. On the left is a navigation pane with options: Management Information (selected), Services, AFC Settings, Virtual Firewall HA, Logging Mode Settings, NMS, Remote Syslog, Servers, Time Settings, and TSE Settings. The main area is titled 'Management Information' and contains the following sections:

- General:** Hostname (210-X506), Location (room/rack), Model (TippingPoint X506), Serial Number (X-X506-SROGERS-0003).
- Host Management Information:** IP Address (192.168.66.210), Network Mask (255.255.255.0), Default Gateway (192.168.66.1) with an 'Enabled' checkbox checked.
- Software:** TOS (2.5.1.6812), DV (2.5.0.7194).

At the bottom, there are buttons for 'Reboot', 'Shutdown', and 'Reset IPS Filters', along with a 'View LSM' link. The window concludes with 'OK' and 'Cancel' buttons.

The **Device Configuration - Management Information** screen provides the following settings:

**Table 8 - 25: Management Port Information**

Option	Description	Valid Input
Model Number	The number of the device model, such as 2400	—
Serial Number	The serial number of the device	—
Name	The host name of your TippingPoint. It should be the same host name as the one listed for the TippingPoint device's 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 the TippingPoint device	A maximum of 32 characters describing where the TippingPoint device is located.
IP Address	The IP address that you will use to make a network connection to your TippingPoint device.	A valid IP address on the network segment the TippingPoint 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 TippingPoint device is attached to	A valid network mask for the network segment on which your TippingPoint device resides in dotted decimal IP address (255.255.255.255) notation.
Default Gateway	The gateway through which the TippingPoint device communicates with external network entities, and through which external network entities communicate with the TippingPoint device. You can enter a number of gateways for <b>Gateway and Routing</b> .	A network device that contains routing tables that list the TippingPoint device and external network entities as well
Software	TippingPoint Operating System (TOS) and Digital Vaccine (DV) version numbers	Setting related to this item have moved to <a href="#">"System Update" on page 328</a> .

### How To: Configure the Management Port

1. From the Navigation menu, expand a specific device entry, select **Device Configuration** and then click **Edit** on the details screen.
2. On the **Device Configuration** Wizard screen, click the **Management Information** option.
3. Specify the **Name** and **Location** for the device.
4. In the **Host Management Port** section, enter the **Network Mask**.

5. In the **Gateway and Routing** section, do the following:
  - Click the **Enabled** check box.
  - Enter the **Default Gateway IP**.
  - Enter the **Destination IP, Subnet Mask, and Gateway IP**.
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.

### How To: Reset Filters

1. On the **Device Configuration Wizard** screen, click the **Management Information** option.
2. To reset all filters, click **Reset Filters**. You see the following message as confirmation:

This command will reset all filters back to their recommended state. It will also delete all user-created action sets, rate limiters, traffic thresholds, etc. Would you like to continue?
3. Click **OK** to reset all filters.

### Services for X-Family Devices

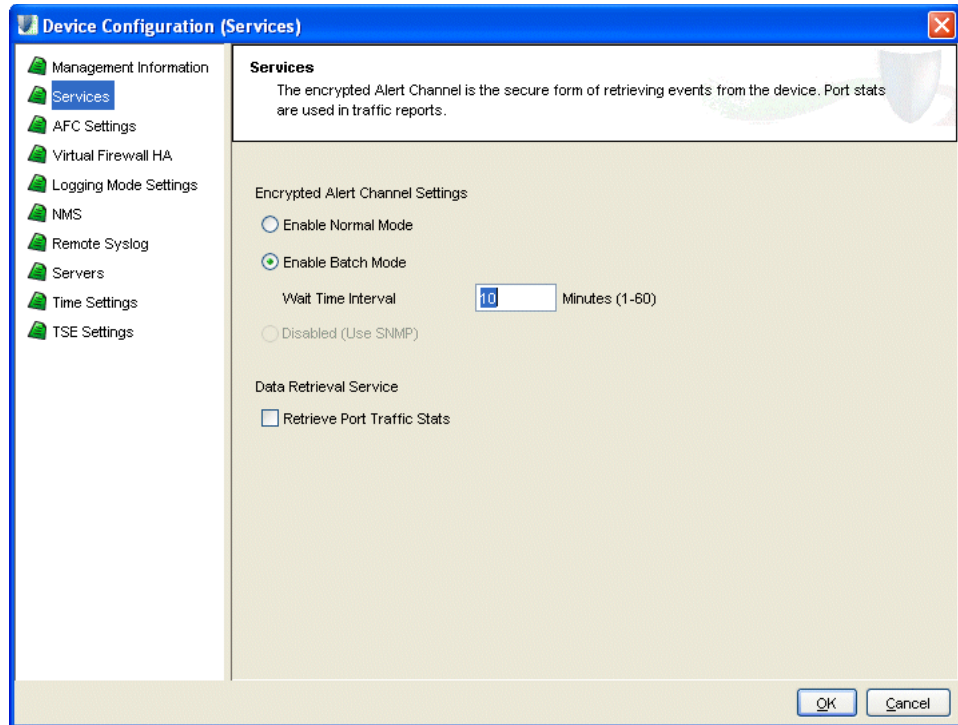
On the **Device Configuration (Services)** screen, you can configure settings for the encrypted Alert Channel, which is a secure form of retrieving events from the device.

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.
- **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. This option is the default.

The following is the **Device Configuration (Services)** screen for X-Family devices.

Figure 8 - 26: Device Configuration (Services) Screen for X-Family Devices



### How To: Configure Services

1. On the **Device Configuration Wizard** screen, select **Services** from the navigation pane. The **Device Configuration (Services)** screen displays.
2. For V 2.1 and higher TOS devices, you can configure settings for **Encrypted Alert Channel Settings**, which compile and send alerts not using SNMP. Select one of the following settings:
  - **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
3. Optionally, you can also set a **Data Retrieval** option. Select the check box to **Retrieve Port Traffic Stats**. The SMS retrieves and displays the traffic stats by port per device.
4. 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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

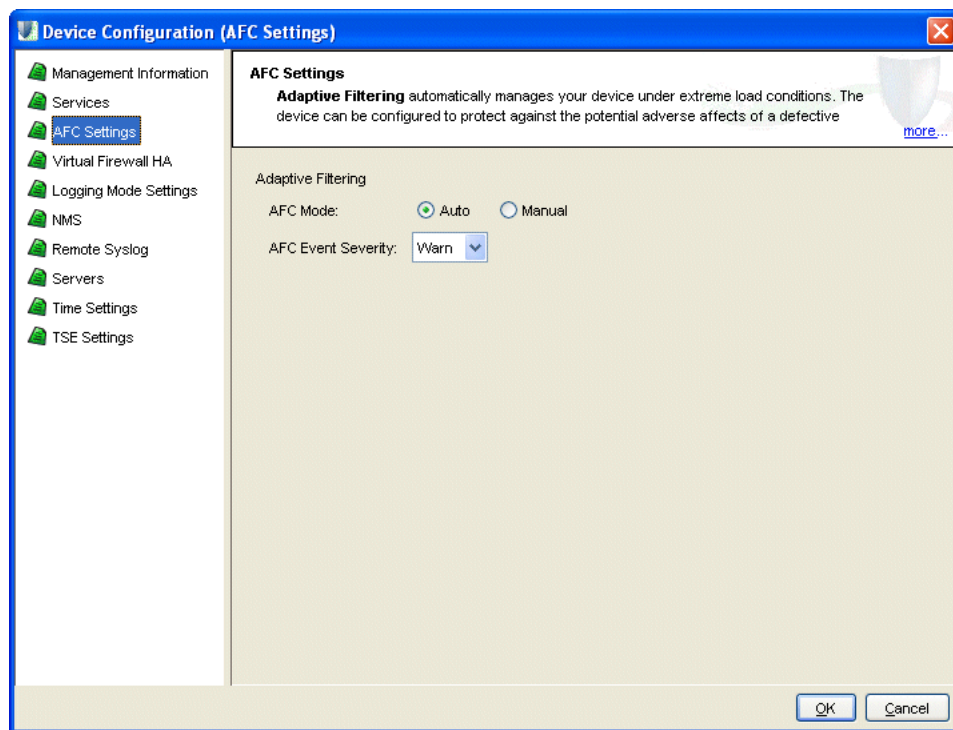
## AFC Settings

Adaptive Filtering automatically manages your device under extreme load conditions. The device can be configured to protect against the potential adverse affects of a defective filter. On rare occurrences, the system may experience extreme load conditions that may cause the device to enter High Availability due to traffic congestion caused by filter failure.

To prevent the device from entering HA, the device disables the filter causing the possible congestion of traffic. For **AFC Mode**, choose **Auto** or **Manual** AFC Mode. For **Event Severity**, choose **Info**, **Warn**, **Error**, or **Critical**.

The following is the **Device Configuration (AFC Settings)** screen for X-Family devices.

Figure 8 - 27: Device Configuration (AFC Settings) Screen for X-Family Devices



### How To: Configure the AFC Settings

To prevent the device from entering HA, the device disables the filter causing the possible congestion of traffic.

1. On the **Device Configuration** Wizard screen, select **AFC Settings** from the navigation pane. The **Device Configuration (Services)** screen displays.
2. For **AFC Mode**, choose **Auto** or **Manual** AFC Mode.
3. For **Event Severity**, choose **Info**, **Warn**, **Error**, or **Critical** from the drop-down list.
4. Click **OK**.

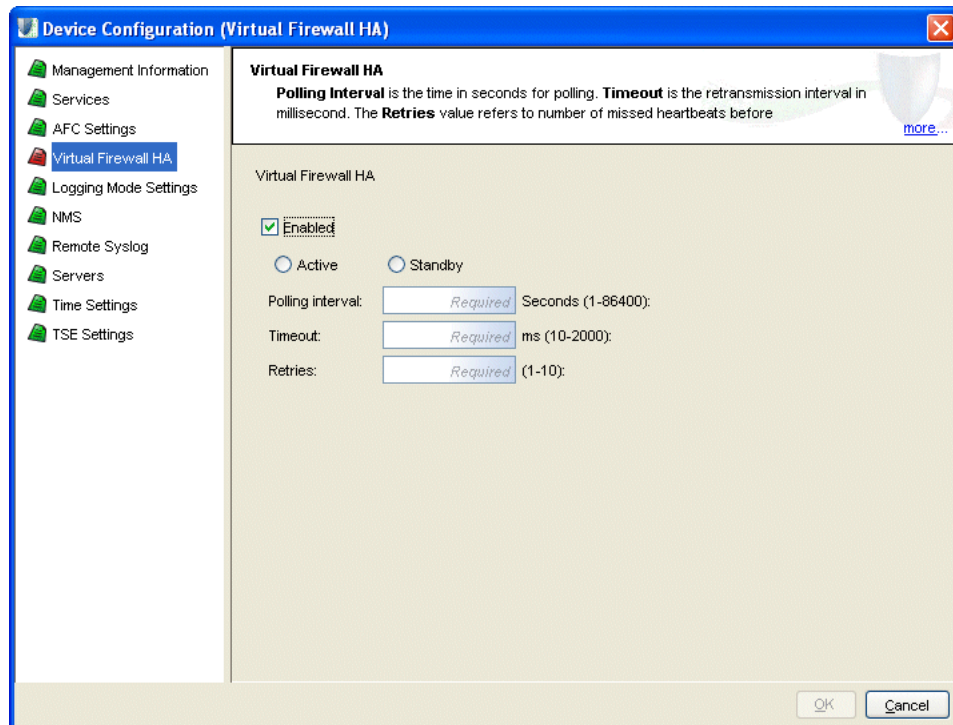


## Virtual Firewall HA for X-Family Devices

From the **Device Configuration (Virtual Firewall HA)** screen you can enable the Virtual Firewall High Availability (HA) feature and set the function to **Active** or **Standby** mode.

The following is the **Device Configuration (Virtual Firewall HA)** screen for X-Family devices.

Figure 8 - 28: Device Configuration (Virtual Firewall HA) Screen for X-Family Devices



Configure the following settings:

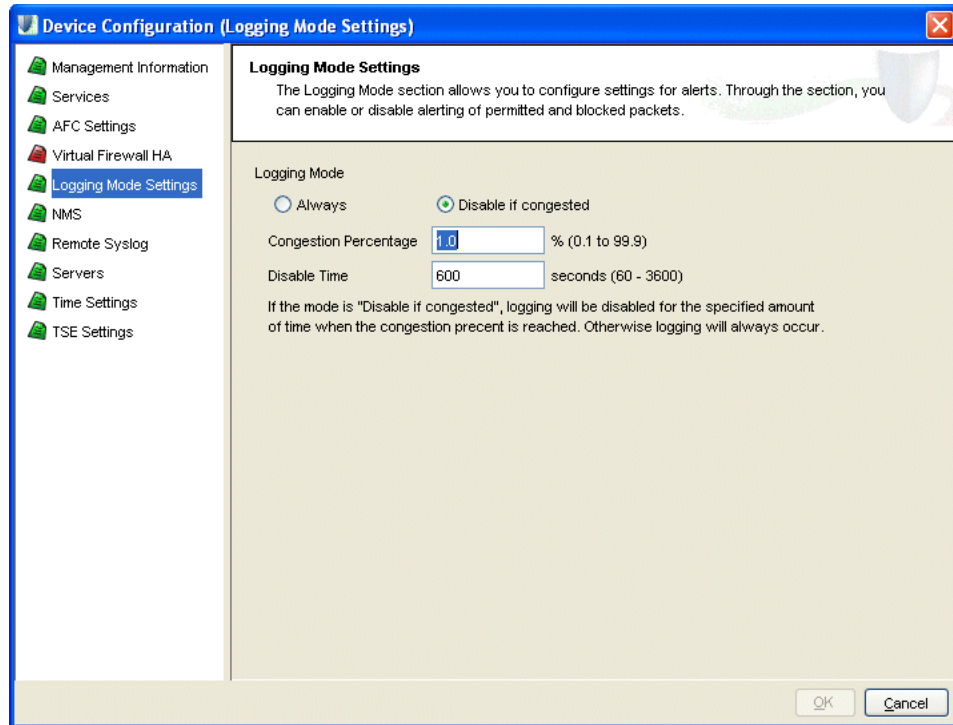
1. On the **Device Configuration Wizard** screen, select **Virtual Firewall HA** from the navigation pane. The **Device Configuration (Virtual Firewall HA)** screen displays.
2. To enable the **Virtual Firewall HA**, select the **Enabled** check box, and then select with **Active** or **Standby**.
3. Specify the following information:
  - **Polling Interval** — the time in seconds for polling
  - **Timeout** — retransmission interval in milliseconds
  - **Retries** — value refers to number of missed heartbeats before failover.
4. Click **OK**.

## Logging Mode Settings

The Logging Mode section allows you to configure settings for alerts. On the **Device Config (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**.

The following is the **Device Configuration (Logging Mode)** screen for X-Family devices.

Figure 8 - 29: Device Configuration (Logging Mode) Screen for X-Family Devices



### How To: Configure Logging Mode Settings

The Logging Mode section allows you to configure settings for alerts. Through the section, you can enable or disable alerting of permitted and blocked packets.

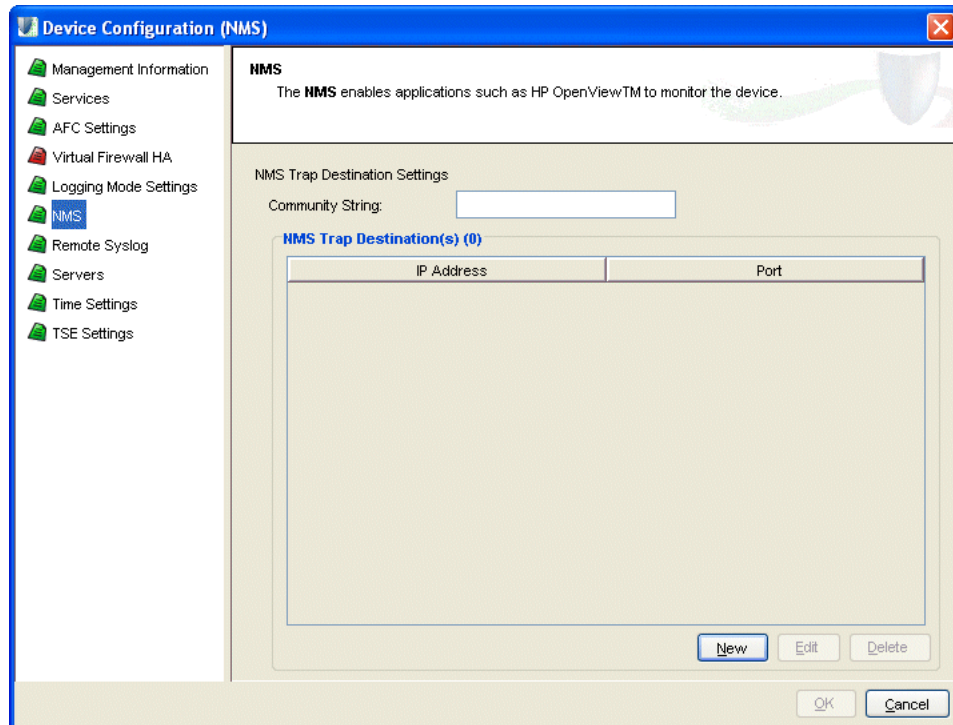
1. On the **Device Configuration Wizard** screen, select **Logging Mode Settings** from the navigation pane. The **Device Configuration (Logging Mode Settings)** page displays.
2. Specify the Logging Mode as **Always** or **Disable if congested**.
3. If you select **Disable if congested**, specify the following options:
  - **Congestion Percentage** — percent of congestion that triggers disable time.
  - **Disable Time** — amount of time that logging will be disabled after the congestion percentage is reached.
4. Click **OK**.



## NMS

The NMS enables applications such as HP OpenView™ to monitor the device. Port 123 is the default

Figure 8 - 30: Device Configuration (NMS) Screen for X-Family Devices



### How To: Configure NMS

1. On the **Device Configuration** Wizard screen, select **NMS** from the navigation pane. The **Device Configuration (NMS)** page displays.
2. In the NMS Trap Destination Setting Section, enter or edit a **Community String** (1-31 characters).
3. Click the **New** to create a new NMS configuration or select an existing NMS listing and click **Edit** to change a configuration.
4. Enter the **Trap IP Address** and the **Trap Port**.
5. Click **OK**.
6. On the **Devices** screen, click **OK**

## 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.

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 (|). For more information about email and other contacts, see [Chapter 6, “Profiles”](#).

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 may 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-
00000000164,"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-
00000000164,"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.

**Table 8 - 26: Remote Syslog Field 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)


Table 8 - 26: Remote Syslog Field Descriptions

Field	Description
5	Sequence ID
6	(reserved)
7	Action performed (Block or Permit)
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

### How To: Create/Edit Remote Syslog Servers

1. On the **Device Configuration** Wizard screen, select **Remote Syslog** from the navigation pane. The **Device Configuration (Remote Syslog)** screen displays.
2. Select the type of server(s) and enter the IP Address for the log server(s) you selected.
3. Click the **New** for a new configuration or select an existing listing and click **Edit** to change an existing configuration.
4. Enter an **IP Address**.
5. Enter a **Port**.
6. Select an **Alert Facility** from the drop-down menu: none or select from a range of 0 to 31.
7. Select a **Block Facility** from the drop-down menu: none or select from a range of 0 to 31.
8. Select a **Delimiter** for the generated logs: **Horizontal Tab**, **Comma**, **Semi-colon**, or **Pipe**.
9. Click **OK**.

10. 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.

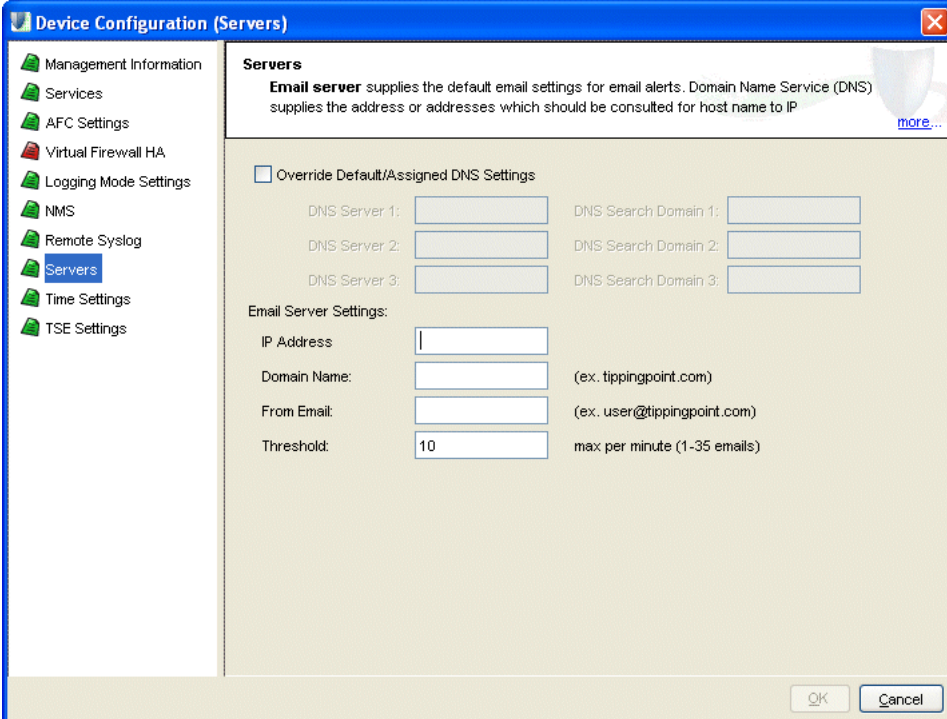
If an error occurs, the copper cable translator may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Blue” on page 543](#).

## Servers

From the **Device Configuration (Servers)** screen, you can define the mail server used by the IPS to notify e-mail contacts about attacks and configure NMS trap destination settings

The following is the **Device Configuration (Servers)** screen for X-Family devices.

Figure 8 - 31: Device Configuration (Servers) Screen for X-Family Devices



### How To: Configure Servers

1. On the **Device Configuration Wizard** screen, select **Servers** from the navigation pane. The **Device Configuration (Servers)** screen displays.
2. If you want to override DNS settings, select the **Override Default/Assigned DNS Settings** check box and complete the respective entries for the DNS server(s) and DNS Search Domain(s).

3. In the **Email Server Settings** section, 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.
4. 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 may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

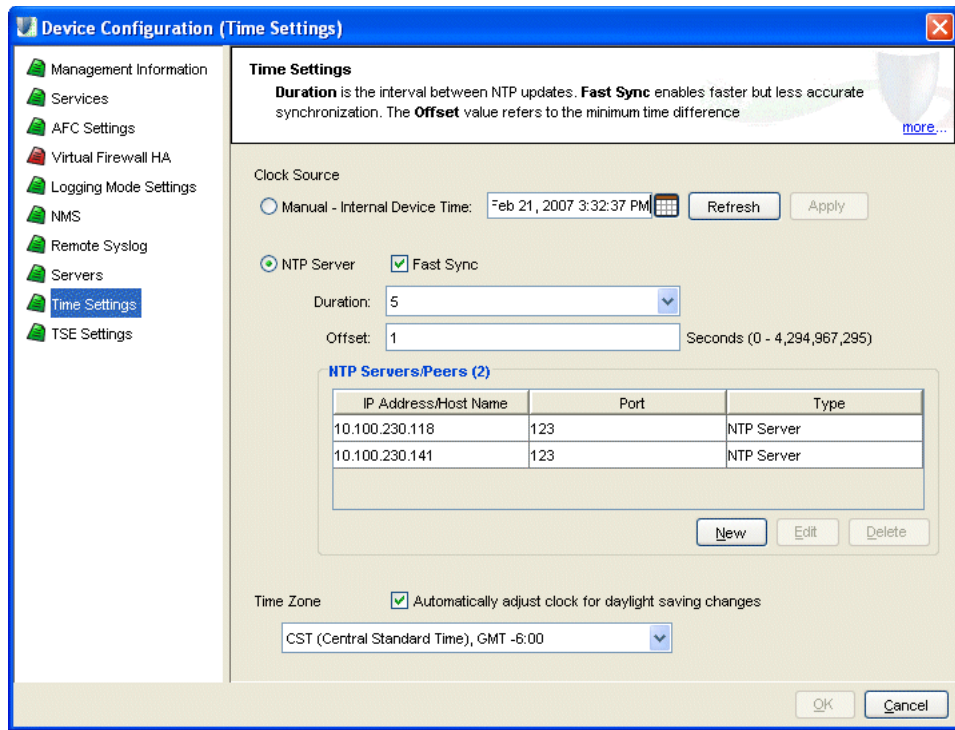
## Time Settings

On the **Device Config (Time Settings)** screen, you can configure the settings for 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.



**Note** TippingPoint recommends that you use the SMS as your primary SNTP server. The SMS IP address is displayed at the bottom of the timekeeping panel.

Figure 8 - 32: Device Configuration (Time Settings) Screen for X-Family Devices



The **Device Configuration - Time Options** screen includes the following information:

Table 8 - 27: Time Option Information

Column	Description
Internal Device Time	The internal time for the device.
NTP Server	A remote timekeeping server for the device.
Fast Sync	Enables faster but less accurate synchronization.
Duration	The interval between NTP updates.
Offset	Refers to the minimum time difference before NTP updates clock.
Time Zone	Indicates the time zone for the device, including an option for daylight savings time

From the Time zone drop-down menu, you can choose from the following time zones:

**Table 8 - 28: Time Zone Definitions**

Time Zone Code	Offset from UTC (hours)	Daylight Savings Time	Time Zone Long 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
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

Table 8 - 28: Time Zone Definitions

Time Zone Code	Offset from UTC (hours)	Daylight Savings Time	Time Zone Long Name
GMT-4	-4	OFF	Time zone GMT-4
GMT-3	-3	OFF	Time zone GMT-3
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 TippingPoint 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.

### How To: Configure the Time Options

1. From the Navigation menu, expand a specific device entry, select **Device Configuration** and then click **Edit** on the details screen.
2. On the **Device Configuration Wizard** screen, click the **Time Settings** options. The **Device Configuration (Time Settings)** screen displays.
3. In the **Clock Source** section, select one of the following:
  - **Manual/Internal Device Time** — Sets the IPS to use its internal CMOS clock
  - **Remote NTP Server** — Sets the IPS to use an Internet Network Time Protocol (NTP) server



4. If you select **Remote NTP Server**, do the following:
  - Select a **Duration** amount in minutes from the drop-down box.
  - Enter an **Offset** amount in seconds.
5. To configure NTP Servers/Peers, click **New** to create a new setting or select from the **NTP Servers/Peers** table and click **Edit**.
  - Enter or edit the IP Address/Host Name.
  - Enter or edit the Port.
  - Select the type of NTP sever from the drop-down box.
  - Click **OK** to return to the Device Configuration Wizard screen for Time Settings.
6. To enable daylight saving time, select the **Automatically adjust clock for daylight saving changes** check box.
7. In the **Time Zone** section, select a time zone from the drop-down menu.
8. 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.

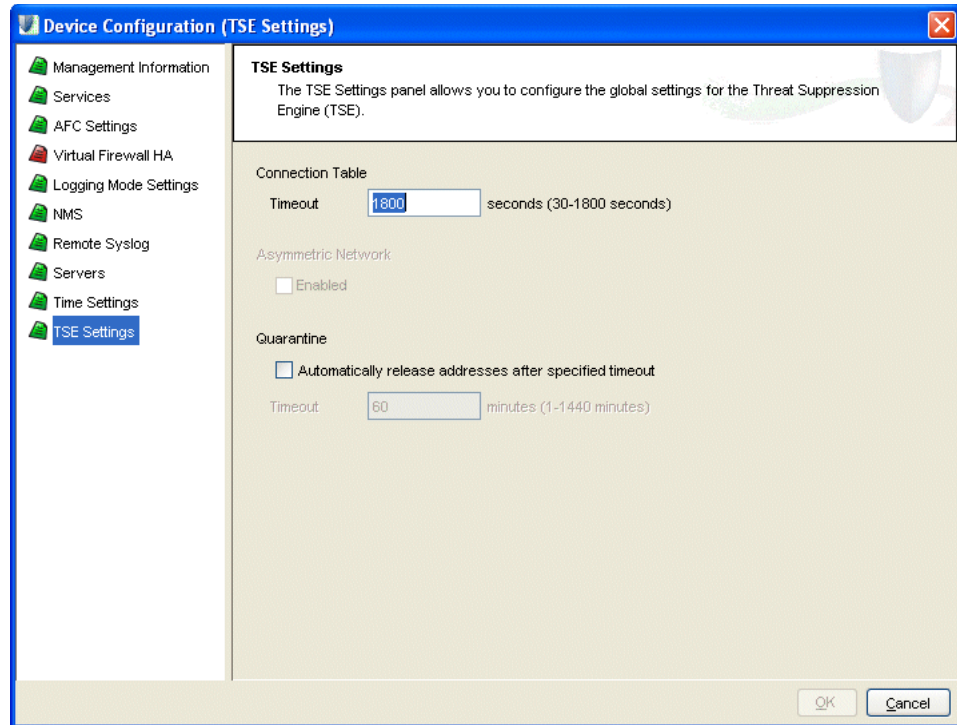
If an error occurs, the copper cable translator may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## TSE Settings

On the **Device Configuration (TSE Settings)** screen allows you to configure the global settings for the Threat Suppression Engine (TSE).

The following is the Device Configuration (TSE Settings) screen for X-Family devices.

Figure 8 - 33: Device Configuration (TSE Settings) Screen for X-Family Devices



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 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.
- **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.

For information on monitoring TSE events, see [“Device Monitoring” on page 309](#).

#### How To: Configure TSE Settings

1. On the **Device Configuration** Wizard screen, select **TSE Settings** from the navigation pane. The **Device Configuration (TSE Settings)** screen displays.
2. Enter the **Connection Table Timeout**. This value is 30-1800 seconds.

3. If your network used asymmetric routing, select the check box for the **Asymmetric Network** to enable.
4. If you want to automatically release IP addresses from Quarantine after a specified amount of time, select the associated check box and then specify the **Timeout** value in minutes.



**Note** If you unmanage a device and then remanage the device, the Quarantine settings are reset to the default value.

5. 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.

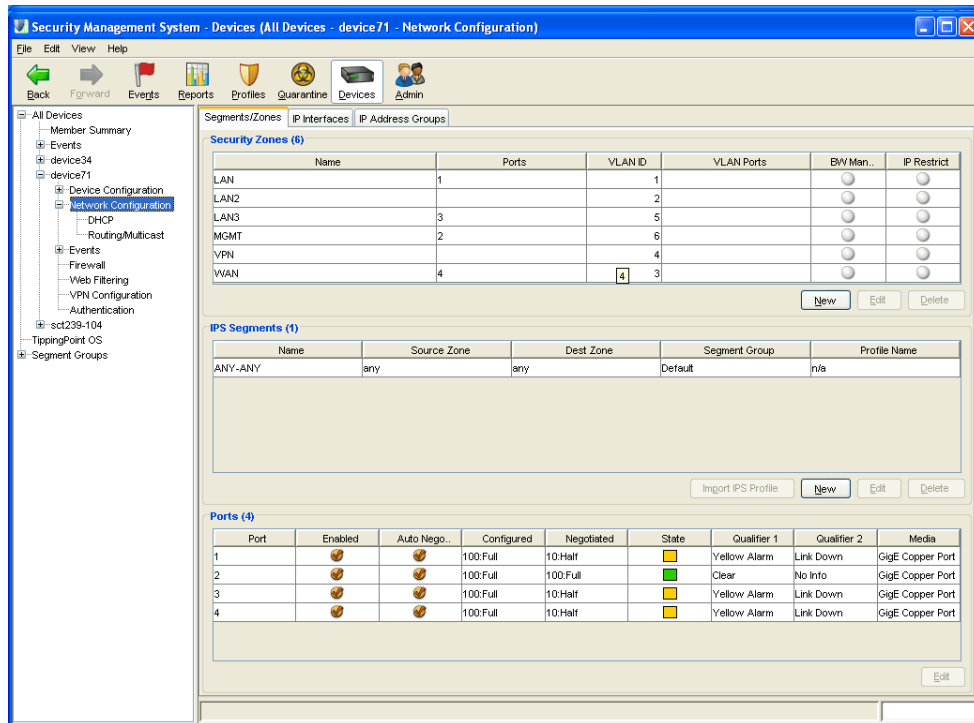
If an error occurs, the copper cable translator may not support auto-negotiation. See [“Edit IPS Segment Details” on page 398](#) or [“IPS Port Out-of-Service” on page 543](#).

## X-Family Devices: Network Configuration

Through the SMS, you can view information about all of the security zones and 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.

The following is the **Devices - Network Configuration** screen (**Segment Zones Tab**) for X-Family devices.

Table 8 - 29: Devices - Network Configuration for X-Family Devices



This section contains the following items

- [“Network Configuration: Segments/Zones Tab” on page 395](#)
- [“Network Configuration: IP Interfaces Tab” on page 400](#)
- [“Network Configuration: IP Address Groups Tab” on page 401](#)
- [“Network Configuration: DHCP” on page 402](#)
- [“Network Configuration: Routing Multicast” on page 403](#)

You can do the following tasks:

- [“Create/Edit Security Zone” on page 397](#)
- [“Edit IPS Segment Details” on page 398](#)
- [“Edit Port Details” on page 398](#)
- [“Import a Profile” on page 399](#)
- [“Create/Edit a Named IP Addresses” on page 401](#)
- [“Create/Edit a Named Group of IP Addresses” on page 401](#)
- [“Edit DHCP Server Settings” on page 402](#)
- [“Create New DHCP Static Mapping” on page 403](#)
- [“View/Refresh Routing Table” on page 405](#)
- [“Edit Unicast/Multicast Routing Settings” on page 405](#)
- [“Create a New Static Route” on page 405](#)

## Network Configuration: Segments/Zones Tab

Each Ethernet port and VPN tunnel is associated with one security zone, unless you use VLANs. If you configure VLANs, then a port can be in more than one security zone.

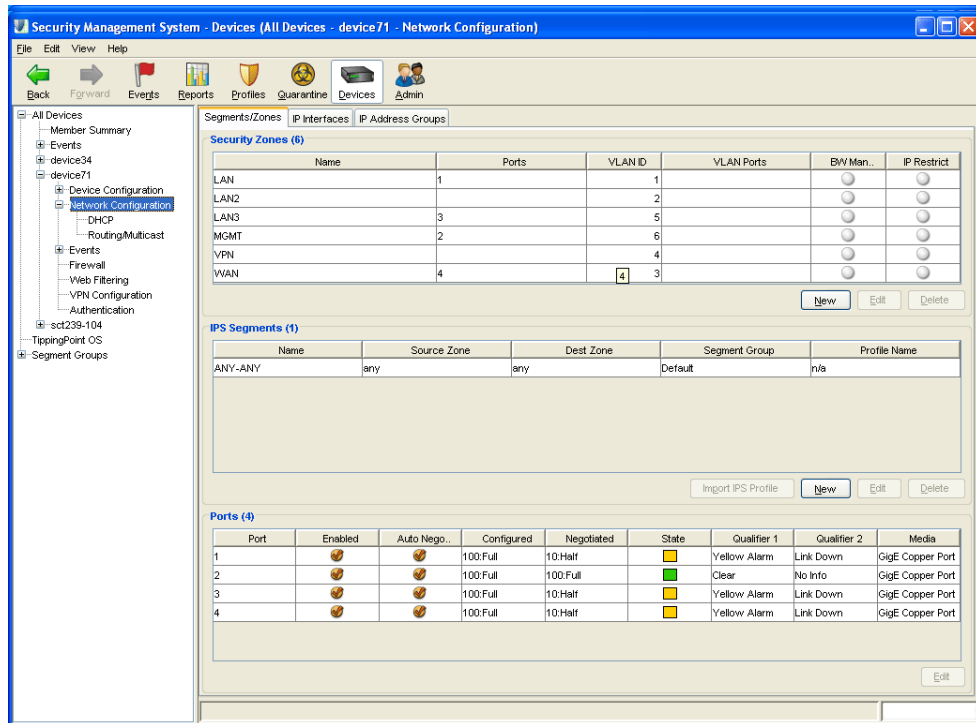
Any traffic originating from or destined to devices in a zone will be directed through the device and policed by firewall policies, if the traffic passes through to another zone. However, traffic moving between devices within any zone that you have defined (intra-zone traffic) will not be subject to firewall evaluation or IPS filtering (for example, a user on the LAN zone, accessing the local LAN printer) and will not pass through the device.

Devices in your network that communicate freely and do not require restricted access between them should be placed in the same zone.

This section contains the following items:

- [“Viewing Security Zone Information” on page 396](#)
- [“Adding, Editing, and Configuring Security Zones” on page 397](#)
- [“Adding, Editing, and Configuring Segments and Ports” on page 398](#)
- [“Importing a Profile” on page 399](#)

Table 8 - 30: Devices - Segment Zones Tab for X-Family Devices



### Viewing Security Zone Information

To view security zone information, log on to the SMS Client, select **Devices**, choose a managed device, select Network Configuration and then select **Segments/Zones** tab. The following information is available for each zone:

Table 8 - 31: Security Zones Summary Information

Column	Description
Name	The name of the Security Zone. Initially, the X-Family device is configured with LAN and WAN default zones
Port(s)	The ports on the X-Family device that have been assigned to each zone
VLAN ID	Identifies the VLAN associated with the security zone (if applicable)
VLAN Port(s)	The physical ports that have been allocated to the VLAN (if applicable)
Bandwidth Management	Whether bandwidth rate limiting has been applied, and the access speeds in Kbps for outbound (upload) traffic and inbound (download) traffic across the device. Applying bandwidth limitation physically limits the rate of traffic flow
IP Address Restrictions	The IP addresses for this security zone, either an <b>IP Address Group</b> , <b>IP subnet</b> or <b>IP range</b>

Each device is configured with predefined, default security zones. Consult the X-Family documentation for additional information.

## Adding, Editing, and Configuring Security Zones

Although the device is pre configured with default security zones, you can modify these or create your own security zones, with associated security policies and traffic shaping rules, according to the needs of your users and the topology of your network. After security zones are created, they can be associated in zone pairs.

### How To: Create/Edit Security Zone

1. On the **Devices** Navigation pane, expand the entry for a TippingPoint X-Family device.
2. Select **Network Configuration** and then select the **Segments/Zones** tab.
3. From the **Security Zones** area, and click the **New** button or select an entry from the list and click **Edit**. The setup wizard displays.
4. Specify a **Name** for the security zone.
5. Check the Ethernet port that you want to add to the zone.
6. **The VLAN ID** is required if VLAN Tagging is enabled and VLAN Tagged Ports are the physical ports that have been allocated to the VLAN. A security zone for use in a VPN does not need a physical port assigned to it.
7. Click **Next** or select **Bandwidth Management** from the wizard navigation pane.
8. Select **Enable Bandwidth Rate Limiting** if you want to prevent packet queuing on a WAN device.
9. If you select the **Enable Bandwidth Rate Limiting** option, specify the following items:
  - Limit outbound traffic to
  - Limit inbound traffic to

The access speeds in Kbps for outbound (upload) traffic and inbound (download) traffic physically limits the rate of traffic flow across the X-Family device. Values should be between 1 and 100,000 Kpbs.
10. Click **Next** or select **Network Protection** from the wizard navigation pane.
11. If you want to restrict the IP addresses of clients in the Security Zone for additional security purposes, configure the following options:
  - Restrict Security Zone to the following IP Addresses
  - Prevent this Security Zone from sending to VPN Tunnels
12. Click **OK** or **Finish**.



- Note:** Be sure all IP hosts that use the zone are within the IP addresses specified including:
- directly attached hosts connected to the zone via the Ethernet ports associated with the zone.
  - remote IP subnets connected via routers in the zone.
  - IP pools specified for any PPTP or L2TP server where the VPNs terminate in the security zone.

## Adding, Editing, and Configuring Segments and Ports

### How To: Edit IPS Segment 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**.
4. In the **IPS Segments** table, select an entry and 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 Fallback mode:
  - **Block All**
  - **Permit All**
8. 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 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.
9. Click **OK**.

### How To: 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**.
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 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.

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.

To resolve this issue, do the following:

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 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.

## Importing a Profile

After you have added and started managing a device, you may 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. You can also import a SMS profile for IPS and X-Family devices from the Segment Groups screen. See [“Importing Device Profiles” on page 341](#).

For more information on filters and profiles, see [Chapter 6, “Profiles”](#).

### How To: Import a Profile

1. From the Navigation menu, expand the **All Devices** listing and select an X-Family device by the device name. Open the tree of options for that device and select **Network Configuration**.
2. Select the Segments/Zones tab, select segment from the IPS Segments table, and then do one of the following tasks:
  - Click **Import IPS Profile**.
  - On the Menu Bar, select the **File** —> **Import Profile from Device** menu item.
3. The SMS imports the filters from the device into the SMS. The SMS names the profile using the segment's 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 [“IPS Profiles \(All Devices\)” on page 157](#) for more information on distributing profiles.

## Network Configuration: IP Interfaces Tab

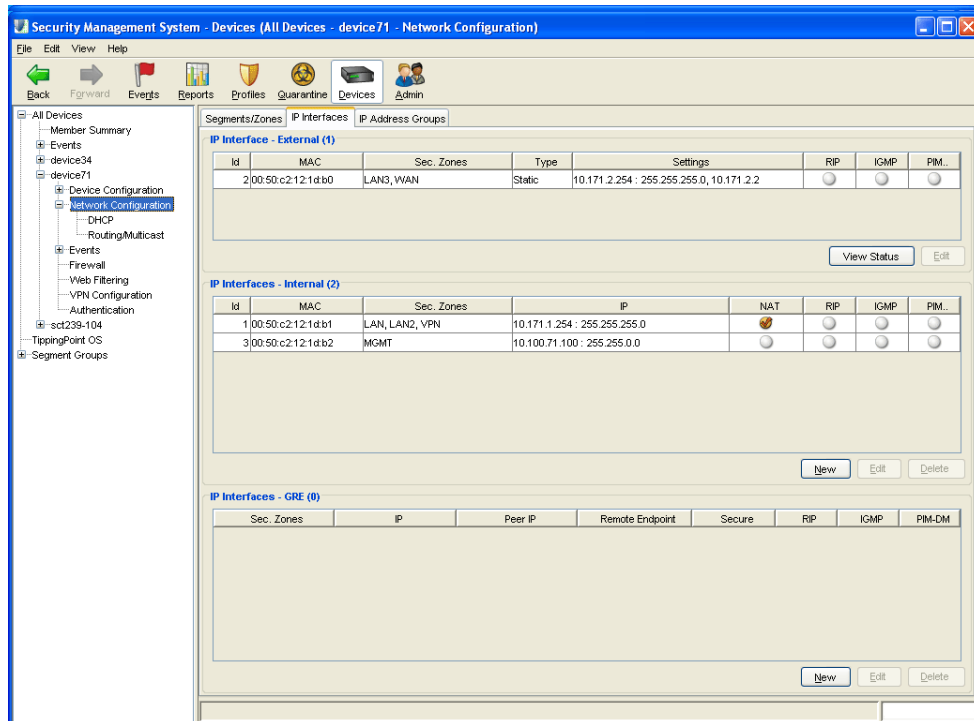
The Network Configuration Tab provides the following Interface options:

- External Interface
- Internal Interface
- GRE Interface

Each type of IP Interface has the following configuration options:

- General Setting
- Security Zones
- RIP Setting
- Multicast Settings

Table 8 - 32: Devices - IP Interfaces Tab for X-Family Devices



## Network Configuration: IP Address Groups Tab

### How To: Create/Edit a Named IP Addresses

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named IP Addresses** tab.
3. From the **Named IP Addresses** section, click **New** to create a new Named IP address or select an entry from the **Named IP Addresses** list and click **Edit**.
4. In the **Named IP Address** dialog, specify a name.
5. In the **IP Address** section, select IP Host, IP Subnet or IP Range and specify the entry.
6. Click **OK** to add the named Address to the list.

### How To: Create/Edit a Named Group of IP Addresses

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named IP Addresses** tab.
3. From the **Named IP Address Groups** section, click **New** to create a new group or select an entry from the group list and click **Edit**.

4. In the **Named IP Address Group** dialog, specify a name for the group.
5. Click **Add**. The **Add Named IP Address** dialog displays.
6. To add an existing named IP address or addresses to your new group, choose an entry from the list. If you want to edit an existing named address, select an entry and click **Edit**.
7. If you want to create a new named address, click **New**. In the **Named IP Address** dialog, enter a name, select IP Host, IP Subnet or IP Range, specify the entry, and click **OK**.
8. Repeat the steps for adding named IP addresses until you have all that you need.
9. In the **Add Named IP Address** dialog, click **OK**.

## Network Configuration: DHCP

Dynamic Host Configuration Protocol (DHCP) provides a method to dynamically allocate IP addresses to computers on your network.

You can perform the following tasks:

- [“Edit DHCP Server Settings” on page 402](#)
- [“Create New DHCP Static Mapping” on page 403](#)

### DHCP Leases Tab

The X-Family device can be configured to act as a DHCP Server for devices on its LAN-side interfaces requiring IP configuration. Use the DHCP Server dialog to:

Enable or disable DHCP Server on the X-Family device. If the DHCP Server is disabled, you can enable DHCP Relay to allow the X-Family device to relay client requests to a remote DHCP server.

Select the DHCP Address Pool for use by clients.

Configure DHCP options for DNS, WINS Server and NBX Network Call Processor.

### DHCP Settings Tab

The X-Family device can be configured to act as a DHCP Server for devices on its LAN-side interfaces requiring IP configuration. DHCP Static Mapping

Static Mapping allows you to assign a particular IP address to a device such as a printer or DNS server.

#### How To: Edit DHCP Server Settings

1. On the **Devices** Navigation pane, expand the entry for a TippingPoint X-Family device.
2. Select **Network Configuration**, select **DHCP**, and then select the **DHCP Settings** tab.
3. From the **DHCP Server** area, click **Edit**. The DHCP Server/Relay - Edit screen displays.

4. From the **DHCP Server** tab, you can perform the following tasks:
  - Enable or disable DHCP Server on the X-Family device.
  - If the DHCP Server is disabled, you can enable DHCP Relay to allow the X-Family device to relay client requests to a remote DHCP server.
  - Select the DHCP Address Pool for use by clients.
  - Configure DHCP options for DNS, WINS Server and NBX Network Call Processor. Create New DHCP Static Mapping
  
5. If you want to allow a DHCP server at one site to provide IP configuration to clients attached to a remote LAN via VPN, use DHCP VPN relay, use the **DHCP Relay** tab to perform the following tasks:
  - Relay DHCP requests to a DHCP Server.
  - Relay DHCP requests over a VPN tunnel.
 In order to use this option:
  - You must disable the DHCP Server in order to use DHCP Relay.
  - For DHCP Relay over VPN, you can only use DHCP Relay when the VPN between the two X-Family units is set up to use Internet Key Exchange (IKE).
  - For DHCP Relay over VPN, any LAN devices attached to the Remote VPN Relay agent that are not using DHCP must be configured as Static Mappings
  
6. After you complete your changes, click **OK**.

#### How To: Create New DHCP Static Mapping

1. On the **Devices Navigation** pane, expand the entry for a TippingPoint X-Family device.
2. Select **Network Configuration**, select **DHCP**, and then select the **DHCP Settings** tab.
3. From the **DHCP Static Mapping** area, click **New**. The **DHCP Static Mapping - Create** screen displays.
4. Enter the IP Address and MAC Address for the device, such as a printer or DNS server.
5. Click **OK**.

## Network Configuration: Routing Multicast

A static route defines the gateway to use for a particular network. From the **Routing/Multicast** screen you can view the current routing table, make changes to the settings and create or delete static routes.

The following is the **Devices - Network Configuration - Routing/Multicast** screen for X-Family devices.

Table 8 - 33: Devices - Routing/Multicast Screen for X-Family Devices

The screenshot shows the 'Current Routing Table (15)' with the following data:

Destination	Network Mask	Next Hop	Metric	Age	Status
0.0.0.0	0.0.0.0	10.171.2.2	8	0	Static
10.100.0.0	255.255.0.0	10.100.71.100	1	0	Direct
10.100.71.100	255.255.255.255	127.0.0.1	1	0	Local
10.171.1.0	255.255.255.0	10.171.1.254	1	0	Direct
10.171.1.254	255.255.255.255	127.0.0.1	1	0	Local
10.171.2.0	255.255.255.0	10.171.2.254	1	0	Direct
10.171.2.254	255.255.255.255	127.0.0.1	1	0	Local
127.0.0.0	255.0.0.0	127.0.0.1	1	0	Local
152.67.136.0	255.255.255.0	10.100.0.254	1	0	Static
152.67.137.0	255.255.255.0	10.100.0.254	1	0	Static
152.67.138.0	255.255.255.0	10.100.0.254	1	0	Static
152.67.139.0	255.255.255.0	10.100.0.254	1	0	Static
152.67.140.0	255.255.255.0	10.100.0.254	1	0	Static
216.136.107.0	255.255.255.0	10.100.0.254	1	0	Static
216.136.56.0	255.255.255.0	10.100.0.254	1	0	Static

The 'Unicast/Multicast Routing Settings' section shows:

- IGMP: Disabled
- PIM-DM: Disabled
  - Query Interval: 30 seconds (1-6000)
  - Prune Timeout: 180 seconds (1-9000)
- RIP: Disabled
  - Routing Update Timer: 30 seconds (1-6000)

The 'Static Routes (8)' section shows:

Destination	Network Mask	Gateway	Me..
0.0.0.0	0.0.0.0	10.171.2.2	8
216.136.56.0	255.255.255.0	10.100.0.254	1
216.136.107.0	255.255.255.0	10.100.0.254	1
152.67.136.0	255.255.255.0	10.100.0.254	1
152.67.137.0	255.255.255.0	10.100.0.254	1
152.67.138.0	255.255.255.0	10.100.0.254	1
152.67.139.0	255.255.255.0	10.100.0.254	1

RIP is used for exchanging unicast routing information between routers and hosts. RIP regularly broadcasts routing information to other devices on the network. RIP version 1 - static metrics are used to compare routes. RIP version 2 - adds support for subnets and authentication of routing updates. Split Horizon - reduces convergence time by not allowing routers to advertise networks in the direction from which those learned. This also reduces loops. Poison Reverse - routes learned from a neighbor are advertised back to it with metric 16 (unreachable). In a single-path network this has no advantage over split horizon. However, in multi-path networks this greatly reduces loops.



**Note** RIP must be enabled globally for the interface to use RIP. This setting is located in the Routing view.

You can perform the following tasks:

- [“View/Refresh Routing Table” on page 405](#)
- [“Edit Unicast/Multicast Routing Settings” on page 405](#)
- [“Create a New Static Route” on page 405](#)

### How To: View/Refresh Routing Table

1. From the **Devices** Navigation pane, select an X-Family device, and expand all the options including **Network Configuration**.
2. Select **Routing/Multicast** from the Navigation pane. The Network Configuration - **Routing/Multicast** screen displays.
3. To refresh the entries in the Current Routing Table, click **Refresh**.

### How To: Edit Unicast/Multicast Routing Settings

1. From the **Devices** Navigation pane, select an X-Family device, and expand all the options including **Network Configuration**.
2. Select **Routing/Multicast** from the Navigation pane. The Network Configuration - **Routing/Multicast** screen displays.
3. From the **Unicast/Multicast Routing Settings** area, click **Edit**.
4. In the **Unicast/Multicast Routing Settings**, select the appropriate option.
5. If you choose RIP, specify the amount of second for the **Routing Update Timer**.
6. If you Choose PIM-DM, specify the **Query Interval** and **Prune Timeout**.
7. Click **OK**.

### How To: Create a New Static Route

1. From the **Devices** Navigation pane, select an X-Family device, and expand all the options including **Network Configuration**.
2. Select **Routing/Multicast** from the Navigation pane. The Network Configuration - **Routing/Multicast** screen displays.
3. From the **Static Routes** area, click **New**. The Static Route - Create dialog displays.
4. Specify the following information about the route:
  - IP Address — IP address of the destination network for the static route
  - Subnet Mask — the subnet mask of the destination network
  - Gateway — the IP address of the device where the X-Family device forwards traffic destined to the destination network
  - Metric — a number (between 1 and 15) that is used to determine the order the static route is accessed
5. Click **OK**.

# X-Family Devices: Security Configurations

X-Family devices provide security features and functions that can be managed using the SMS. These features include the following items:

- [Firewall](#)
- [Web Filtering](#)
- [VPN Configuration](#)
- [Authentication](#)

## Firewall

The X-Family device polices traffic between the security zones according to a set of firewall rules. Using these rules, you can prioritize, permit, block, filter, authenticate, schedule and monitor traffic between security zones. You can define the order in which the firewall rules are applied, so that traffic is checked first against the higher priority rules.

You can configure the firewall settings for a single device. You can also configure the firewall rules for multiple devices using a single Firewall Profile. For more information, see [“Firewall Profiles \(X-Family Devices\)” on page 237](#).

From the Firewall screen you can manage the following items:

- Firewall Rules
- Services
- Service Groups
- Schedules
- Virtual Servers (IP Forwarding)

## Firewall Rules Tab

The **Firewall Rules** Table provides a convenient location to create, copy and edit firewall rules. For additional information, see [“Firewall Profiles \(X-Family Devices\)” on page 237](#).

You can perform the following tasks:

- [“Add a Firewall Rule” on page 407](#)
- [“Manage Firewall Rules” on page 407](#)
- [“Edit a Firewall Rule” on page 408](#)



### How To: Add a Firewall Rule

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Firewall Rules** tab.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
2. Click the **New** button.  
The setup wizard displays. 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.
3. On the **Action Definition** screen, complete the following information:
  - Action to take on a packet
  - Service that the rule applies to
  - Enable/Disable status If desired, you can enable on a schedule, such as typical working days and hours.
4. On the **Target Traffic** screen, choose which traffic path (Source and Destination Zones) to apply this firewall rule.
5. On the **Bandwidth Management** as an optional step, you can enable and configure bandwidth management to provide better control over network resources
6. On the **User Authentication** screen as an optional step, you can allow to be applied only to authenticated users.
7. On the Other Settings screen, you can enable logging, set time for inactivity, and add any comments.
8. Click **Finish** to save your Firewall rule.

### How To: Manage Firewall Rules

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Firewall Rules** tab.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
2. The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
3. Select a rule or rules and perform any of the following tasks:
  - Use the up- and down-arrows to change the order in which rules will be applied.
  - Click **Copy Rule(s)** to make a copy of a rule.
  - Click **Delete** to remove the rule for the firewall profile.

### How To: Edit a Firewall Rule

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Firewall Rules** tab.  
The **Firewall Rules** table displays and lists the rules in the order they will be applied to the X-Family device.
2. Select a rule from the list and click the **Edit** button.  
The setup wizard displays. 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.
3. On the **Action Definition** screen, complete the following information:
  - Action to take on a packet
  - Service that the rule applies to
  - Enable/Disable status If desired, you can enable on a schedule, such as typical working days and hours.
4. On the **Target Traffic** screen, choose which traffic path (Source and Destination Zones) to apply this firewall rule.
5. On the **Bandwidth Management** as an optional step, you can enable and configure bandwidth management to provide better control over network resources
6. On the **User Authentication** screen as an optional step, you can allow to be applied only to authenticated users.
7. On the Other Settings screen, you can enable logging, set time for inactivity, and add any comments.
8. Click **Finish** to save your Firewall rule.

### Services Tab

From the Custom Firewall Services area, you can create and manage custom service. from the Default Firewall Services area, you can edit any default services.

You can perform the following tasks:

- [“Add a Custom Service” on page 409](#)
- [“Edit a Custom Service” on page 409](#)

### How To: Add a Custom Service

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Services** tab.
2. Click **New**.
3. On the **Add Service** screen, complete the following information:
  - Service Name
  - Protocol for the service
  - Destination Port Range
4. Click **OK**.

### How To: Edit a Custom Service

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Services** tab.
2. Select a custom or default service and click **Edit**.
3. On the **Edit Service** screen, make the desired edits of the following information:
  - Service Name
  - Protocol for the service
  - Destination Port Range
4. Click **OK**.

## Service Groups

From the Service Groups area, you can create new service groups and edit existing groups.

You can perform the following tasks:

- [“Add a Service Group” on page 409](#)
- [“Edit a Custom Service” on page 410](#)

### How To: Add a Service Group

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Service Groups** tab.
2. Click **New**.
3. On the **Add Service group** screen, use the arrow buttons to move the desired available services to the **Selected Services** area.
4. Click **OK**.

### How To: Edit a Custom Service

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Service Groups** tab.
2. Select a service group and click **Edit**.
3. On the **Edit Service Group** screen, use the arrow button to move services to the **Selected Services** area
4. Click **OK**.

### Schedules

You can perform the following tasks:

- [“Add a Schedule” on page 410](#)
- [“Edit a Schedule” on page 410](#)

### How To: Add a Schedule

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Schedules** tab.
2. Click **New**.
3. On the **Firewall Rule Schedule** screen, specify a name for the schedule and click **Add**.
4. On the **Schedule - Time Interval** screen, define the time ranges to include and click **OK**.
5. On the **Firewall Rule Schedule** screen, click **OK** to save your schedule.

### How To: Edit a Schedule

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Schedules** tab.
2. Click **Edit**.
3. On the **Firewall Rule Schedule** screen, make any desired changes to the name of the schedule.
4. To make changes to the schedule, select the listed schedule and click **Edit**.
5. On the **Schedule - Time Interval** screen, make any desired changes to the time ranges and click **OK**.
6. On the **Firewall Rule Schedule** screen, click **OK** to save your schedule.

## Virtual Servers (IP Forwarding)

IP Forwarding allows external devices access to internal servers.

You can perform the following tasks:

- [“Add a Virtual Server” on page 411](#)
- [“Edit Web Filtering Global Settings” on page 412](#)

### How To: Add a Virtual Server

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Virtual Servers (IP Forwarding)** tab.
2. Click **New**.
3. On the **Virtual Server** screen, complete the following information:
  - Public IP
  - Service
  - Local IP Address
4. Click **OK**.

### How To: Edit a Virtual Server

1. From the **Devices** Navigation pane, select an X-Family device, select **Firewall**, and the **Virtual Servers (IP Forwarding)** tab.
2. Select a listing from the Virtual Server list and click **Edit**.
3. On the **Virtual Server** screen, make any desired changes to the Local IP Address.
4. Click **OK**.

## Web Filtering

The SMS allows you to apply web content filtering and manage this function across multiple X-Family devices. You must define this service on the device. For more information, consult your X-Family device documentation.

This section contains the following items:

- [“Web Filtering Tab” on page 412](#)
- [“Manual Web Filtering Tab” on page 413](#)

You can perform the following task:

- [“Edit Web Filtering Global Settings” on page 412](#)
- [“Edit 3Com Content Filter Settings” on page 412](#)
- [“Enable/Disable Manual Web Filtering” on page 413](#)

## Web Filtering Tab

### How To: Edit Web Filtering Global Settings

1. From the **Devices** Navigation pane, select an X-Family device, select **Web Filtering**, and the **Web Filtering** tab.
2. From the **Web Filtering Global Settings** area, select the **Edit** button. the **Web Filtering Settings - Edit** screen displays.
3. On the **General Setting** tab, make any desired changes to the Default Rule and Filtering Action.
4. If you want the X-Family device to display a custom page to clients that encounter a blocked web request:
  - Select the **Custom Response Page** tab.
  - In the text area, enter the custom HTML to display.
5. Click **OK**.

### How To: Edit 3Com Content Filter Settings



**Note** You can specify which Web requests are allowed or blocked by allowing or denying access to certain well-known categories of Web sites e.g. news, sports. This is a subscription-based service which requires the purchase of a license from your reseller.

1. From the **Devices** Navigation pane, select an X-Family device, select **Web Filtering**, and the **Web Filtering** tab.
2. From the **3Com Content Filter Settings** area, select the **Edit** button. the **3COM Content Filter Service - Edit** screen displays.
3. Enable the service and select the appropriate server and click **OK**.

### Enable/Disable 3Com Content Categories

1. From the **Devices** Navigation pane, select an X-Family device, select **Web Filtering**, and the **Web Filtering** tab.
2. From the **Manual Web Filtering** area, click the **Edit** button. The **Manual Web Filtering - Edit** screen displays.
3. To enable this feature, select the **Enable** checkbox To disable this feature, deselect the **Enable** checkbox.
4. Click **OK**.

## Manual Web Filtering Tab

Web Filtering allows or denies access to different Web sites based on their URLs, domain names, IP addresses, regular expression pattern matching and keyword matching.



**Note** For the X-Family device to use content filtering, you must set up a firewall rule that applies it.

### How To: Enable/Disable Manual Web Filtering

1. From the **Devices** Navigation pane, select an X-Family device, select **Web Filtering**, and the Manual **Web Filtering** tab.
2. From the **Manual Web Filtering** area, select a content category from the list.
1. Click the **Enable** or **Disable** button.

## VPN Configuration

A Virtual Private Network (VPN) is a means of establishing a secure connection between two points across a public network, for example, the Internet. A VPN is a private connection between two points, which in reality uses tunneling across a public connection from the Initiation Point to the Termination Point. For more information, see your TippingPoint X-Family documentation.

The two methods of setting up a site-to-site VPN connection include the following types:

- **IPSec** — The standard X-Family method of setting up a network-to-network VPN connection.
- **GRE over IPSec** — Used to support applications such as dynamic routing and multicast, in which the data is encapsulated within a GRE packet. IPSec then treats the packets as unicast traffic.

This section contains the following items:

- [“IPSec Associations Tab” on page 414](#)
- [“IKE Proposals Tab” on page 415](#)
- [“L2TP/PPTP Settings Tab” on page 416](#)
- [“VPN Configuration Troubleshooting” on page 418](#)

You can perform the following task:

- [“Enable/Disable IPSec Global Setting” on page 414](#)
- [“Add/Edit IPSec Global Association” on page 414](#)
- [“Set Up IPSec Security Association \(IKE\)” on page 415](#)
- [“Enable/Edit L2TP Configuration Settings” on page 416](#)
- [“Enable/Edit PPTP Configuration Settings” on page 417](#)

## IPSec Associations Tab

IPSec is a protocol that can be used to secure IP traffic. It is a flexible protocol with a wide range of encryption options. IPSec is commonly used both for connections between separate private networks (tunnels) and for connections between remote PCs and private networks.



**Note:** You must enable IPSec globally to use IPSec VPNs.

### How To: Enable/Disable IPSec Global Setting

1. From the **Devices** Navigation pane, select an X-Family device, select **VPN Configuration**, and the **IPSec Associations** tab.
2. From the **IPSec Global Settings** area, click the **Edit** button. The **Edit VPN IPsec Global Settings** screen displays.
3. On the **VPN IP Sec Global Settings** screen:
  - Select the **Allow IP Global VPN** checkbox to enable this option. If this option is not selected, the VPN connections configured for the X-Family device will not be activated.
  - Enter the Local **Domain Name** and **Local Email Address**.
4. To disable this feature, deselect the checkbox.
5. Click **OK**.

### How To: Add/Edit IPSec Global Association

1. From the **Devices** Navigation pane, select an X-Family device, select **VPN Configuration**, and the **IPSec Associations** tab.
2. From the **IPSec Security Associations** area, and click the **New** button or select an entry from the list and click **Edit**. The setup wizard displays.
3. For the **Basic Setup** screen:
  - Give the security association a name, and check the **Enable Security Association** option. The SA name must match the SA name on the remote X-Family device. For a site-to-site VPN the SA



name must be unique to the VPN connection. If you want to use GRE and L2TP, you must check that option.

- Enter the address of the terminating VPN X-Family device (the remote target of the VPN link) in the **Peer IP Address** field. If the remote device does not have a fixed IP address, then leave this field blank or set to 0.0.0.0.



**Note:** If the Peer IP Address is set to 0.0.0.0, then this SA will only accept tunnels, and not initiate them.

4. After all items are complete, click **Next**.
5. For the **Tunnel Setup** screen:
  - If you want the VPN to use Tunnel mode, check **Enable IPSec Tunnel connections** and configure the Tunnel connection options.
  - If **Enable IPSec Tunnel connections** is not selected, you do not need to configure the tunnel security zone, forwarding between IPSec tunnels, or destination networks.
6. After all items are complete, click **Finish**.

## IKE Proposals Tab

If you are using IKE as your keying mode, you need to configure an IKE Proposal to select the security attributes that are used to protect the VPN connection. IPSec Security Association setup wizard has two screens to complete, IKE Phase 1 Setup and IKE Phase 2 Setup.

### How To: Set Up IPSec Security Association (IKE)

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **VPN Configuration**.
2. From **VPN Configuration** screen, select the **IKE Proposals** tab.
3. In the List pane, do one of the following tasks:
  - Select an existing Security Association and click **Edit**.
  - Click **New** to create a new Security Association.
4. Complete each of the two setup screens. For additional information about the needed information, click the **more** link located in the top right-hand corner the wizard setup screen.
5. When all information is complete, click **Finish**.

## L2TP/PPTP Settings Tab

L2TP over IPSec is the recommended method for setting up client-to-site VPNs.

Layer 2 Tunneling Protocol (L2TP) is a mechanism that provides a PPP (Point-to-Point Protocol) connection between a user and a terminating device over an IP network. PPP is the protocol that is typically used to allow a dial-up user to connect to the Internet, authenticate and obtain their IP configuration in order to access the private LAN behind the L2TP terminator.

Although PPP provides a level of security and authentication, when L2TP is run over IPSec (L2TP/IPSec) much better security and authentication is provided.



**Note:** When secured with IPSec, L2TP uses IPSec transport mode, as both the VPN client and L2TP terminator have a public IP address.

After completing the IPSec connection between the client and the X-Family device, an L2TP tunnel is established and the PPP connection within L2TP authenticates the VPN client user and provides the VPN client with an appropriate *local* IP address.

Layer 2 Tunneling Protocol (L2TP) allows a dial-up user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP Server on the VPN. L2TP sends PPP frames through a tunnel between a user and the L2TP Server.



**Note:** To use X-Family device as an PPTP VPN terminator, you must check Support L2TP when you are configuring IPSec. See [“IPSec Associations Tab” on page 414](#).

Point-to-Point Tunneling Protocol (PPTP) is an encrypted VPN protocol like IPSec, although not as secure as IPSec. PPTP does not support gateway to gateway connections and is only suitable for connecting remote users. The X-Family device acts a PPTP Server for VPN termination, and is compatible with Windows PPTP VPN clients such as Windows XP. It also supports MPPE 128-bit encryption.

### How To: Enable/Edit L2TP Configuration Settings

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **VPN Configuration**.
2. From **VPN Configuration** screen, select the **L2TP/PPTP Setting** tab.
3. In the **L2TP Configuration Settings** area, click the **Edit** button. The **L2PTP Server Configuration** dialog displays.
4. To enable the server, select the **Enable Server** checkbox, select the appropriate **Security Zone** from the drop down menu, and select the **Requires Encryption** check box, if necessary.

To make changes to an existing Security Zone, click **Edit**. To define a new Security Zone, click **New**. For information on using the Security Zone setup wizard, see [“Network Configuration: Segments/Zones Tab” on page 395](#).

5. In the **DNS Server** area, select the appropriate option. If you choose **Specify DNS Server** option, enter the address for the **DNS Server 1** and **DNS Server2**.
6. In the **WINS Servers** area, enter the address for the **WINS Server 1** and **WINS Server2**.
7. In the **L2TP Addresses** area, select the appropriate option. If you choose **Specify IP Address Group** option, select a group from the drop down box.  
  
To make changes to an existing IP Address Group, select a group from the drop down menu, and click **Edit**. To define a new IP Address Group, click **New**. For information on using the **Named Address** setup, see Admin chapter > Named Resources.
8. When all information is complete, click **OK**

### How To: Enable/Edit PPTP Configuration Settings

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **VPN Configuration**.
2. From **VPN Configuration** screen, select the **L2TP/PPTP Setting** tab.
3. In the **PPTP Configuration Settings** area, click the **Edit** button. The **PPTP Server Configuration** dialog displays.
4. To enable the server, select the **Enable Server** checkbox, select the appropriate **Security Zone** from the drop down menu, and select the **Requires Encryption** check box, if necessary.  
  
To make changes to an existing Security Zone, click **Edit**. To define a new Security Zone, click **New**. For information on using the Security Zone setup wizard, see [“Network Configuration: Segments/Zones Tab” on page 395](#).  
  
In the **DNS Server** area, select the appropriate option. If you choose **Specify DNS Server** option, enter the address for the **DNS Server 1** and **DNS Server2**.
5. In the **WINS Servers** area, enter the address for the **WINS Server 1** and **WINS Server2**.
6. In the **IP Addresses** area, select the appropriate option. If you choose **Specify IP Address Group** option, select a group from the drop down box.  
  
To make changes to an existing IP Address Group, select a group from the drop down box, and click **Edit**. To define a new IP Address Group, click **New**. For information on using the **Named Address** setup, see Admin chapter > Named Resources.
7. When all information is complete, click **OK**

## VPN Configuration Troubleshooting

The following may help you if you are having problems with a site-to-site VPN connection:

- The X-Family device is unable to establish a connection with the remote X-Family unit, due to incorrectly configured IP addressing information.
- IPSec keying proposal — Phase 1 and 2 must be configured with the same parameters on both of the X-Family units connected in the VPN tunnel. TippingPoint recommends that you use a default IKE proposal.
- Check that the authentication mechanism, keys, shared secrets or certificates, are correctly configured on both devices.
- Check firewall rule configuration, to ensure that VPN traffic, from the source and destination devices, is allowed.
- Check the **VPN** —> **IPSec/IKE Status** page on the Web Interface to determine if there is a problem and to see the status of the VPNs.
- Check the X-Family Logs to see if a problem is indicated in any of the entries.
- For IPSec tunnel mode, ensure that the tunnel security zone is correct and that the configured destination networks match the remote IP subnets
- For IPSec transport mode, ensure that the GRE interface is configured and routing is enabled.

The following may help you if you are having problems with a client-to-site VPN connection:

- The X-Family device is unable to establish a connection with the remote VPN clients, due to incorrectly configured IP addressing information.
- Connection method — the VPN client is not compatible with the method selected (for example, older Windows VPN clients, which do not support L2TP).
- Check the **VPN** —> **IPSec/IKE Status** page on the LSM to determine if there is a problem and to see the status of the VPNs.
- Check the X-Family Logs to see if a problem is indicated in any of the entries.
- Incorrect authentication setup, preventing the client from authenticating with the X-Family unit.
- Firewall rule is configured incorrectly, to block VPN traffic.

## Authentication

This section contains the following items:

- [“Authentication Tab” on page 419](#)
- [“X509 Certificates Tab” on page 421](#)

You can perform the following tasks:

- [“Edit Radius Configuration” on page 419](#)
- [“Add/Edit Local Users” on page 420](#)
- [“Edit Local User Preferences” on page 420](#)
- [“Create/Edit Privilege Groups” on page 421](#)
- [“Import a Local Certificate” on page 421](#)
- [“Import CA Certificate” on page 422](#)
- [“Export CA Certificate” on page 422](#)
- [“Import Local Signed Certificate” on page 422](#)

### Authentication Tab

- **Radius Configuration** — provides support for authentication for Local User access to the network through the device, and covers VPN client dialup, Inter-site VPN access, Internet access, and Content filtering bypass.
- **Local User Preference** — sets inactivity timeout in minutes for logged in local users.
- **Local Users** — when adding users, you can also limit the access available to the users by assigning them to a Privilege Group.
- **Privilege Groups** — control access to X-Family operations.

#### How To: Edit Radius Configuration

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **Authentication** tab.
3. To enable Radius Authentication, select the Enable RADIUS Authentication check box and then select or deselect the following RADIUS configuration options:
  - User Authentication
  - VPN Client Access
4. To set the default privilege group that will control access to X-Family devices, select an entry from the **Default Privilege Group** drop-down list.
  - To edit an existing Privilege Group, select the entry, click **Edit**. See [“Create/Edit Privilege Groups” on page 421](#)
  - To create a new Privilege Group, click **New**. See [“Create/Edit Privilege Groups” on page 421](#).

5. Specify the following parameters:
  - **Server Timeout** in seconds (from 1 to 30)
  - **Server Retries** (from 1 to 10)
6. Specify the following information for the Primary and Secondary Radius Server:
  - IP Address
  - Port
  - Shared Secret
  - Authentication Method
  - Click **OK** to save your settings.

### How To: Add/Edit Local Users

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
1. From Device **Authentication** screen, select the **Authentication** tab.
2. In the **Local Users** area, click **New** to add a new user or select an entry from the list and click **Edit**. The **Local User** dialog displays.
3. Complete the following entries
  - Name
  - Password
  - Firm Password
4. To control access to X-Family devices, select an entry from the **Privilege Group** drop-down list.
  - To edit an existing Privilege Group, select the entry, click **Edit**. See [“Create/Edit Privilege Groups” on page 421](#)
  - To create a new Privilege Group, click **New**. See [“Create/Edit Privilege Groups” on page 421](#).
5. Click **OK** to save your settings.

### How To: Edit Local User Preferences

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **Authentication** tab.
3. From the Local User Preferences area, click **Edit**.
4. Specify the following settings for logged in local users.
  - **Inactivity Timeout** in minutes (between 0 and 999)
  - **Maximum Session Time** in minutes (between 0 and 999)
5. Click **OK** to save your settings.

### How To: Create/Edit Privilege Groups

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
1. From Device **Authentication** screen, select the **Authentication** tab.
2. In the **Privilege Group** area, click **New** to create a new privilege group or select an entry from the group list and click **Edit**. The **Privilege Group** dialog displays.
3. Specify a **Name**, and select the following access option or options:
  - **VPN Client Access**
  - Firewall Rule Authentication
  - Bypass Web Filtering
4. Click **OK** to save your settings.

### X509 Certificates Tab

- **Local Certificates** — are digitally signed certificates that are used to authenticate HTTPS and IPSec on the X-Family device.

Local Certificates are authenticated by CA Certificates, which issued by a Certificate Authority (CA). The X-Family device uses PKCS#12 format for importing Local Certificates with their private key. PKCS#12 format is a commonly used portable format for importing certificates into browsers. The imported file may also include the CA Certificate, in which case the X-Family device adds the CA Certificate to the CA list.

- **CA Certificates** — are encrypted digital certificates issued and signed by a Certificate Authority, which is commonly referred to as a trust third party.
- **Certificate Requests** — Certificate Requests contain the information that must be submitted to the Certificate Authority so that a signed CA Certificate can be issued.

### How To: Import a Local Certificate

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **X-509 Certificates** tab.
3. To import a Local Certificate, click the **Import** button in the **Local Certs** area. The **Local Certificate - Import** dialog displays.
4. Perform the following tasks:
  - Enter the name of the file containing the Local Certificate in the **Certificate File** field, or click **Browse** and navigate to the file.
  - Enter the certificate name in the **Certificate Name** field.
  - Enter the password for the certificate in the Certificate Password field.

This password is issued by the Local Certificate provider and must match the password that was used to export the certificate.

5. Click **OK** to return to the **X509 Certificates** tab.

### How To: Import CA Certificate

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **X-509 Certificates** tab.
3. To import a Local Certificate, click the **Import** button in the **CA Certs** area. The **CA Certificate - Import** dialog displays.
4. Perform the following tasks:
  - Enter the name of the file containing the CA Certificate in the **Certificate File** field, or click **Browse** and navigate to the file.
  - Enter a unique name to use locally for the CA Certificate in the **Certificate Name** field. The name should be between 1 and 20 alphanumeric characters and can contain the \_ (underscore) character.
5. Click **OK** to return to the **X509 Certificates** tab.

### How To: Export CA Certificate

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **X-509 Certificates** tab.
3. To export a Local Certificate, select a certificate from the **CA Certs** list, click the **Import** button, and follow the export instructions.
4. Click **OK** to return to the X509 Certificates tab.

### How To: Import Local Signed Certificate

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **X-509 Certificates** tab.
3. To import a Local Signed Certificate, click the **Import Local Cert** button in the **Certificate Requests** area. The **Signed Local Certificate - Import** dialog displays.
4. Enter the name of the file containing the signed Local Certificate in the **Certificate File** field, or click **browse** and navigate to the file.

After import if the X-Family device verifies that the certificate can be trusted and that it matches the Certificate Request, the certificate is then imported and included in the Local Certificates table and the Certificate Request is deleted. If the import fails, an error message explaining the failure is displayed.

5. Click **OK** to return to the **X509 Certificates** tab.



### How To: Create Certificate Request

1. From the **Devices** Navigation menu, expand an X-Family device listing and select **Authentication**.
2. From Device **Authentication** screen, select the **X-509 Certificates** tab.
3. In the **Certificate Requests** area, click **Create**. The **Certificate Request - Create** dialog displays.
4. In the **Name** field, specify a file name for the certificate.
5. Select the appropriate length for the certificate from the drop down box.
6. Enter a **Distinguished Name** that uniquely identifies a certificate.  
This name, defined when creating the Certificate Request, is used by the Local Certificate and can be between 1 and 64 characters. Click **OK** to return to the **X509 Certificates** tab.
7. Select other checkboxes as needed and complete those fields.
8. Click **OK** to return to the **X509 Certificates** tab.



**Note:** The X-Family uses PKCS#10 format for Certificate Requests. When a request is created, a public/private key pair is generated, and the public key is included in the PKCS#10 format which is based on Public Key Cryptography Standards.

## X-Family Devices: Event Monitoring

Through the **Events** screen for an individual device, you can monitor the following system-specific information for an X-Family device:

- [X-Family Device Events: System Log](#)
- [X-Family Device Events: Audit Log](#)
- [X-Family Device Events: VPN Log](#)

For additional information on monitoring your X-Family device, see [“Device Monitoring” on page 309](#).

You can do the following:

- [View Log](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

### How To: View Log

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.
2. Select a device and expand the options.



3. Select a log option:

- **System Log**
- **Audit Log**
- VPN Log

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:

- Select a **Star Time**. Click the calendar icon  and select the start and end times for the range. See [“Date and Time Controls” on page 37](#).
- Select an **End Time**. Click the calendar icon  and select the start and end times for the range. See [“Date and Time Controls” on page 37](#).
- Click **Refresh**.

### How To: Reset Logs

1. On the **Devices** screen, expand the **All Devices** in the Navigation pane.

2. Select a device.

3. Click **Events** and one of the following log options:

- **System Log**
- **Audit Log**
- **VPN Log**

4. Do one of the following:

- Display a log screen and click **Reset**.
- On the Menu Bar, select the **File** —> **Reset Device Logs** menu item and select the log you want to reset: system, audit, alert, block, or all.
- To reset all logs, you can select the **All Logs** option. On the Menu Bar, select the **File** —> **Reset Device Logs** —> **All Logs** menu item.



**Note** Resetting all logs does not reset the audit log.

## X-Family Device Events: 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.



**Note** Any access level user can view the system log, but only Administrator and Super User level users can print the system log.

The following table details the system log details:

**Table 8 - 34: 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](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

## X-Family Device Events: Audit Log

The audit log keeps track of device user activity that may 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 Super User level users can view, print, reset, and download the audit log.

The following table details the audit log details:

**Table 8 - 35: 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, Super User, 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](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

When you view the log, the user listed for the logged events may include SMS, LSM, and CLI. These entries are entered by those applications into the audit log, as a Super User level of access.

## X-Family Device Events: VPN Log

The VPN log keeps track of VPN activity that may have security implications. The following table details the audit log details:

**Table 8 - 36: Audit Log Details**

Heading	Description
Time	The time of the alert added to the log
Message	Log entry
Src Addr	Source address of triggered traffic
Dst Addr	Destination address of triggered traffic
Src Port	Source port of triggered traffic
Dst Port	Destination port of triggered traffic

 **Note** Only Super User level users can view, print, reset, and download the audit log.

You can do the following:

- [View Log](#) — Details how to view a log
- [Reset Logs](#) — Details how to reset logs

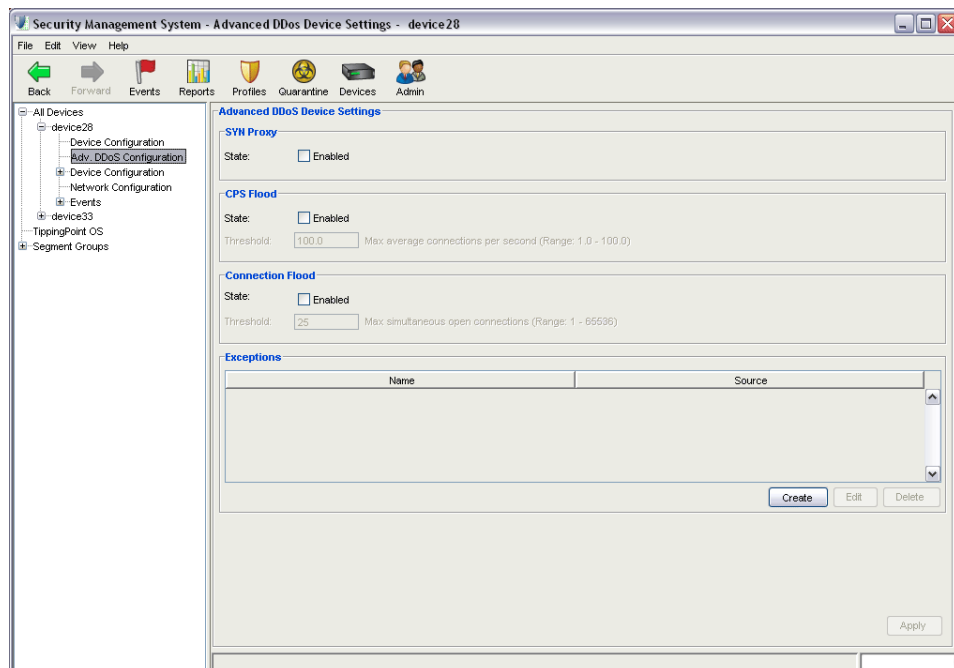
## E-Series: Advanced DDoS

For TippingPoint E Series 1200E/2400E/5000E devices, the **Adv. DDoS Configuration** screen provides option to enable options, configure threshold settings, and manage exceptions for Advanced DDoS filters. This configuration screen displays only for TippingPoint E Series devices not including the TippingPoint 100E/200E. Configuration options for other devices display only on the **Profiles** screen. You can access this screen directly through the **Devices** screen, or when creating and editing TippingPoint E-Series filters through the **Profiles** screen.

For more information on Advanced DDoS filters, see [“Advanced DDoS Filters” on page 212](#)

The following is the **Devices - Adv. DDoS Configuration** screen for E-series devices.

**Figure 8 - 34: Devices - Adv. DDoS Configuration Screen for E-Series Devices**



### How To: Configure Advanced DDoS Filter Options

1. On the **Devices Navigation** pane, select the **Adv. DDoS Configuration** option for a TippingPoint E-Series device (not including the TippingPoint 100E/200E). The **Advanced DDoS Device Settings** screen displays.
2. For SYN Proxy, click the **Enabled** check box.
3. For CPS Flood, click the **Enabled** check box and enter a **Threshold** setting (1.0 to 199.0 range).
4. For Connection Flood, click the **Enabled** check box and enter a **Threshold** setting (1 to 65536).
5. To create an exception, click **Create**. The **Filter - DDoS Create/Edit Exception** dialog box displays.
  - Enter a **Name**.
  - Enter a **Source Address** and select a format.
6. Click **OK**.

## DDoS Preferences

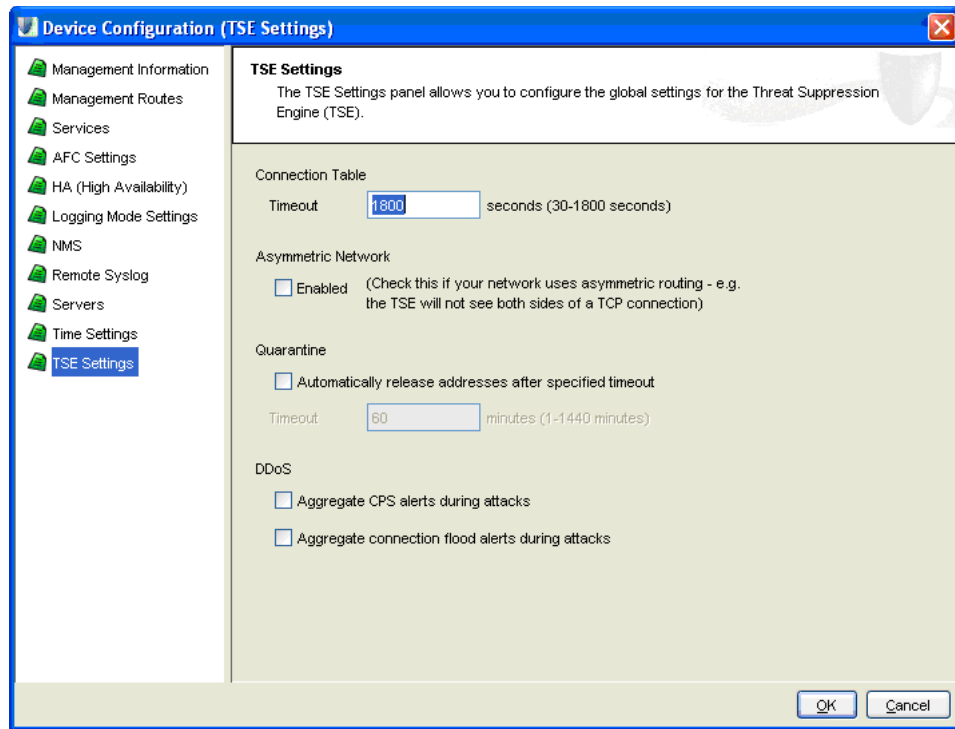
In the **Device Configuration (TSE Settings)** screen, the following DDoS settings are supported:

- 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.

The following is the **Devices - Configuration (TSE Settings)** screen for E-series devices.

**Figure 8 - 35: Devices - Configuration (TSE Settings) Screen for E-Series Devices**



### How To: Set DDoS Preferences

1. To access the Device Configuration Wizard do one of the following:
  - On the **All Devices** screen, select a TippingPoint E-Series device (not including the TippingPoint 100E/200E) and click **Edit**.
  - Select a TippingPoint E-Series device (not including the TippingPoint 100E/200E), select the management port listing from the component list, and then click **Edit**.
2. From the Device Configuration Wizard panel menu, select **TSE Settings**.
3. In the **Device configuration (TSE Settings)** screen, make the desired changes. Available options include:
  - **Connection Table:** Timeout in seconds
  - **Asymmetric Network:** Enabled/Disabled
  - **Quarantine:** Release Quarantined addresses automatically, Timeout in minutes
  - **DDoS:** Aggregate CPS and/or connection flood alerts during attacks
4. Click **OK**.





# 9

# Administration

*The Admin screen provides functionality to manage the SMS. These tasks include managing users and user roles, setting and viewing log contents, backing up the system database, specifying SMS configuration information, and upgrading SMS software and licenses.*

## Overview

SMS administration can be divided into system administration, user administration, and SMS server configuration.

This section includes the following topics:

- [“Administration: What’s New” on page 432](#)
- [“General Administration” on page 437](#)
- [“How To Tasks” on page 433](#)
- [“General Administration” on page 437](#)
- [“Database Administration” on page 454](#)
- [“SMS Server Properties” on page 460](#)
- [“High Availability” on page 475](#)
- [“Named Resources” on page 487](#)

The primary purpose of system administration is to allow users with Super User authority, or role access, to configure the settings that effect the entire SMS application. You can back up and restore the system database, define server properties, manage user accounts, and view the system and audit logs. User administration helps you maintain the security of TippingPoint by tightly controlling and tracking user access, sessions, and behavior in the SMS.

Through the **Admin** screen, you can also upgrade SMS software and add additional SMS licenses for increased session access and management spaces for additional devices. By default, your SMS can

manage twenty-five (25) TippingPoint security devices. Through the **Admin** screen, you can upgrade your license. Contact your TippingPoint representative for more information.



**Note** Users with Super User authority can perform any action in the SMS Administration window. Users with Administrator and Operator authority can view information in this screen.

## Administration: What's New

This section outlines the following major changes for the current SMS release:

- [High Availability](#)
- [Remote Syslog](#)
- [Named Resources](#)

### High Availability

The SMS includes the following enhancements to the HA functionality:

- **Seamless Failover** — Upon failover, the SMS Client closes all windows and automatically negotiates a new connection with the SMS HA cluster. The Negotiating HA Connection status dialog displays while the SMS attempts to renegotiate the connection. When the connection is complete, the status dialog disappears, the Client returns to the previous application.
- **Failover** — Because the passive SMS functions in a similar manner as the Watchdog monitor feature on an individual SMS, the active SMS may attempt to restart before any attempt is made to fail over to the passive SMS. This new behavior should significantly reduce the number of failovers caused by software error.
- **Shutdown and Reboot** — Shutdown and reboot operations now function the same way in HA as they do in a non-HA SMS environment. After shutdown and reboot, the active SMS and passive SMS return to their respective previous states.
- **Warning Messages** — When the system goes into failover and synchronization, a warning message displays and indicates the actions that users should and should not take.
- **Event Synchronization** — The user now has the ability to choose if they want to include the event data. Choosing not to include event data may reduce the amount of time for a synchronization.
- **Synchronization Progress** — During synchronization of the HA cluster, the SMS Client now displays a progress indicator that indicates the status of the synchronization effort. If immediate access is needed, synchronization can also be cancelled.

See [“High Availability” on page 475](#).

## Remote Syslog

Five new log formats were added. New logs include:

- SMS 2.5 Syslog Format
- X-Family Firewall Block
- X-Family Firewall Session
- SMS System
- SMS Audit

For the 2.5 event format, four fields were added and two were removed. New log fields include:

- Source Zone Name
- Destination Zone Name
- Incoming Physical Port
- VLAN ID

Deleted fields include:

- Device Slot — no longer valid for 2.5 devices
- Device Segment — no longer valid for 2.5 devices

See [“Management Information” on page 460](#).

## Named Resources

Added the ability to name resources individually or as a group so that they can be used with various SMS features. types of resources include VLAN IDs, IP addresses, and email addresses. See [“Named Resources” on page 487](#).

# How To Tasks

### *General Administration*

- [“How To: View the SMS System Log” on page 438](#)
- [“How To: View an SMS System Log Entry” on page 438](#)
- [“How To: View the SMS Audit Log” on page 440](#)
- [“How To: View an SMS Audit Log Entry” on page 441](#)
- [“How To: Download and Install the SMS Software” on page 443](#)
- [“How To: Import and Install SMS Software” on page 444](#)
- [“How To: Upgrade the SMS License” on page 445](#)
- [“How To: Create/Edit a User Account” on page 451](#)
- [“How To: Delete a User Account” on page 452](#)
- [“How To: Terminate a User Session” on page 453](#)

### ***Database Administration***

- [“How To: Refresh Database Maintenance” on page 456](#)
- [“How To: Edit Database Maintenance” on page 456](#)

### ***Database Maintenance***

- [“How To: Cleanup Database Maintenance” on page 456](#)
- [“How To: Backup the SMS Database” on page 457](#)
- [“How To: Restore the SMS Database” on page 458](#)
- [“How To: Schedule a Database Backup” on page 459](#)

### ***SMS Server Properties***

- [“How To: Configure the Management Settings” on page 469](#)
- [“How To: Create a new Remote Syslog for Events” on page 469](#)
- [“How To: Edit a Remote Syslog for Events” on page 470](#)
- [“How To: Configure the Network Settings” on page 471](#)
- [“How To: Configure the Authentication Settings” on page 474](#)

### ***High Availability***

- [“How To: Configure High Availability - Primary Only Option” on page 481](#)
- [“How To: Configure High Availability - Primary + Secondary Option” on page 482](#)
- [“How To: Disable High Availability” on page 484](#)

### ***Named Resources***

- [“How To: Create/Edit a Named IP Address” on page 488](#)
- [“How To: Create/Edit a Named Group of IP Addresses” on page 488](#)
- [“How To: Create/Edit a Named VLAN ID” on page 489](#)
- [“How To: Create/Edit a Named Group of VLAN IDs” on page 489](#)
- [“How To: Create/Edit a Named Email Address” on page 489](#)
- [“How To: Create/Edit a Named Group of Email Addresses” on page 490](#)

## Navigation and Menu Options

The Administration screen includes the following panes and options:

- [“Main Screen” on page 434](#)
- [“Navigational Pane” on page 435](#)
- [“Menu Bar Options” on page 436](#)

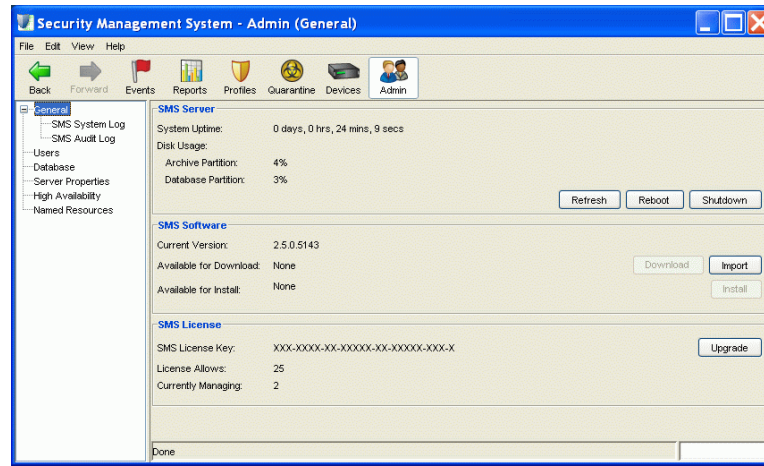
### Main Screen

The **Admin (General)** screen displays general and log information for the SMS. By default, the **Admin (General)** screen displays the server, software, and license information for the SMS.

To open the **Admin (General)** screen, click the **Admin** button on the SMS Toolbar.

The following is the Admin (General) screen

Figure 9 - 1: Admin (General) Screen



## Navigational Pane

The **Admin** Navigation pane includes the following screens:

- **General** — Provides information to manage system and audit logs, to manage the health of the SMS server, and to install software and license upgrades. See [“General Administration” on page 437](#) for details.
- **Users** — Provides options for creating and managing user accounts and managing user sessions. See [“In the Upgrade License section, enter the New License Key, and then click Apply. User Administration” on page 445](#) for details.
- **Database** — Provides database maintenance information and options for setting database backup and restore locations. See [“Database Administration” on page 454](#) for details.
- **Server Properties** — Provides options for maintaining management, network, and authentication settings for the SMS server. See [“SMS Server Properties” on page 460](#).
- **High Availability** — Provides configuration for deployment of two SMS servers acting as a primary system with a secondary back-up system. See [“High Availability” on page 475](#).
- **Named Resources** — Provides options for setting up a named entity or a group of named IP addresses, VLAN IDs and email addresses so that the named resources can be used with various SMS features. See [“Named Resources” on page 487](#).

Selected options display in the Main/List pane. For more information on that pane, see [“Main/List Pane” on page 21](#).

## Menu Bar Options

The available menu items for the Menu Bar differ according to the displayed screen and user access settings. Each screen provides options for the following:



**Note** The following list may change depending on the displayed screen or selected item in the main pane.

- **File** — Provides options to create new entries and other functions based on the currently selected and displayed screen. These options include the following:
  - *New* — *Creates a new item based on selection, such as user*
  - *Download SMS Software* — *Downloads SMS software updates*
  - *Import SMS Software from File* — *Imports an SMS software update from a file*
  - *Upgrade SMS License* — *Displays the screen for upgrading your SMS license*
  - *Log Off* — *Logs you out of the SMS*
  - *Exit* — *Closes the SMS*
- **Edit** — Provides edit options based on the currently selected and displayed screen.
  - *Details* — *Displays the details of a selected entry*
  - *Delete* — *Deletes a selected entry*
  - *Preferences* — *Displays the System Preferences dialog box. See [“System Preferences” on page 27](#).*
- **View** — Displays the screens for the options listed in the Navigation Pane.
  - *General*
  - *Users*
  - *Database*
  - *Server Properties*
  - *SMS System Log*
  - *Named Resources*
  - *High Availability*
  - *Dashboard* (see [“SMS Dashboard” on page 24](#))
- **Help** — Displays the following:
  - *Contents* — *Opens and displays the TippingPoint Security Management System Online Help.*
  - *Context sensitive help for the displayed screen.*
  - *About* — *detailed information on your currently installed Client (version number, build number, network address, and start time), and SMS (name, serial number, version, user ID, and user role), Java version and vendor, and client OS information.*

# General Administration

## Log Administration

Through the **Admin (General)** screens, users with Super User access can review and modify settings for the logs. The system and audit logs are vital components for the SMS and TippingPoint system. These logs compile and store events and data regarding the behavior and performance of the system. To reset all logs in the system, see [“How To: Reset Logs” on page 371](#).

The **Admin (General)** screen provides the following logs:

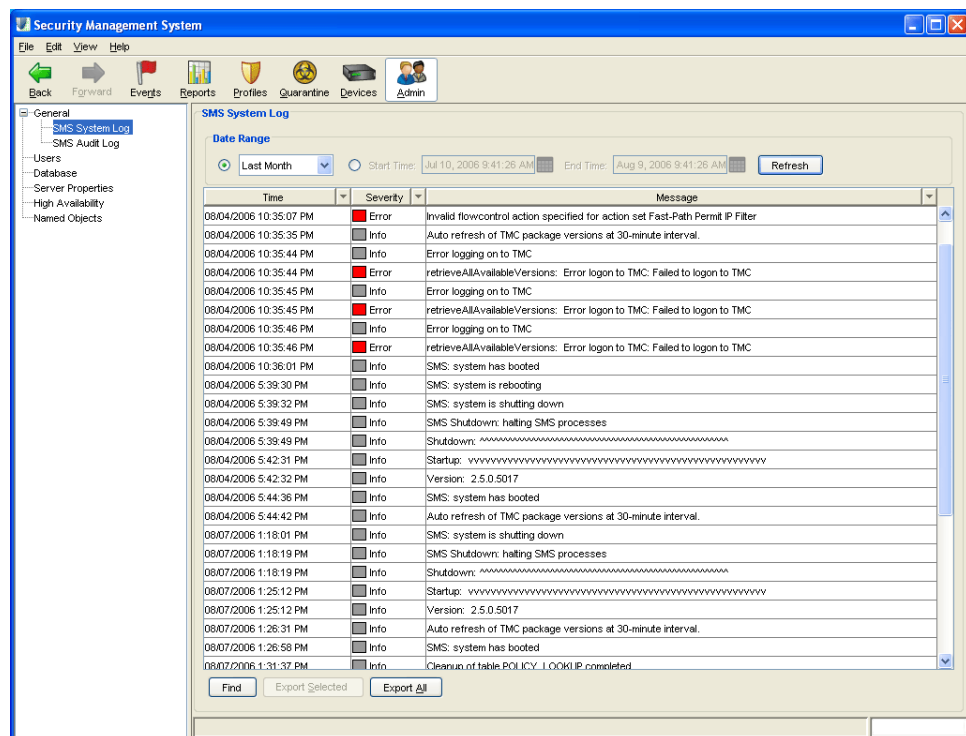
- [“SMS System Log” on page 437](#)
- [“SMS Audit Log” on page 439](#)

## SMS System Log

Through the **Admin (General - SMS System Log)** screen, you can view the system log for the SMS system. The system log contains information about the software processes that control TippingPoint devices, including startup routines, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with your TippingPoint SMS.

The following is the **Admin (General - SMS System Log)** screen:

Figure 9 - 2: Admin (General - SMS System Log) Screen



The SMS System Log includes the following information:

**Table 9 - 1: SMS System Log Information**


Column	Description
Time	The date and time of the alert or event
Severity	The severity level of the alert or event
Message	The details about the event, such as a health event or entered query

The following severity levels exist:

- **Error** — Indicates critical issues and events that occurred on your system, such as failure to log into services. These logged issues can indicate performance issues.
- **Warn** — Indicates minor issues and events that occurred on your system such as processing a filter. These events do not cause a detriment to the system.
- **Info** — Indicates events that occurred on your system without detriment to your system, such as a system shutdown and restart. These are informative messages.

To review more information on a entry, you can open a record. The entry opens, detailing the time, severity, and message. Using arrow buttons, you can continue to browse through the log entries.

**How To: View the SMS System Log**

1. On the **Admin** Navigation pane, expand the **General** entry.
2. Do one of the following:
  - On the Navigation pane, select **General** —> **SMS System Log**.
  - On the Menu Bar, select **View** —> **SMS System Log**.
 The **Admin (General - SMS System Log)** screen displays.
3. By default, the log contains information about activity that has occurred during the current day. To change the **Date Range** of listed entries, click the **Start Time** and **End Time** calendar icons  and select new values. Click **Refresh**. See [“Date and Time Controls” on page 37](#).
4. To locate a particular entry, click **Find**.
5. To update the entries in the List pane, click **Refresh**.
6. To sort entries, click the table headings. The list displays in ascending or descending order depending on the column.

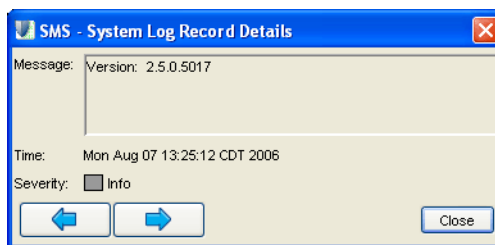
**How To: View an SMS System Log Entry**

1. On the **Admin (General - SMS System Log)** screen, select an entry. Do one of the following:
  - Double-click an entry.
  - Right-click the entry and choose **Details**.



The SMS - System Log Record Details dialog box displays.

Figure 9 - 3: SMS - System Log Record Details Dialog

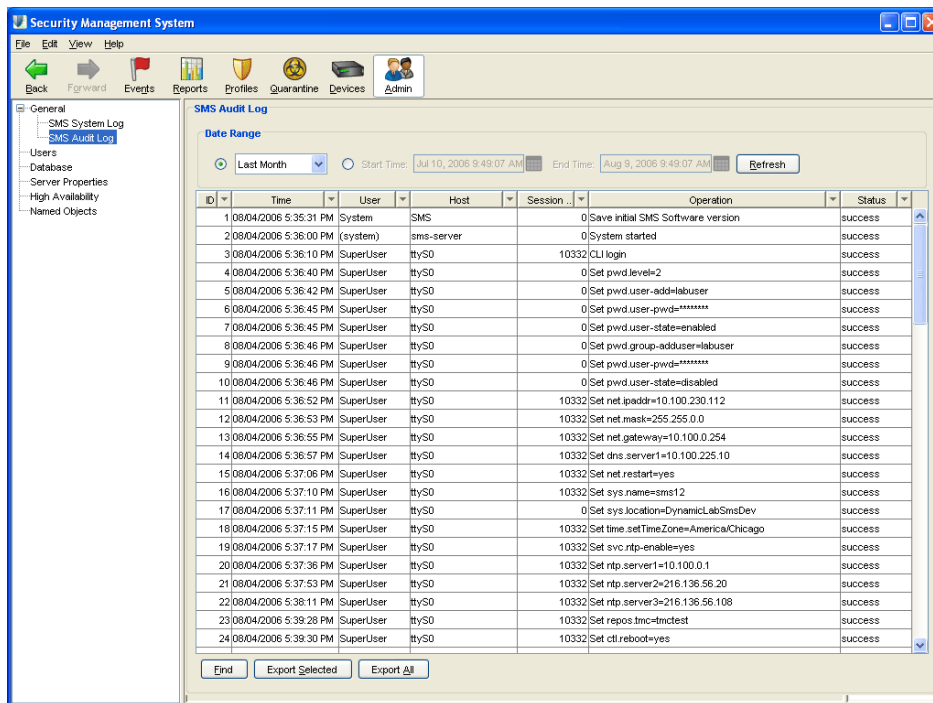


2. To continue reviewing entries, click the forward or back buttons.
3. Click **OK** to close.

### SMS Audit Log

The SMS Audit log collects and displays detailed information about user activity.

Figure 9 - 4: Admin (General - SMS Audit Log) Screen




The SMS Audit Log includes the following information:

**Table 9 - 2: SMS Audit Log**

Column	Description
ID	
Time	The date and time the action was taken
User	The username of the user that performed the action. The user may 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.
Host	The hostname of the client from which the user logged in
Session ID	An ID number assigned by the server for the logon session. You might also see the following session ID numbers: <ul style="list-style-type: none"> <li>• -1 indicates the user is not yet authenticated</li> <li>• 0 or -2 might indicate system actions rather than user actions</li> </ul>
Operation	The action performed by the user
Status	The result of the action; options are success or failure

You can also view user activity from the [Active Sessions](#) section of the **Admin (Users)** screen. When you view the log, the user listed for the logged events may include SMS users on the SMS system.

#### How To: View the SMS Audit Log

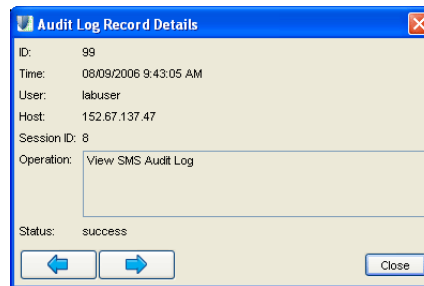
1. On the **Admin** Navigation pane, expand the **General** entry.
2. On the Navigation pane, select **General (SMS Audit Log)**.  
The **Admin (General - SMS Audit Log)** screen displays.
3. By default, the log contains information about activity that has occurred during the current day. To change the **Date Range** of listed entries, click the **Start Time** and **End Time** calendar icons  and select new values. Click **Refresh**. See [“Date and Time Controls” on page 37](#).
4. To locate a particular entry, click **Find**.
5. To update the entries in the List pane, click **Refresh**.
6. To sort entries, click the table headings. The list displays in ascending or descending order depending on the column.

### How To: View an SMS Audit Log Entry

1. On the **Admin (General - SMS Audit Log)** screen, select an entry.
2. Do one of the following:
  - Double-click an entry.
  - Right-click the entry and choose **Details**.

The **Audit Log Record Details** dialog box displays.

Figure 9 - 5: Audit Log Record Details



3. To continue reviewing entries, click the forward or back buttons.
4. Click **OK** to close.

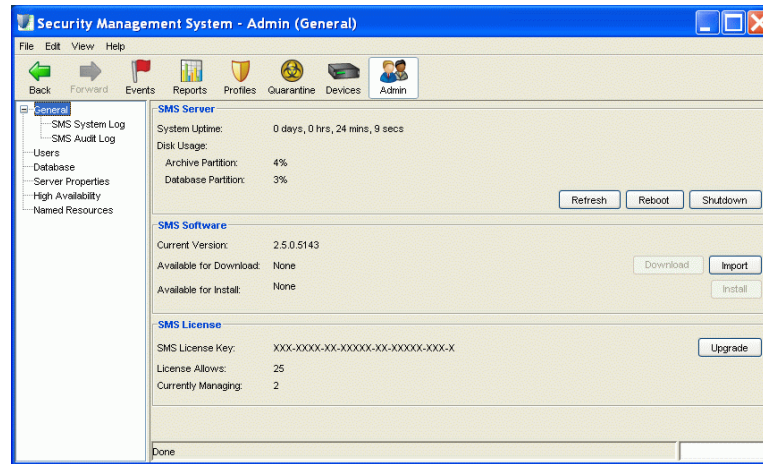
## SMS Status

At times, you may need to review the status of the system health and update software. Through the **Admin (General)** screen, the following information is available:

- [“SMS Server” on page 442](#)
- [“SMS Software” on page 442](#)
- [“SMS License” on page 444](#)

The following is the Admin (General) Screen.

Figure 9 - 6: Admin (General) Screen



## SMS Server

From the **SMS Server** section of the **Admin (General)** screen you can review and manage the health of the SMS server.

You can do the following in this section:

- **Refresh** — To see the current information for the SMS, click **Refresh**. The information refreshes on the screen.
- **Reboot** — If a health problem is apparent and a reboot is warranted, click **Reboot**.
- **Shutdown** — To halt and turn-off the SMS, click **Shutdown**.

## SMS Software

From the **SMS Software** section of the **Admin (General)** screen you can install an upgrade of your SMS software through one of two ways:

- [“Download and Install the SMS Software” on page 443](#)
- [“Import and Install SMS Software” on page 444](#)



**CAUTION** Upgrading the SMS software causes the SMS Server to reboot and closes all connections. You may want to make sure other users are not logged in during an update of the SMS.

The **SMS Software** section displays the following information:

Table 9 - 3: SMS Software Information

Information	Description
Current Version	The version number for the software currently installed on your SMS

Table 9 - 3: SMS Software Information (Continued)

Information	Description
Available for Download	The most recent version on the TMC. If this number and the Current Version number match, you do not need to download or upgrade.
Available for Install	The version that you downloaded from the TMC that is available for installation.

### How To: Download and Install the SMS Software

Downloading gets the latest software from the Threat Management Center web site (<https://tmc.tippingpoint.com>). When complete, you can choose to install the listed available package.



**CAUTION** Because a full upgrade of the SMS software is over 400 MB, it can take a significant amount of time to download depending on your network configuration.

1. Open the **Admin (General)** screen.
2. Do one of the following:
  - In the **SMS Software** section, click **Download**.
  - On the Menu Bar, select **File** —> **Download SMS Software**.
3. Click **Download from TMC**. A dialog box displays with a drop-down list of available packages by version. Select the latest package.
4. Click **Download**. A dialog box displays with the download progress. When complete, click **Hide**. The package downloads and displays in the TOS Inventory table.
5. Select a package entry in the TOS Inventory.
6. Click **Distribute**. The New Distribution dialog box displays.
7. Select the **Targets** for the distribution as **All Devices** or browse the expandable list to select specific device targets. You can also select the priority. By default, it is set for High priority. To perform the update without taking significant resources, you can deselect this option. However, the update may take more time to complete.



**Note** The screen displays a note that the update reboots the IPS device and may replace the Digital Vaccine with an older package.

8. Click **OK**. The update installs on the selected device(s).




**Note** You must update the SMS prior to updating your devices.


Do not perform updates of TOS or DV packages to X505 devices through the SMS. Perform these updates directly through the X505 LSM.

### How To: Import and Install SMS Software

Importing gets the software from a file, such as a CD release from TippingPoint or previously downloaded file. When you import, the system imports the file and installs it directly with one step.

 **Note** The import checks if the package being imported is a back-level version (or older version). It downloads the package from the client and starts the upgrade process. The SMS does not support rolling back to back-level versions. You should always upgrade, not rollback, to an SMS software version.

1. You must first download the file from TMC, <https://tmc.tippingpoint.com>.

 **Note** To avoid unexpected behavior on the SMS, do not change the name of this file.

2. Open the **Admin (General)** screen.
3. Do one of the following:
  - In the **SMS Software** section, click **Import**.
  - On the Menu Bar, select **File** —> **Import SMS Software from File**.
4. The **Choose File** dialog box opens. Locate the file, and then click **OK**.
5. The SMS prompts you with a message. Click **OK** to continue. The installation process begins. When complete, the SMS server reboots. If you click **Cancel**, the procedure cancels without updating the SMS software.

### SMS License

From the **SMS License** section of the **Admin (General)** screen, you can upgrade the SMS license. The **SMS License** section lists information about the currently installed license for your SMS.

By default, each license key allows you to manage 25 devices. To manage more devices, you must purchase a new license and install its license key. You can purchase licenses to manage five, ten, or 100 devices.

 **Note** When you unmanage a device, it no longer counts against your SMS license. See [“Devices” on page 293](#) for details.

The **SMS License** section displays the following information:

**Table 9 - 4: Health Information**

Information	Description
SMS License Key	Displays the currently installed license key. If you are using the default license, this value appears as <b>XXX-XXXX-XX-XXXXXX-XX-XXX-X</b> .
License Allows	Indicates how many IPS devices you can manage with this license
Currently Managing	Indicates how many IPS devices you are managing at present. This value changes as you manage and unmanage devices.

### How To: Upgrade the SMS License

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 when the license will be available.
3. Once the purchased license is available, open the **Admin (General)** screen.
4. Open the **Admin - SMS License** screen by one of the following methods:
  - Locate the **SMS License section**, and then click **Upgrade**
  - Select the menu item **File** —> **Upgrade SMS License**
5. In the **Upgrade License** section, enter the **New License Key**, and then click **Apply**. User Administration

To maintain a secure management interface, you must create users specifically for SMS operations and assign user roles to limit their access to SMS functionality. The SMS ships with a **Super User** user account defined at the factory. This is used for initial configuration of the system, creation of other user accounts, and access to the SMS CLI.



**Note** You must create a new account during the OBE configuration process. For more information, see the TippingPoint SMS Installation and Configuration Guide.

If you need to recover your password, the SMS provides an automated recovery mechanism. For information, see [“Password Recovery” on page 541](#).



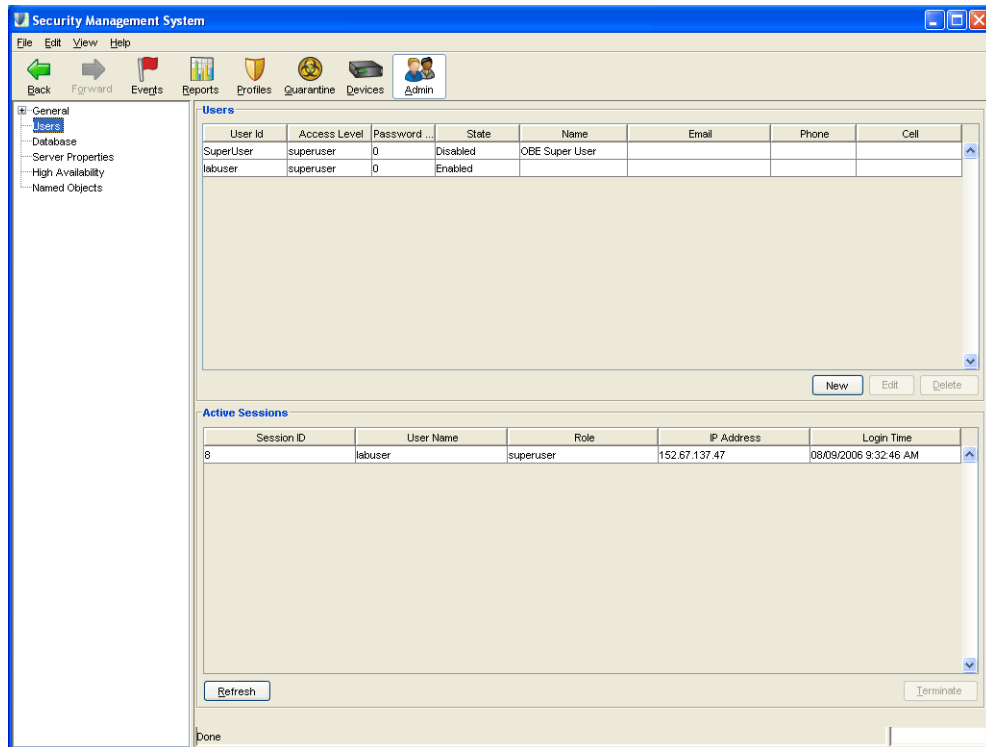
**CAUTION** You should take care to always maintain at least one active account with Super User access, because this account is used during password recovery.



**Note** If you use a RADIUS server for user authentication, the **State** for the accounts displays as “RADIUS.”

The following is the **Admin - Users** screen:

Figure 9 - 7: Admin - Users Screen



From the **Admin - Users** screen, you can do the following:

- [Create/Edit a User Account](#)
- [Delete a User Account](#)

Each account has the following settings:

- [Usernames](#)
- [Passwords](#)
- [User Roles](#)

This section also has information on the following items:

- [Security Level Capabilities](#)
- [Managing User Accounts](#)
- [Password Expired](#)
- [Active Sessions](#)



## Username

The name for a user account is the username. You assign a username to a user account when you create the account. A valid username name meets the following criteria depending on the level of security:

**Table 9 - 5: Security Levels and Account Names**

Level	Description
Low Security - Level 0	User names cannot contain spaces.
Medium Security - Level 1	User names must contain at least 6 characters without spaces.
High Security - Level 2	User names must meet Level 1 restrictions and the following: <ul style="list-style-type: none"> <li>• Must contain at least two alphabetic characters</li> <li>• Must contain at least one numeric character</li> <li>• Must contain at least one non-alphanumeric character. A non-alphanumeric character includes any character that is not a digit or a letter. Do not use spaces in the User name.</li> </ul>



**Note** If your user account is not authorized for the proper user roles, menu items and screen options may be disabled. See [“User Roles” on page 448](#) for more information.

The following are examples of user account usernames:

**Table 9 - 6: Username Examples**

Valid Login Names	Invalid Login Names
fjohnson	fredj (too short in Levels 1 and 2, valid for Level 0)
fredj123	fred j 123 (contains spaces)
fredj-123	fj123 (too short)
fredj-*123	fj 123 (contains spaces)

## Passwords

Passwords are a vital component of a user account. Many malicious attacks against networks and services occur with poorly constructed and used passwords. To provide a high-level of protection for the TippingPoint system, you should always use strong passwords. Strong passwords follow the High Level Security as described in the following table. The password requirements depend on the security level of the system.

The following table details the levels and requirements:

**Table 9 - 7: Security Levels and Passwords**

Level	Description
Low Security - Level 0	Passwords are unrestricted. Any length and format is allowed for the password. A password must be defined.
Medium Security - Level 1	Passwords must contain at least 8 characters without spaces.
High Security - Level 2	Passwords must meet Level 1 restrictions and the following: <ul style="list-style-type: none"> <li>• Must contain at least two alphabetic characters</li> <li>• Must contain at least one numeric character</li> <li>• Must contain at least one non-alphanumeric character. A non-alphanumeric character includes any character that is not a digit or a letter. Do not use spaces in the password.</li> </ul>



**Note** A non-alphanumeric character includes any character that is not a digit, a letter, or a space. **The password must not contain any spaces.**

The following are examples of passwords:

**Table 9 - 8: Password Examples**

Valid Passwords	Invalid Passwords
my-pa55word	my-pa55 (too short)
my-b1rthday	mybirthday (must contain numeric)
myd*g'snam3	mydogsnam3 (must contain a non-alphanumeric character)

## User Roles

The following user roles are available:

- **Super User** — Full access to use and manage all function available in the system. Super users can manage all reports (saved, scheduled, results), devices, profiles, and segment groups. This role grants access to the other user roles.
- **Administrator** — Advanced access to monitor and manage functions in the system. This role has access to all devices, profiles, segment groups as granted by the Super User.
- **Operator** — Basic access to review the status of the system. This role has read-only access to all devices, profiles, segment groups as granted by the Super User.



**Note** SSH and Telnet access is restricted to Super Users.

These messages may indicate when the user logged in, performed actions, and logged out.



**Note** If you need to recover your password, the SMS provides an automated recovery mechanism. For information, see [“Password Recovery” on page 541](#).

## Security Level Capabilities

Security level/user capabilities are summarized in the table below.

**Table 9 - 9: User Role Capabilities**

Functional Area	Operator	Administrator	Super-user
Events	view all event types (for segments with granted access)	all - for all event types (for segments with granted access)	all
Reports	view all reports	create reports (against segments and devices with granted access)	all
Profiles *	view	create and manage reports (with granted access)	all
Device Configuration	view (with granted access)	all (with granted access)	all
Admin/User	change own password	change own password	can create and edit all user accounts
Help	view	view	view

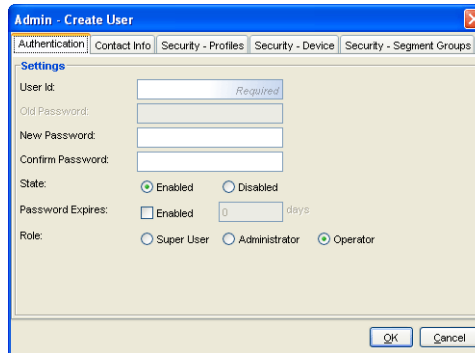
\* Shared Settings are Super Users-only

## Managing User Accounts

Through the **Admin - Users** screen, you can view, create, edit, and delete user accounts. You must have Super User role access to perform these procedures. The **Create/Edit User** dialog box allows you to view, create, and edit information for a user account. This information includes the account user name, password, password expiration date, and identification information.

When you create or edit a user account, a dialog box displays with various tabs for entering user data.

Figure 9 - 8: Admin - Create/Edit User Dialog Box




The user information includes the following tabbed sections:

Table 9 - 10: User Information

Tab	Description
Authentication	The information for the account including username, password, expiration, and assigned user role. The username is entered when opening the SMS Client.
Contact Info	The contact information for the account including name, phone number, and email address.
Security - Profile	The list of profiles the user has permission to access and modify configuration settings for. Only a user with Super User role access can modify these settings for an account.
Security - Device	The list of devices the user has permission to access and modify configuration settings for. Only a user with Super User role access can modify these settings for an account.
Security - Segment Groups	The list of segment groups the user has permission to access and distribute profiles to. Only a user with Super User role access can modify these settings for an account.

 **CAUTION** If you cannot log in to the SMS in any Super User role, you can perform a password recovery or contact TippingPoint support. For information, see [“Password Recovery” on page 541](#).

 **Note** Passwords are encrypted. They display as asterisk marks (\*) in the fields.



**Note** Note: If you define an account or password expiration date, that definition represents the total number of days for the setting and not the number of days remaining.

You can do the following:

- [“How To: Create/Edit a User Account” on page 451](#)
- [“How To: Delete a User Account” on page 452](#)



**Note** A user can not access the SMS if you delete their account. If you want to suspend the usage of their account, simply edit the account and select the **Disable** check box.

### How To: Create/Edit a User Account

1. Open the **Admin - Users** screen.
2. Do one of the following, to create a new user:
  - Click **New**.
  - On the Menu Bar, select the **File** —> **New** —> **User** menu item.
  - Right-click an entry and click **New**.

To edit, select a user entry and do one of the following:

- Double-click the user account entry.
- Click **Edit**.
- On the Menu Bar, select the **Edit** —> **Details**.
- Right-click an entry and click **Edit**.

The appropriate dialog box displays.

3. On the **Authentication** tab, enter the user information for the account:
  - Enter a **User Id**. See [“Usernames” on page 447](#) for information on username creation rules.
  - Select **Enabled** to enable the account.
  - Enter a new password in the **New Password** and **Confirm Password** fields. The two passwords must match exactly to be accepted. See [“Passwords” on page 447](#) for information on password creation rules. Leave the old password empty.
  - Optionally, select the **Enabled** check box to enable password expiration. Define an expiration period (in days) for the password in the **Password Expires** field.
  - Select a **Role** for the account: **Super User**, **Administrator**, and **Operator**. See [“User Roles” on page 448](#) for more information.

4. On the **Contact Info** tab, enter the contact information for the account:
  - In the **Name** field, enter the full name of the user.
  - In the **Email** field, type the e-mail address of the user, such as bob@mail.com.
  - In the **Phone Number** field, enter the area code and phone number of the user.
  - In the **Cell** field, enter the area code and cell phone number of the user.
5. On the **Security - Profiles** tab, select the profiles the user can access and modify configuration settings for. To modify settings on devices, the user must have the Administrator or Super User role.
6. On the **Security - Device** tab, select the devices the user can access and modify configuration settings for. To modify settings on devices, the user must have the Administrator or Super User role.
7. On the **Security - Segment Group** tab, select the segment group the user can access and distribute profiles to.
8. Click **OK**.

### How To: Delete a User Account

1. Open the **Admin - Users** screen.
2. Select a user account and do one of the following:
  - Click **Delete**.
  - On the Menu Bar, select the **Edit** —> **Delete**.
  - Right-click an entry and click **Delete**.

The system displays a message verifying the deletion.

3. Click **OK**.



**Note** A user can not access the SMS if you delete their account. If you want to suspend the usage of their account, simply edit the account and select the **Disable** check box.

## Password Expired

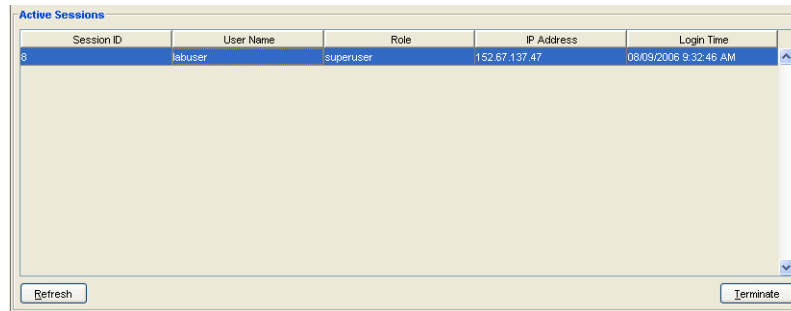
The **Password Expired** dialog box is displayed when a user attempts to logon to the SMS after the expiration date set for their password. You must type your expired password, a new password, and a confirmation of your new password.

## Active Sessions

The Active Sessions section of the **Admin - Users** screen lists all the existing logon sessions on the server. You can terminate an active sessions from this screen. The SMS Client will close on the user immediately without warning.

If you have the Super User role, you can terminate any session that appears in this section by selecting a session and clicking the **Terminate** button.

**Figure 9 - 9: Active Sessions**



The **Active Sessions** section displays the following information:

**Table 9 - 11: Active Sessions Details**

Column	Description
Session ID	An ID number assigned by the server for the logon session
User Name	The username of the user that performed the action
Role	The role assigned to that user name. This role includes super user, administrator, and operator.
IP Address	The IP address of the workstation from which the user logged in
Login Time	The date and time the user logged on

If you have Super User authority, you can terminate a user session from this dialog box and have access to all sessions. Admin and operator users only see their access.

#### How To: Terminate a User Session

1. Open the **Admin - Users** screen.
2. Locate the **Active Sessions** section.
3. Select an active session.
4. Click **Terminate**.

The client session immediately closes for the user. The user does not receive a warning before the client closes. The user does receive an alert telling him or her to contact the Super User.



**Note** Only users with Super User role access can terminate an active session.

# Database Administration

The SMS database stores and organizes all information required to operate your TippingPoint environment. Through the **Admin - Database** screen, you can perform a database backup and restore using a database wizard. This wizard provides options for backing up the database directly to your local system or the SMS server. The backup options also include NFS and Samba (SMB). Using the wizard, you can quickly and easily backup and restore your database without recalling complex commands or code. You can also set a scheduled backup for the database.



**Note** You should perform backup and restore procedures using the wizard in the SMS Client.

This screen allows you to backup and restore your database. See [“Database Backup and Restore” on page 457](#). You can also manage database maintenance. In the **Database Maintenance** section, you can select a section of data and do the following:

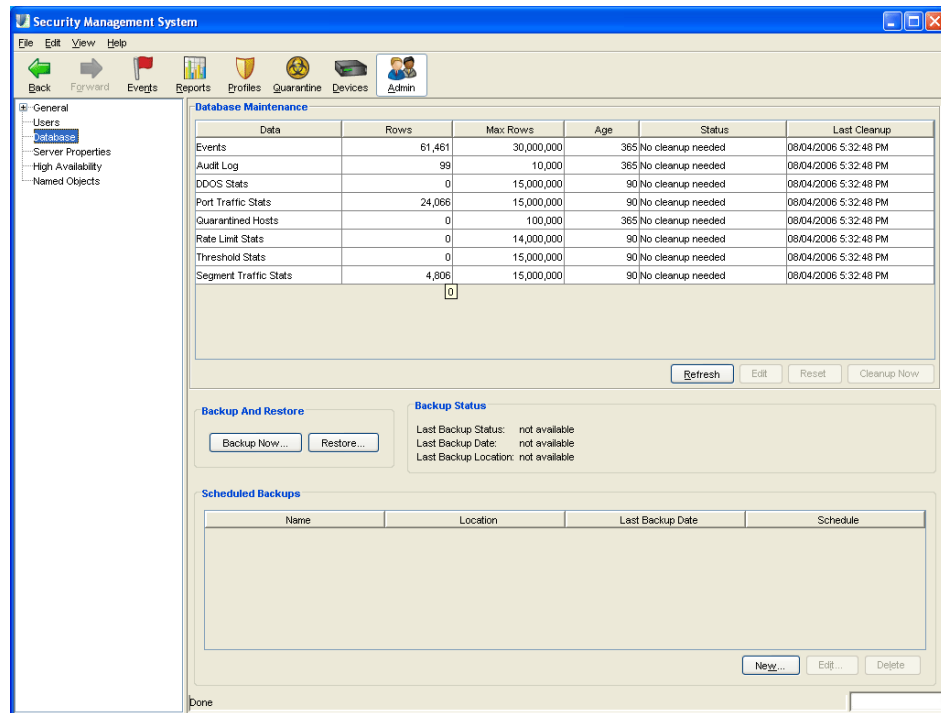
- Edit the maintenance settings. These settings allow you to enter values for the maximum rows of database entries and the amount of days to keep data before removing it.
  - *Set the Max Rows for each table in the database.*
  - *Set the age for the data.*
- Perform cleanup procedures for selected database entries. The SMS system removes all entries older than the **Age** setting and entries that outnumber the **Max Rows** setting. This process runs automatically on a daily basis. You can run a cleanup process anytime by clicking **Cleanup Now**.

When the database reaches the Max Rows value for the table or the data entries reach the Age setting, the SMS begins a clean-up process. This process removes entries based on the max allowed entries and age of the data. If the max number of rows is reached, a clean-up process is scheduled even if the data is



not older than the configured data age. Also, if the data becomes older than the configured age, it is removed even if the max number of rows is not reached.

Figure 9 - 10: Admin - Database Screen



The **Database Maintenance** section displays the following information:

Table 9 - 12: Database Maintenance Details

Column	Description
Data	The name of the database data
Rows	The current number of rows of the data in the database
Max Rows	The 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	The amount of days to keep data before clearing it. The system clears data older than this setting. You can edit this setting.
Last Cleanup	The last time the entries were cleaned. Cleanup occurs daily. You can also perform a cleanup by clicking <b>Cleanup Now</b> .

From the Database screen you can do the following tasks:

- **Database Maintenance**
  - [“Database Maintenance” on page 456](#)
  - [“Edit Database Maintenance” on page 456](#)
  - [“Cleanup Database Maintenance” on page 456](#)
- **Database Backup and Restore**
  - [“Backup the SMS Database” on page 457](#)
  - [“Restore the SMS Database” on page 458](#)
- **Scheduled Backups**
  - [“Schedule a Database Backup” on page 459](#)

## Database Maintenance

### How To: Refresh Database Maintenance

1. From the **Admin** Navigation menu, select **Database**.
2. In the **Database Maintenance** section, click **Refresh** to update the list of events when the database was backed up or restored.

### How To: Edit Database Maintenance

1. From the **Admin** Navigation menu, select **Database**.
2. In the **Database Maintenance** section, select an entry and click **Edit**. The **Admin - Maintenance Settings** dialog box displays.
3. In the **Database Management** section, specify which data you want to clear.
  - Enter a value for the number of days for cleanup purposes. Entries older than this entry will be removed when you perform cleanup.
  - Enter a value for the max number of records for 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. The default value is 10,000. For Quarantine, the default is 100,000.
4. Click **OK**.

### How To: Cleanup Database Maintenance

1. From the **Admin** Navigation menu, select **Database**.
2. In the **Database Maintenance** section, select an entry and click **Cleanup Now**.

Depending on settings, the system removes or archives all entries older than the **Age** setting and more than the set **Max Rows**.

## Database Backup and Restore

The database contains configuration and administrative data for the SMS system, including user accounts, and segment and device configuration. When planning the backup (immediate and scheduled) of your SMS, you should perform the operation during a time when users will not actively modify data. The time and space needed for this backup and restore could also take a good deal of time depending on the type of data you backed up. You should take the time and access to users when scheduling the procedures in your office or network environment. Performing the procedures during high-usage times during your office hours could cause performance errors.



**TIP** Perform the backup (immediate and scheduled) and restore of your database during off hours of your office. For example, running the procedures after office hours ensures a full copy of current settings and information and better performance when performing the operation.

During the backup and restore procedure, the SMS client automatically verifies files. If the restore file is corrupted or incorrect, the system displays an error message. You can review these error messages in the System Log. The message states either the backup or restore operation failed. If the file verifies without error, the system overwrites the database of the SMS restoring the saved configuration and administrative settings. After all backup and restore operations complete, the system automatically reboots, ensuring database integrity.



**Note** To cancel a backup or restore operation, click the **Cancel** button.

When you complete the backup or restore operation, the system performs the following tasks:

- Mounts the backup or restore destination.
- Stops the database and SMS server applications
- Copies the database and configuration files to (for backups) or from (for restores) the user-specified directory
- Unmounts the backup or restore destination
- Restarts the database and SMS server applications

You can do the following tasks:

- [“Backup the SMS Database” on page 457](#)
- [“Restore the SMS Database” on page 458](#)
- [“Schedule a Database Backup” on page 459](#)

### How To: Backup the SMS Database

1. From the **Admin** Navigation menu, select **Database**.
2. From the **Backup and Restore** area, click **Backup Now**.  
The **SMS Backup Wizard** displays.

3. Click **Next**.  
The **Backup Configuration** page displays.
4. Configure the following data backup settings, and then click **Next**:
  - **Include # of the most recent Digital Vaccine(s)** — Includes a set number of Digital Vaccine updates (not to exceed six) to the backup.
  - **Include # of the most recent Device TOS packages** — Includes a set number of TOS updates (not to exceed six) to the backup.
  - **Include contents of events table** — Saves the contents of the event table. Including this large amount of data may cause the backup procedure to take an extended amount of time and space. You should not include this information when backing up during busy office hours.
  - **Email the backup results to the SMS notification list members** — Sends e-mail confirmation and status to the list of notifications set in the **Server - Network** screen.
  - **Use timestamp as suffix of the backup file name** — Appends the date and military time to the filename for archiving purposes.
5. Select the **Backup Location**, and then click **Next**:
  - **HTTP(S) downloadable from SMS**
  - **NFS**
  - **SMB (Microsoft Share)**
6. If you selected **HTTP(S) downloadable from SMS**, write down or cut and paste the **Properties**, **Schedule**, and **Location** information that is displayed. You will need this information when downloading the final backup.
7. If you selected **NFS**, enter the following **Remote Mount Configuration** information, and then click **Next**:
  - **Location** — The path of the file. For example:  

```
host:/export/...path.../filename.bak
```
8. If you selected **SMB (Microsoft Share)**, enter the following **Remote Mount Configuration** information, and then click **Next**:
  - **Location** — The path of the file. For example:  

```
//host/share/...path.../filename.bak
```
  - **Username** — Your SMB username
  - **Domain** — Your SMB domain
  - **Password** — Your SMB password
9. Click **Finish**. The backup procedure begins and may take a considerable amount of time depending on your configuration.


### How To: Restore the SMS Database

1. From the **Admin** Navigation menu, select **Database**.
2. From the **Backup and Restore** area, click **Restore**. The **SMS Restore Wizard** displays.

3. Click **Next**.
4. A file browser opens. Browse to and select the backup file for the database you want to restore.
5. The SMS system runs verification procedures against the database. If the database is corrupted or has an issue, the SMS displays an error message. The file must pass the verification to be used.
6. If the file passes verification, the database is restored. A status message displays the process. It overwrites the currently used database. You should perform this procedure without other users accessing the system.

The system automatically reboots.

### How To: Schedule a Database Backup

1. From the **Admin** Navigation menu, select **Database**.
2. In the **Scheduled Backups** area, click **New** or select an existing backup and click **Edit**. The **SMS Backup Wizard** displays and guides you through the setup.
3. Schedule the backup: One Time, Daily, Weekly, or Monthly.
4. For a **One Time** schedule, select a date by clicking the calendar icon . See [“Date and Time Controls” on page 37](#). Click **Next**.
5. For a **Daily** schedule, select **Daily** and a time. Click **Next**.
6. For a **Weekly** schedule, select **Weekly** and a day from the available check boxes. Then select a time. For example, Wednesday at 12:00am. Click **Next**.
7. For a **Monthly** schedule, select **Monthly** and a day and time from the drop down menus. For example, you can select On the 1st day at 12:00am. Click **Next**.
8. Configure the data backup settings and click **Next**:
  - **Email the SMS notification list the backup results** — Sends e-mail confirmation and status to the list of notifications set in the **Server - Network** screen.
  - **Include contents of the event table** — Saves the contents of the event table. Including this large amount of data may cause the backup procedure to take an extended amount of time and space. You should not include this information when backing up during busy office hours.
  - **Include # of the most recent (by import date) Digital Vaccine packages** — Includes a set number of Digital Vaccine updates (not to exceed six) to the backup.
  - **Include # of the most recent (by import date) Device update packages** — Includes a set number of TOS updates (not to exceed six) to the backup.
9. The final screen provides a summary of the schedule. You can create one schedule for backups. To edit this schedule, perform these instructions again.

# SMS Server Properties

Through the **Admin** screen, users with SuperUser access can modify the SMS server settings, including management and network parameters.

The required configuration was defined when the SMS server was initially installed on your network. However, you can change this information at any time from the **Admin** screen. See [“Getting Started” on page 31](#) for more detailed information about required configuration settings. The `set` command in the [“CLI Reference” on page 491](#) provides information about optional configuration settings.

You can also use these configuration settings to connect to netForensics™. SMS can connect to and access functionality and information with netForensics.

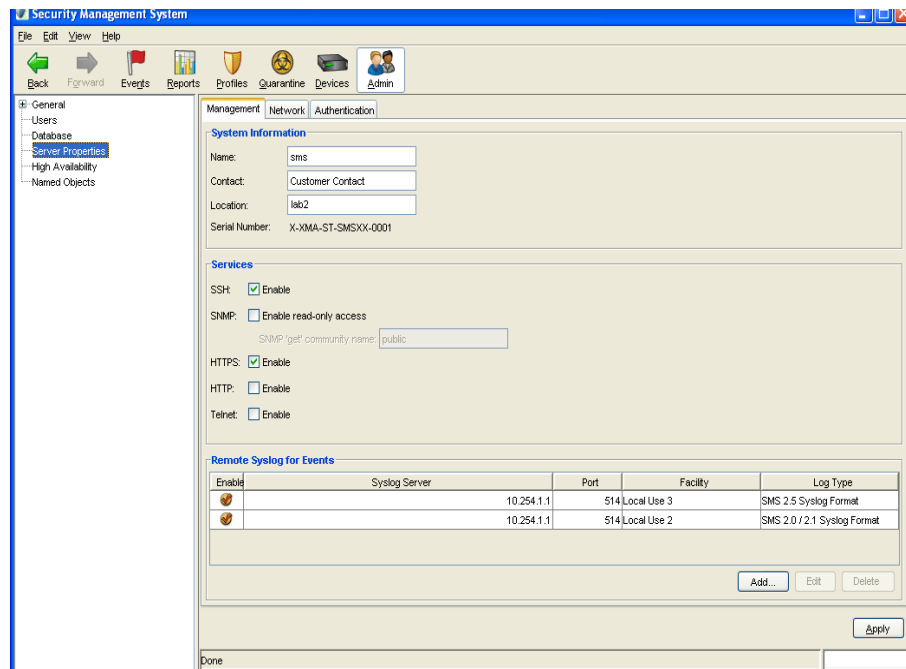
You can update the following information:

- [“Management Information” on page 460](#)
- [“Network Information” on page 470](#)

## Management Information

On the **Server Properties - Management** screen, you can update information for management network settings. These settings include the server information and service for the SMS server. You can update information and enable services for communicating between the devices, SMS, and CLI. You should carefully consider the services you enable. Not all services are secure, such as HTTP and Telnet.:

Figure 9 - 11: Server Properties - Management Screen



The **Server Properties - Management** screen has the following settings:

Table 9 - 13: Management Settings

Setting	Description
Name	The fully-qualified hostname of the SMS. When using High Availability, you may want to name the SMS according to being the active or passive system.
Contact	The name or e-mail address of the system administration responsible for the server
Location	The location of the server or administrator
Serial Number	The serial number of the server
SSH	Secure communication connection used for CLI. Requires Super User access.
SNMP	Provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). If you enable SNMP, you establish read-only access to the system. You can restrict access with the <b>SNMP 'get' community name</b> field. The default name is "public."
HTTPS	Secure network communication for web pages. Enabling HTTPS enables web services for the SMS. See <i>TipingPoint SMS Web Services API</i> .
HTTP	Unsecure network communication connection for web pages. Enabling HTTPS enables web services for the SMS. See <i>TipingPoint SMS Web Services API</i> .
Telnet	Unsecure network communication connection used for CLI. Requires Super User access.
Remote Syslog for Events	Option to specify the IP address and port to send events. You can use this option for netForensics Integration. The feature provides an option to use: <ul style="list-style-type: none"> <li>• SMS 2.0/2.1 Syslog format</li> <li>• SMS 2.5 Syslog format</li> <li>• X-Family firewall block</li> <li>• X-Family firewall session</li> <li>• SMS System</li> <li>• SMS Audit</li> </ul>



**Note** Remember that SNMP, HTTP, and Telnet are not secure services.



**Note** SMS Web Services is available for integrations. To implement these services, enable HTTP/HTTPS. For more information, see [TippingPoint SMS Web Services API](#).

## Remote Syslog Record Formats and Examples

The SMS supports Remote Syslog for events. To set up remote syslogs, see [Create a new Remote Syslog for Events](#). For information about record formats and example logs, refer to the following:

### *SMS 2.0/2.1 Syslog*

- [SMS 2.0/2.1 Syslog Format](#)
- [SMS 2.0/2.1 Syslog Example](#)

### *SMS 2.5 Syslog*

- [SMS 2.5 Syslog Format](#)
- [SMS 2.5 Syslog Example](#)

### *Firewall Session Syslog*

- [Firewall Session Syslog Format](#)
- [Firewall Session Syslog Example](#)

### *Firewall Block Syslog*

- [Firewall Block Syslog Format](#)
- [Firewall Block Syslog Example](#)

### *SMS Audit Syslog*

- [SMS Audit Syslog Format](#)
- [SMS Audit Syslog Example](#)

### *SMS System Syslog*

- [SMS System Syslog Format](#)
- [SMS System Syslog Example](#)

## SMS 2.0/2.1 Syslog Format

Table 9 - 14: Remote Syslog Events Record Format (SMS V2.0/2.1)

Column	Definition
0	Syslog category — "<32>" — This field is the defined facility, and the severity.
1	Action Type: <ul style="list-style-type: none"> <li>• 7 is Permit</li> <li>• 8 is Block</li> <li>• 9 is P2P</li> </ul>



Table 9 - 14: Remote Syslog Events Record Format (SMS V2.0/2.1) (Continued)

Column	Definition
2	Severity: <ul style="list-style-type: none"> <li>• 0 is Normal</li> <li>• 1 is Low</li> <li>• 2 is Minor</li> <li>• 3 is Major</li> <li>• 4 is Critical</li> </ul>
3	Policy UUID — TippingPoint UUID for policy
4	Signature UUID — TippingPoint UUID for Signature
5	Signature Name — User friendly name of Signature & Policy
6	Signature Number
7	Signature Protocol — This is the protocol of signature, IP, UDP, TCP, HTTP, and so on.
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 Signature
17	Event timestamp in milliseconds

## SMS 2.0/2.1 Syslog Example

The following is an example of output for the log:

```
<34>[TAB]7[TAB]4[TAB]00000002-0002-0002-0002-
000000002557[TAB]00000001-0001-0001-0001-000000002557[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
```

The default settings are TAB for delimiter and Security/Authorization for facility.

## SMS 2.5 Syslog Format

Table 9 - 15: Remote Syslog Events Record Format (SMS V2.5)

Column	Definition
0	Syslog category — "<32>" — This field is the defined facility, and the severity.
1	Action Type: <ul style="list-style-type: none"> <li>• 7 is Permit</li> <li>• 8 is Block</li> <li>• 9 is P2P</li> </ul>
2	Severity: <ul style="list-style-type: none"> <li>• 0 is Normal</li> <li>• 1 is Low</li> <li>• 2 is Minor</li> <li>• 3 is Major</li> <li>• 4 is Critical</li> </ul>
3	Policy UUID — TippingPoint UUID for policy
4	Signature UUID — TippingPoint UUID for Signature
5	Signature Name — User friendly name of Signature & Policy
6	Signature Number
7	Signature Protocol — This is the protocol of signature, IP, UDP, TCP, HTTP, and so on.
8	Source Address
9	Source Port
10	Destination Address
11	Destination Port
12	Source Zone Name
13	Destination Zone Name

Column	Definition
14	Incoming Physical Port
15	VLAN ID
16	Device Segment — Device segment of above slot that got event
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

## SMS 2.5 Syslog Example

The following is an example of output for the log:

```
7<tab>2<tab>00000002-0002-0002-0002-000000000053<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
```

The default settings are TAB for delimiter and Security/Authorization for facility.

## Firewall Session Syslog Format

Table 9 - 16: Remote Syslog Events Record Format (Firewall Session)

Column	Definition
0	Source Address
1	Source Port
2	Destination Address
3	Destination Port
4	Source Zone Name
5	Destination Zone Name
6	Device Name — User friendly name of the device event was received
7	Protocol Name
8	Rule ID
9	Category
10	URL
11	Session Duration
12	Transferred Bytes
13	Message
14	Timestamp in milliseconds

## Firewall Session Syslog Example

The following is an example of output for the log:

```
192.168.200.254<tab>8<tab>10.0.0.1<tab>8<tab>VPN<tab>this-
device<tab>zaxby-1<tab>1<tab>ICMP(1)<tab>9<tab><tab><tab>
<tab>0<tab>Regular Session Start<tab>1168484316066
```

The default settings are TAB for delimiter and Security/Authorization for facility.

## Firewall Block Syslog Format

Table 9 - 17: Remote Syslog Events Record Format (Firewall Block)

Column	Definition
0	Source Address
1	Source Port
2	Destination Address
3	Destination Port
4	Hit count
5	Source Zone Name
6	Destination Zone Name
7	Incoming Physical Port
8	VLAN ID
9	Device Name
10	Protocol Name
11	Protocol Type
12	Rule ID
13	Category
14	URL

## Firewall Block Syslog Example

The following is an example of output for the log:

```
10.100.0.1<tab>8<<tab>192.168.66.214<tab>8<tab>60<tab>WAN<tab>this-
device<tab>0<tab>0<tab>214-X506-
Dalhart<tab>ICMP<tab>firewall<tab>12<tab>><tab><tab>
<tab>1169221801013
```

The default settings are TAB for delimiter and Security/Authorization for facility.

## SMS Audit Syslog Format

Table 9 - 18: Remote Syslog Events Record Format (SMS Audit)

Column	Definition
0	user
1	Client Address
2	client Port
3	Session ID
4	Status
5	Description
6	Event timestamp in milliseconds

## SMS Audit Syslog Example

The following is an example of output for the log:

```
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.

## SMS System Syslog Format

Table 9 - 19: Remote Syslog Events Record Format (SMS System)

Column	Definition
0	Severity: <ul style="list-style-type: none"> <li>• 2 is Info</li> <li>• 3 is Warning</li> <li>• 4 is Error</li> <li>• 4 is Critical</li> </ul>
1	Message
2	Event timestamp in milliseconds

## SMS System Syslog Example

The following is an example of output for the log:

```
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.

## How To: Configure the Management Settings

1. From the **Admin** Navigation menu, select **Server Properties**.
2. Select the **Management** tab.
3. In the **System Information** section, do the following:
  - For the **Name**, enter the fully-qualified host name of the SMS server.
  - For the **Contact**, enter the name or e-mail address of the system administrator.
  - For the **Location**, enter the location of the server or administrator.
4. In the **Services** section, you can enable/disable services. If a check box is selected, the service is enabled. Select from the following services:
  - **SSH** — Network communication connection used for CLI. This connection is secure.
  - **SNMP** — Establishes read-only access to the system. You can restrict access with the **SNMP 'get' community name** field. The default name is "public."
  - **HTTPS** — Network communication connection for web pages. This connection is secure. Enabling this option enables web services. See *TippingPoint SMS Web Services API*.
  - **HTTP** — Network communication connection for web pages. This connection is unsecure.
  - **Telnet** — Network communication connection used for CLI. This connection is unsecure.



**Note** SMS Web Services is available for integrations. To implement these services, enable HTTP/HTTPS. For more information, see *TippingPoint SMS Web Services API*.

5. Click **Apply**.




**Note** You must click **Apply** to save changes for the management settings prior to modifying network information.

## How To: Create a new Remote Syslog for Events

1. From the **Admin** Navigation menu, select **Server Properties**.
2. Select the **Management** tab.
  - Click the **Add** button.
  - Enter the **IP address** and the **Port** number.
  - From the drop down menu, select one of the following log type formats:
    - SMS 2.0/2.1 Syslog Format
    - SMS 2.5 Syslog format
    - X-Family firewall block
    - X-Family firewall session
    - SMS System
    - SMS Audit
  - Select the **Facility: User Level, System Daemon, Security/Authorization, Log Audit, Log Alert**, or from **Local Use 0** through **Local Use 7**.
  - Select a **Delimiter: TAB, COMMA, SEMI-COLON, or PIPE**.
  - Optionally, select the desired header information.

3. Click **Save**.

 **Note** You can use the Remote Syslog for Events option for netForensics Integration.

 **Note** After configuring the Remote Syslog for Events, you can select the Remote Syslog option for action set contacts through the Profiles screen.

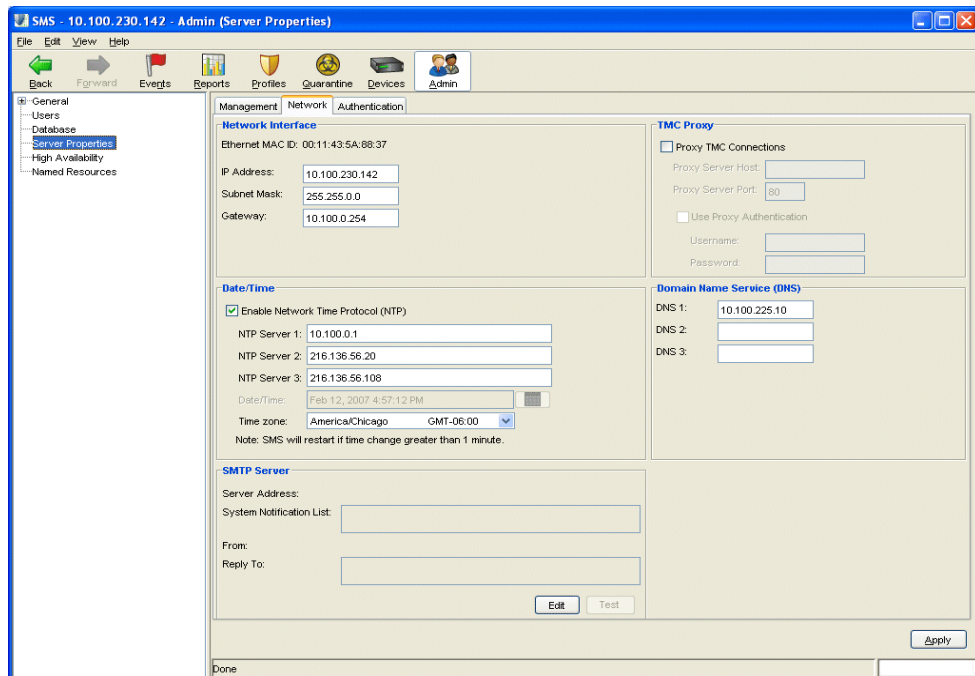
### How To: Edit a Remote Syslog for Events

1. From the **Admin** Navigation menu, select **Server Properties**.
2. Select the **Management** tab.
3. In the **Edit Syslog Notification Settings** dialog, make any needed changes.
4. Click **OK**.

## Network Information

The **Server Properties - Network** screen allows you to configure the network interface, date and time settings, SMTP server, TMC proxy, and the Domain Service (DNS):

Figure 9 - 12: Server Properties - Network Screen





The **Server Properties - Network** screen has the following settings:

**Table 9 - 20: Network Settings**

Setting	Description
Network Interface	Displays the Ethernet MAC address. Allows you to specify a static IP address, subnet mask, and default gateway settings for the server.
Date/Time	Allows you to set the server date and time either manually, or by using Network Time Protocol (NTP). You can also set the time zone.
SMTP Server	Allows you to enter the SMTP server information, including your mail server and accounts for sender and reply to. Configuring this setting sends information to the account, including Digital Vaccine downloads and distribution.
TMC Proxy	Allows you to enter the proxy server information for connecting to the Threat Management Center (TMC). This option also includes authentication for the proxy server.
Domain Name Service (DNS)	Allows you to define up to three Domain Name Service servers in this panel. DNS servers are optional.

### How To: Configure the Network Settings

1. From the **Admin** Navigation menu, select **Server Properties**.
2. Select the **Network** tab.
3. In the **Network Interface** section, do the following.
  - Enter the specific **IP Address**.
  - Enter the **Subnet Mask**.
  - Enter the **Default Gateway**.
4. In the **Date/Time** section, set the server date and time either manually, or by using Network Time Protocol (NTP). You can also set the time zone.

To define the time using the NTP servers:

- Select the **Enable Network Time Protocol (NTP)** check box.
- Type the server IP addresses in the **NTP Server 1**, **NTP Server 2**, and **NTP Server 3** fields as appropriate. You must specify at least one NTP server. You may define one or two additional NTP servers as backups.



**Note** The SMS can also provide time for your IPS devices. To keep IPS and SMS times consistent, TippingPoint recommends that you use NTP for the SMS and that you set the SMS server as the NTP server for your devices.

To define the time manually:

- Deselect the **Enable Network Time Protocol (NTP)** check box.
- Click on the calendar icon to the right of the **Date/Time** field. Use the calendar control to select a new time and date. If you need more information about the operation of the control, see [“Date and Time Controls” on page 37](#).




**CAUTION** Do not set the time backwards on the SMS server as it might cause inconsistencies in some system services which depend tightly on time.

To define the time zone, click the **Time zone** drop-down list and select the desired time zone.


5. In the **SMTP Server** section, click **Edit**.  
The **Edit SMTP Server Settings** window displays.  
Define the following fields:
  - **Server Address:** Enter the name of your e-mail server.  
For example: mail.your-domain.com.
  - **SMTP Port**
  - **System Notification List:** The SMS email notification sends messages for certain events. To enable this feature, you must configure the SMTP and add at least one email address to the System Notification List. The SMS sends emails for the following:
    - SMS HA fail-over and activation
    - SMS start and stop
    - Critical device failures (i.e. 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
  - **From:** Enter the sender e-mail address.
  - **Reply To:** Enter the e-mail address to which users will reply.
  - To enable authentication, select **Authentication**, and then enter the **Username** and **Password** of the person with the authority to authenticate.
  - Click **OK**.
6. In the **TMC Proxy** section, do the following to use a proxy server connection for the TMC:
  - Select the **Proxy TMC Connections** check box.
  - Enter the IP address for the **Proxy Server Host**.
  - Enter the port for the **Proxy Server Port**.
  - To enable proxy authentication, select **Use Proxy Authentication**, and then enter the Username and Password of the person with the authority to authenticate.
7. In the **Domain Name Service (DNS)** section, enter up to three DNS server IP addresses.

8. Click **Apply**.

 **Note** You must click **Apply** to save changes for the network information prior to modifying management settings.

## Authentication Information

The **Server Properties - Authentication** screen allows you to configure authentication services for users. The SMS provides ACL authentication for user accounts. The system also provides authentication support against a RADIUS server. The RADIUS server only supplies a password authentication, and thus (by implication) controls the enabled status of a user. Authorization is done via the local SMS configuration. User roles and ACLs must be set on the parallel local user account. The SMS Client continues to provide ACL support for defining the user's role. When using RADIUS servers, use account options for modifying passwords, password aging, and the enabled status are disabled.

 **Note** ANY SMS account with the Super User role can log into the SMS with local credentials if the RADIUS servers are unreachable or do not respond within their configured timeout value.

The SMS solely enables granting access to the profiles and/or segment groups. This functionality is not provided on the external RADIUS system.

The SMS provides configuration of two RADIUS servers. If the primary server does not respond within the specified number of time-out seconds, the SMS Client attempts to authenticate using the second RADIUS server (or the back-up server).


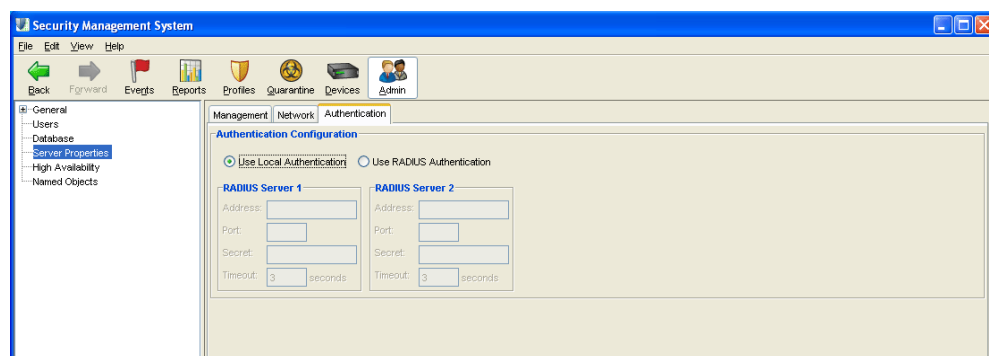
 **Note** Only the SMS provides access through the RADIUS server. Device access does not support using RADIUS.

Figure 9 - 13: Server Properties - Authentication Screen



The **Server Properties - Authentication** screen has the following settings:

**Table 9 - 21: Authentication Settings**

Setting	Description
Use Local Authentication	Sets the SMS to authenticate using ACL for authentication
Use RADIUS Authentication	Sets the configuration options for RADIUS servers for authentication

See also [“How To: Configure the Authentication Settings” on page 474](#).

### Creating Accounts

When creating a user account with RADIUS authentication, you should create the account on the RADIUS server. A parallel account having the same user name must be created on the SMS, with appropriate Role and Security permissions. RADIUS users who do not have a parallel SMS account cannot log in to the SMS.

When creating or editing an SMS user account with RADIUS authentication, the account password and enabled status cannot be modified. The RADIUS server manages and controls all user passwords and the account enabled status. If an SMS account does not have a password in RADIUS, the user will not be able to login.

If RADIUS authentication is disabled, all SMS accounts that existed before RADIUS was enabled become available for use with their previous passwords. Any accounts created while in RADIUS mode will be disabled with an unknown password. Such accounts must be explicitly enabled, and their passwords set to a known value, before those users can log in.

### How To: Configure the Authentication Settings

1. From the **Admin** Navigation menu, select **Server Properties**.
2. Select the **Authentication** tab.
3. In the **Authentication Configuration** section, select one of the following: **Use Local Authentication** or **Use RADIUS Authentication**. If you select RADIUS authentication, continue entering data in this section.
4. For the **RADIUS Server 1**, do the following:
  - Enter the RADIUS server address for the **Address**.
  - Enter the **Port** for the server. Ports for authentication and accounting differ (default: auth 1812, acct 1813).
  - Enter the **Secret** for the RADIUS server.
  - Enter the an amount of seconds for the **Timeout** setting.

5. For the **RADIUS Server 2**, do the following:
  - Enter the RADIUS server address for the **Address**.
  - Enter the **Port** for the server. Ports for authentication and accounting differ (default: auth 1812, acct 1813).
  - Enter the **Secret** for the RADIUS server.
  - Enter the an amount of seconds for the **Timeout** setting.
6. Click **Apply**.



**Note** You must click **Apply** to save changes for the network information prior to modifying management settings.

## High Availability

This sections contains the following topics:

- [HA Overview](#)
- [Configuring HA](#)
- [HA Configuration Option Examples](#)
- [Using HA](#)
- [Synchronization Timing](#)

High Availability (HA) provides continuous administration through an active-passive SMS system configuration using a secure network connection. If the active SMS incurs issues or interruptions in service, administration transfers to the passive SMS system.

The redundant (or passive) SMS is configured, synchronized with the active system, and then waits in a standby mode, monitoring the health of the active system. Should the health or communications check fail, this passive SMS will startup and attempt to take over the HA resources.

**IMPORTANT! Make sure your system meets TMC port requirements. See [“Port Information” on page 557](#).**

You can perform the following HA tasks:

- [“How To: Configure High Availability - Primary Only Option” on page 481](#)
- [“How To: Configure High Availability - Primary + Secondary Option” on page 482](#)
- [“How To: Manually Synchronize HA Systems” on page 484](#)
- [“How To: Disable High Availability” on page 484](#)

## HA Overview

In general, the SMS HA feature behaves the same regardless if you choose primary or primary + secondary. The only difference is how the HA specific synchronization data is communicated. For the primary + secondary option, HA specific synchronization data is sent to the peer on the secondary network interface.



**Note** Both SMS systems should use the same version of SMS software. If you add an additional SMS system, make sure to update the SMS software to match the primary system.

Any devices under control of the passive SMS should be removed or transferred to the active system before configuring SMS HA.

These options include two SMS systems deployed in an active/passive mode. Each of these SMS systems includes two network interface ports, a primary and a secondary, which you can select and configure using the SMS HA Configuration Wizard. Configuration options are available to allow the peers to be on different subnets. The primary SMS system is designated as *active*; the back-up system is designated as *passive*. After enabled, you must use the active system for all file updates (TOS, Digital Vaccine, SMS), profile maintenance, device management, reporting, configurations, and database maintenance. Through the **Admin - High Availability** screen, you can disable, configure, view status, and synchronize.

### HA Operations

- **Synchronization** — (manual process) initial operation to clone the active SMS data in order to enter into HA
- **Replication** — (automatic process) After HA setup and synchronization, data is automatically copied or replicated from the active SMS to the passive SMS.

When enabled, all system data is replicated to the peer system in real-time as changes and events occur on the active system.

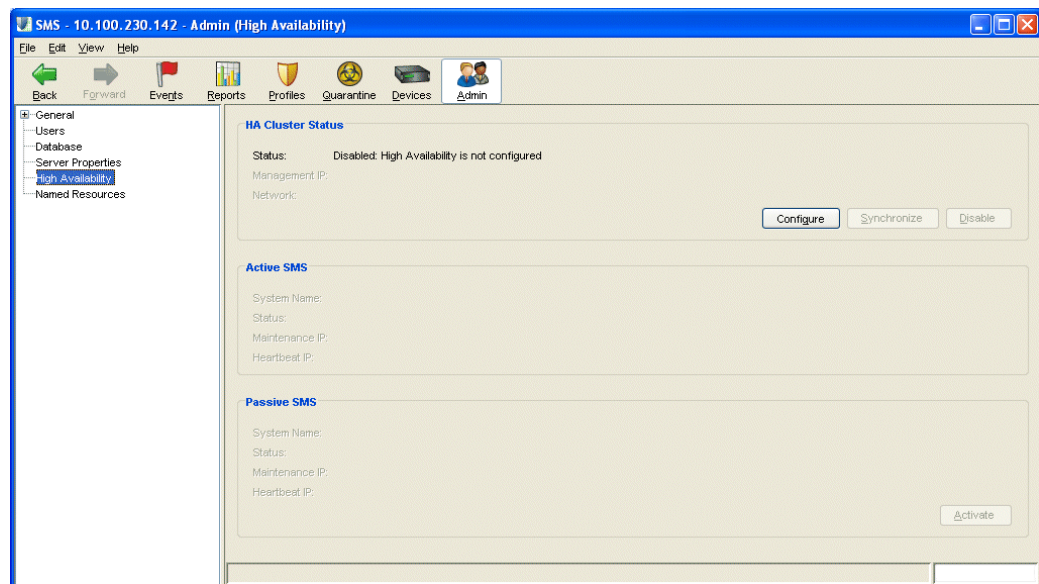
Both systems continually check the status of the other. When interruptions in service occur, the active system gracefully fails over to the passive, or back-up, system. When a failover occurs, the active SMS client connections lose connectivity with the SMS server. With the loss in connection, the SMS Client attempts to contact the peer system. Notifications of the failover are also sent through e-mail, providing further information for the cause of the failover. When the system re-connects to the now active SMS server, the SMS Client displays a notification explaining that a failover occurred.

Failures on the systems include failed synchronization processes, server hardware issues, hardware shutdown or rebooting, and interruptions with traffic and service.



**Note** During High Availability, the serial number of the secondary unit may match that of the primary unit in some places and is no cause for alarm. To assure seamless communication to TMC and any managed devices, the secondary/passive system temporarily assumes the serial number of the active system.

Figure 9 - 14: High Availability



The **High Availability** screen has the following settings:

Table 9 - 22: High Availability Settings

Setting	Description
HA Cluster Status	Details the status and management IP for High Availability. The section also provides functions for configuring HA, synchronizing the passive and active systems, and disabling HA.
Active SMS	Provides status and IP information for the active SMS system
Passive SMS	Provides status and IP information for the passive SMS system. You can activate the Passive SMS, placing the system into HA.

## Configuring HA

The SMS provides an SMS HA Wizard to configure an active/passive pair of SMS systems to form a High Availability cluster. The High Availability SMS configuration includes two SMS servers that can optionally share a virtual IP address and their own unique configuration/service address. The two units can directly connect using the servers' secondary NIC to exchange heartbeat and data synchronization information. If a heartbeat cable is not used, the SMS servers exchange data across their normal management connections.

SMS also supports deployments with active and passive systems in separate networks for data replication and heartbeat status on the secondary interface. You need gateway routing and configuration information from you network administrator to complete SMS HA configuration.

To further improve the SMS system tolerance for hardware faults, optional capabilities for redundant hardware configurations can be utilized. This includes the presence of dual power supplies and the configuration of a RAID 1 storage array. For more information, contact your TippingPoint representative.



**Note** Any devices under control of the passive SMS should be removed or transferred to the active system before configuring SMS HA.

## HA Configuration Wizard

The HA Configuration Wizard provides a convenient method for setting up active and passive SMS devices. You can select from the following basic HA configuration options:

- [Primary Option Only](#) — Primary management interface is used for all HA communication purposes, including heartbeat and data replication. For this option, all data is sent using the primary network interface port.
- [Primary and Secondary Option](#) — The secondary network interface is used for all HA communication purposes, including heartbeat and data replication. When selecting this option, you must configure the second interface port during the installation wizard. For this option, all data required for synchronizing the SMS passes over the secondary port.

You also have the option to assign a virtual IP Address for the HA cluster when the primary network interface IP Addresses are in the same subnets.

See also [“HA Configuration Option Examples” on page 479](#)

### **Primary Option Only**

Use this option when:

- Direct heartbeat cable cannot be used because the SMS HA systems are located in different physical locations
- Dedicated HA network is not available

Before configuring HA for the **Primary Option Only**, gather the following information:

- *Available network IP address to use for the Virtual HA Cluster, optional*
- *IP address, username and password for the passive SMS*

See [“How To: Configure High Availability - Primary Only Option” on page 481](#)

### **Primary and Secondary Option**

Use this option when both SMS HA systems are located in close proximity. Before configuring HA for the **Primary and Secondary Option**, gather the following information:

- *Secondary IP address for the active and passive SMS*
- *Heartbeat cable, optional depending upon setup*
- *Gateway address, optional depending upon setup*

See [“How To: Configure High Availability - Primary + Secondary Option” on page 482](#)



## HA Configuration Option Examples

- [HA Example - Primary Only Option \(same subnet\)](#)
- [HA Example - Primary + Secondary Option \(same subnet\)](#)

Figure 9 - 15: HA Example - Primary Only Option (same subnet)

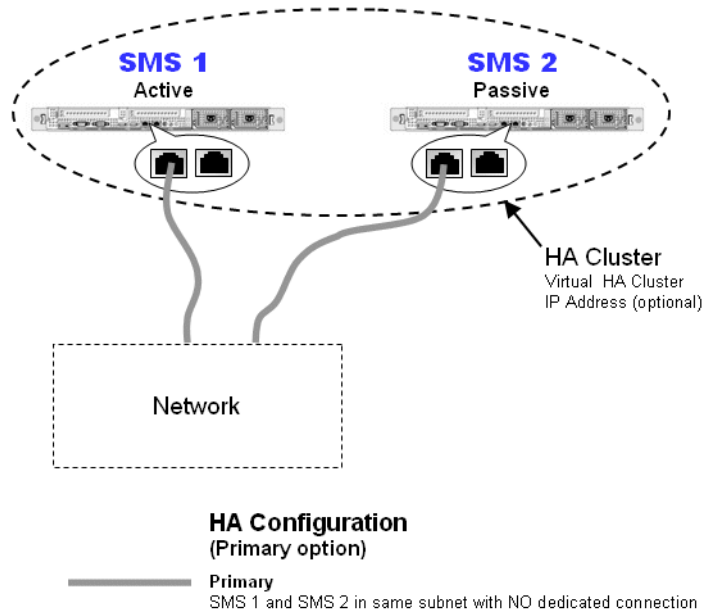
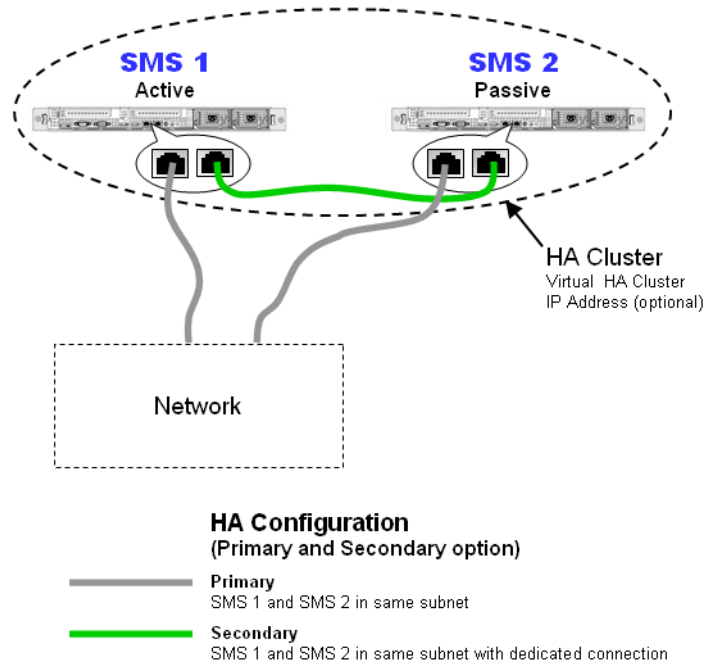


Figure 9 - 16: HA Example - Primary + Secondary Option (same subnet)



**Note** SMS also supports deployments with active and passive systems in separate networks for data replication and heartbeat status on the secondary interface. You need gateway routing and configuration information from your network administrator to complete SMS HA configuration.

## Synchronization Process

After configuring the HA active and passive SMS HA systems, you should manually synchronize the data. The first time you set up an HA cluster, you must synchronize the SMS systems for the HA functionality to run properly. For subsequent synchronizations, you can reduce synchronization time by choosing to exclude event data. The duration of this operation depends on the size of the SMS database, if event data is included, and the network link between the two SMS systems.

When you exclude events, data is not as granular as it is when you include the existing data. Because the replication process runs automatically, all new events will appear on both the active and passive system.



**Note** Synchronization replaces all data on the peer system and restarts the active system. The duration of this operation depends on the size of the SMS database, if event data is included, and the network link between the two SMS systems.

**IMPORTANT! When you perform HA Synchronization, the database of the passive SMS will be overwritten.** The overwritten settings include user accounts, filters, action sets, and further configuration settings. Information from the passive system is not transferred to the active SMS from the passive.

### How To: Configure High Availability - Primary Only Option

Use this option if your active and passive SMS device are in the same network and do NOT have a dedicated connection. See Figure 9 - 15, “HA Example - Primary Only Option (same subnet),” on page 479.

Before you set up an HA cluster using the HA Primary, you must configure the passive SMS using the Setup wizard through the OBE setup or using the SMS CLI `setup` command and gather the following information about your network:

- Available network IP address to use for the Virtual HA Cluster, optional
  - IP address, username and password for the passive SMS
1. Log on to the active SMS.
  2. From the **Admin** Navigation menu on the active SMS, select **High Availability**.
  3. In the **HA Cluster Status** section, click **Configure**.
  4. After the **SMS HA Wizard** opens, follow the instructions and click **Next**.
  5. When the **Network Configuration** screen displays, select **Primary Only** and click **Next**.
  6. The **Primary Network Interface Configuration** screen displays.
    - If you want to manage the cluster using a virtual management IP address:
      - Select the **Use Shared Virtual Management IP** check box.
      - In the **Management IP** field, enter an IP address on the same subnet as the SMS.
    - In the **Passive System** section, enter the IP address for the passive SMS.
    - Click **Next**.
  7. The **Passive SMS Login** screen displays.
    - Enter a **Username** and **Password** for the login account of the passive SMS system.
    - Click **Configure**.
  8. The configuration begins, displaying a **Configuration Status** screen.
  9. When the process completes, the Wizard prompts you to synchronize the systems. The first time you set up an HA cluster, you must synchronize the SMS systems for the HA functionality to run properly. To synchronize, click **Yes**.

For subsequent synchronizations, you can reduce synchronization time by choosing to exclude event data. Even if you exclude the event data from synchronization, future events are replicated.



**Note** Synchronization replaces all data on the peer system and restarts the active system. The duration of this operation depends on the size of the SMS database, if event data is included, and the network link between the two SMS systems.

For information on synchronization and replication, see [“HA Operations” on page 476](#).

**IMPORTANT! When you perform HA Synchronization, the database of the passive SMS will be overwritten.** The overwritten settings include user accounts, filters, action sets, and further configuration settings. Information from the passive system is not transferred to the active SMS from the passive.

When synchronization begins, the following occurs:

- Main client window closes.
- **Synchronization Status** Dialog displays the status of the synchronization.



**CAUTION** If you cancel synchronization before the process is complete, the passive SMS resets to the factory settings and you may lose important data. The active SMS retains all settings.

After the synchronization is completed, the:

- Client reconnects to the active SMS.
- High Availability screen displays updated information for the passive and active systems.

### How To: Configure High Availability - Primary + Secondary Option

Use this option if your active and passive SMS devices are configured for the heartbeat and replications services, have a dedicated connection and are in the same subnet. See Figure 9 - 16, “HA Example - Primary + Secondary Option (same subnet),” on page 480.

Before you set up an HA cluster using the HA Primary + Secondary option, you must configure the passive SMS using the Setup wizard through the OBE setup or using the SMS CLI `setup` command and gather the following information about your network:

- Available network IP address to use for the Virtual HA Cluster, optional
- IP address, username and password for the passive SMS
- Secondary IP address for the active and passive SMS
- Heartbeat cable, optional depending upon setup
- Gateway address, optional depending upon setup

1. Log on to the active SMS.
2. From the **Admin** Navigation menu on the active SMS, select **High Availability**.
3. In the **HA Cluster Status** section, click **Configure**.
4. After the **SMS HA Wizard** opens, follow the instructions and click **Next**.

5. When the **Network Configuration** screen displays, select **Primary and Secondary** and click **Next**.
6. The **Primary Network Interface Configuration** screen displays.
  - If you want to manage the cluster using a virtual management IP address:
    - Select the **Use Shared Virtual Management IP** check box.
    - In the **Management IP** field, enter an IP address on the same subnet as the SMS.
  - In the **Passive System** section, enter the IP address for the passive SMS.
  - Click **Next**.
7. The **Secondary Network Interface Configuration** screen displays.
  - Select **Require secondary network interfaces to share the same subnet** checkbox.



**Note** SMS also supports deployments with active and passive systems in separate networks for data replication and heartbeat status on the secondary interface. You need gateway routing and configuration information from you network administrator to complete SMS HA configuration.

- In the **Active System** section, enter the **Secondary IP** address.
  - In the **Passive System** section, enter the **Secondary IP** address.
  - Click **Next**.
8. The **Passive SMS Login** screen displays.
    - Enter a **Username** and **Password** for the login account of the passive SMS system.
    - Click **Configure**.
  9. The configuration begins, displaying a **Configuration Status** screen.
  10. When the process completes, the Wizard prompts you to synchronize the systems. The first time you set up an HA cluster, you must synchronize the SMS systems for the HA functionality to run properly. To synchronize, click **Yes**.

For subsequent synchronizations, you can reduce synchronization time by choosing to exclude event data. Even if you exclude the event data from synchronization, future events are replicated.



**Note** Synchronization replaces all data on the peer system and restarts the active system. The duration of this operation depends on the size of the SMS database, if event data is included, and the network link between the two SMS systems.

For information on synchronization and replication, see [“HA Operations” on page 476](#).

**IMPORTANT! When you perform HA Synchronization, the database of the passive SMS will be overwritten.** The overwritten settings include user accounts, filters, action sets, and further configuration settings. Information from the passive system is not transferred to the active SMS from the passive.

When synchronization begins, the following occurs:

- Main client window closes.
- **Synchronization Status** Dialog displays the status of the synchronization.



**CAUTION** If you cancel synchronization before the process is complete, the passive SMS resets to the factory settings and you may lose important data. The active SMS retains all settings.

After the synchronization is completed, the:

- Client reconnects to the active SMS.
- High Availability screen displays updated information for the passive and active systems.

### How To: Manually Synchronize HA Systems

1. From the **Admin** Navigation menu, select **High Availability**.
2. In the **HA Cluster** section, click **Synchronize**. You can reduce synchronization time by choosing to exclude event data. Even if you exclude the event data from synchronization, future events are replicated.



**Note** Synchronization replaces all data on the peer system and restarts the active system. The duration of this operation depends on the size of the SMS database, if event data is included, and the network link between the two SMS systems.

### How To: Disable High Availability

1. From the **Admin** Navigation menu, select **High Availability**.
2. In the **HA Cluster** section, click **Disable**. The SMS disables High Availability.
3. The system prompts you with a message to disable the systems.



**Note** If you want to enable HA, you must perform a configuration again.

**IMPORTANT!** After disabling the HA cluster, you will have two identical SMS servers. For the unneeded SMS, TippingPoint recommends that you power off the system or perform a factory reset.

## Using HA

This section contains the following topics:

- [Restricted Management IP Address](#)
- [Timezone Date](#)
- [Shutdown](#)

### Restricted Management IP Address

When using SMS HA, you cannot configure managed devices with a restricted management IP Address. Failover addresses are treated as an SMS IP address change on the managed device, even if you are using a virtual IP Address.

### Timezone Date

The timezone date is not synchronized between the SMS HA systems. This behavior allows for SMS HA systems to be geographically split.

### Shutdown

When you power up an SMS HA cluster after a shutdown operation, the systems will wait up to five minutes to re-establish communications. If this time is exceeded, an HA failover may occur and synchronization may be required. To prevent failover, TippingPoint recommends that you power on both systems simultaneously.

## Synchronization Timing

The following table represents the SMS HA synchronization timing results:

Table 9 - 23: Synchronization Timing Results

Connection	Sync Time	Eff. Transfer Rate	Size of Data
<b>Large SMS Database: Full synchronization</b>			
Direct	20.24	59.7 Mbps	9,136.0 MB
WAN	2:22.48	8.5 Mbps	9,136.0 MB
WAN (w/traffic)	14:28.10	1.4 Mbps	9,136.0 MB
<b>Large SMS Database: Partial synchronization (excludes event data)</b>			
Direct	3.56	7.6 Mbps	171.9 MB
WAN Link	21.22	1.1 Mbps	171.9 MB
<b>Minimal SMS Database: Full synchronization</b>			
Direct	4.16	3.2 Mbps	102.4 MB
WAN Link	7.17	1.9 Mbps	102.4 MB
<b>Minimal SMS Database: Partial synchronization (excludes event data)</b>			
Direct	3.25	n/a*	1.9 MB
WAN Link	4.22	n/a*	1.9 MB

\* This rate is not directly measured because the majority of the synchronization time is spent restoring database content rather than transferring file data.

### Definitions

- **Large SMS Database** — A large number of events (approximately 23 million) and 6 devices managed, 5 TOS images and 20 DV images. This is not the largest SMS database possible, but represents a reasonably loaded SMS file system.
- **Minimal SMS Database** — The smallest data set an SMS can have (immediately after a factory install). No managed devices or event data is present on the SMS. This data size represent the shortest synchronization duration possible for a given connection type.
- **Direct Connection** — The secondary network interface was used to transfer HA data. A crossover cable was connected directly between the two systems.
- **WAN Connection** — Only a primary network interface (no heartbeat network) is configured, the link was an IPSEC tunneled T1 (1.5Mbps). Average latency for this connection was approximately



75ms. The synchronization process had exclusive access to the bandwidth on this link, except where noted.

- **Sync Time** — The duration (in H:M:S) starting when the synchronization task was initiated, until the SMS HA cluster was available for login.
- **Eff. Transfer Rate** — This is the effective transfer rate. This means both synchronization optimizations (compression) and overhead (restarting services, building the set of data to transfer and other administrative tasks) are included in the measured time period. This value may actually appear faster than possible with a given link speed because of these optimizations, or slower due to synchronization overhead.



**Note** These measurements present an example for comparison of various synchronization methods. Actual results will depend on the specific SMS hardware configuration, network speeds and the exact data set on the SMS (which may include IPS events, stats, devices, TOS and DV images).

## Named Resources

This section contains the following items:

- [“Named IP Addresses” on page 488](#)
- [“Named VLAN IDs” on page 489](#)
- [“Named Email Addresses” on page 489](#)

Provides options for setting up a named entity or a group of named IP Addresses, VLAN IDs, and Email Addresses so that the named resources can be used with various SMS features.

For information on locked resources, see the following table.

**Table 9 - 24: Lock Resources**

Locked Resource	Description	User Capabilities
Anonymous resources	created automatically from user input and used for auto complete	Edit - No Delete - Yes
Internal resources	created by the SMS and not the user	Edit - No Delete - No

You can do the following tasks:

- [“Create/Edit a Named IP Address” on page 488](#)
- [“Create/Edit a Named Group of IP Addresses” on page 488](#)
- [“Create/Edit a Named VLAN ID” on page 489](#)
- [“Create/Edit a Named Group of VLAN IDs” on page 489](#)
- [“Create/Edit a Named Email Address” on page 489](#)
- [“Create/Edit a Named Group of Email Addresses” on page 490](#)

## Named IP Addresses

### How To: Create/Edit a Named IP Address

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named IP Addresses** tab.
3. From the **Named IP Addresses** section, click **New** to create a new Named IP address or select an entry from the **Named IP Addresses** list and click **Edit**.
4. In the **Named IP Address** dialog, specify a name.
5. In the **IP Address** section, select IP Host, IP Subnet or IP Range and specify the entry.
6. Click **OK** to add the named Address to the list.

### How To: Create/Edit a Named Group of IP Addresses

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named IP Addresses** tab.
3. From the **Named IP Address Groups** section, click **New** to create a new group or select an entry from the group list and click **Edit**.
4. In the **Named IP Address Group** dialog, specify a name for the group.
5. Click **Add**. The **Add Named IP Address** dialog displays.
6. To add an existing named IP address or addresses to your new group, choose an entry from the list. If you want to edit an existing named address, select an entry and click **Edit**.
7. If you want to create a new named address, click **New**. In the **Named IP Address** dialog, enter a name, select IP Host, IP Subnet or IP Range, specify the entry, and click **OK**.
8. Repeat the steps for adding named IP addresses until you have all that you need.
9. In the **Add Named IP Address** dialog, click **OK**

## Named VLAN IDs

### How To: Create/Edit a Named VLAN ID

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named VLAN IDs** tab.
3. From the **Named VLAN IDs** section, click **New** to create a new Named IP address or select an entry from the **Named VLAN IDs** list and click **Edit**.
4. In the **Named VLAN ID** dialog, specify a name.
5. In the **Named VLAN ID** section, select VLAN ID or VLAN ID Range, specify the appropriate entry or entries.
6. Click **OK** to add the named VLAN ID to the list.

### How To: Create/Edit a Named Group of VLAN IDs

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named VLAN IDs** tab.
3. From the **Named VLAN Groups** section, click **New** to create a new group or select an entry from the group list and click **Edit**.
4. In the **Named VLAN Group** dialog, specify a name for the group.
5. Click **Add**. The **Add Named VLAN ID** dialog displays.
6. To add an existing named VLAN ID or IDs to your new group, choose an entry from the list. If you want to edit an existing named VLAN ID, select an entry and click **Edit**.
7. If you want to create a new named VLAN ID, click **New**. In the **Named VLAN ID** dialog, enter a name, select VLAN ID or VLAN ID Range, specify the appropriate entry or entries, and click **OK**.
8. Repeat the steps for adding named VLAN IDs until you have all that you need.
9. In the **Add Named VLAN ID** dialog, click **OK**.

## Named Email Addresses

### How To: Create/Edit a Named Email Address

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named Email Addresses** tab.
3. From the **Named Email Addresses** section, click **New** to create a new named email address or select an entry from the **Named Email Addresses** list and click **Edit**.
4. In the **Named Email Address** dialog, specify a name.
5. In the **Email Address** section, specify an email address.
6. Click **OK** to add the named email address to the list.

### How To: Create/Edit a Named Group of Email Addresses

1. From the **Admin** Navigation menu, select **Named Resources**.
2. Select the **Named Email Addresses** tab.
3. From the **Named Email Address Groups** section, click **New** to create a new group or select an entry from the group list and click **Edit**.
4. In the **Named Email Address Group** dialog, specify a name for the group.
5. Click **Add**. The **Add Named Email Address** dialog displays.
6. To add an existing named email address or addresses to your new group, choose an entry from the list.
  - If you want to edit an existing named address, select an entry and click **Edit**.
  - If you want to create a new named address, click **New**. In the **Named Email Address** dialog, specify an email address, and click **OK**.
7. Repeat the steps for adding named email addresses until you have all that you need.
8. In the **Add Named Email Address** dialog, click **OK**

# A CLI Reference

*The command line interface (CLI) can be used to configure many aspects of the SMS. It includes wizards, high level commands, and low level commands.*

## Overview

The CLI Reference explains how to use the SMS CLI. It also provides reference information about each command.



**Note** To use the SMS CLI, you must be logged in as **SuperUser**.

This section includes the following topics:

- [“Usage” on page 492](#)
- [“The help Command” on page 495](#)
- [“Command Reference” on page 496](#)
- [“Attribs and Objects” on page 512](#)
- [“Object Reference” on page 513](#)

# Usage

Most SMS commands consist of the following elements:

- command** the name of the command you want to issue
- object** the name of a collection of related attributes (*attrs*)
- attrib** the name of a data variable or parameter on which you want to run the command
- [=value]** optional syntax you can use with the **set** command and other writable commands to define the value of the attrib you specify. If you do not use this syntax, the system goes into **interactive mode** and prompts you for the value. See [“Command Types” on page 492](#) for more information about interactive commands.



**Note** To clear the value of any attrib, type a period (.) after the equal sign (=) or when prompted.

These elements are case-sensitive. You can use any of the following syntax to run an SMS command:

```
command
command object
command object.attrib
command object.attrib=value
```

Other SMS commands use a syntax similar to standard UNIX commands, as shown in the following example:

```
command -option value
```

## Command Types

SMS commands are either read, write, or read and write. In addition, commands are either interactive, non-interactive, or might support both options. *Interactive* commands automatically prompt you for attrib values if you use the appropriate syntax. Interactive commands also provide you with the current values of their attrs.

*Non-interactive* commands are either read-only or require you to specify the values you want to set. For example, the **get** command is non-interactive because it is read-only. As another example, the **date** command is non-interactive. If you want to set the date, you must type `date value`.

## Interactive Mode Syntax

You can use any of the following syntax options to initiate an interactive CLI command:

- *command*  
If you type the command name, the CLI prompts you to set values for all attrs associated with that command.
- *command object*  
If you specify the object of a particular command, the CLI prompts you to set values for all attrs associated with that object.
- *command object.attrib*

If you specify an object and attrib of a particular command, the CLI prompts you to set the value of the attrib you specified.

## Example

Following is an example of the **set** command in interactive mode. Items in bold are typed by the user. Items in brackets ([ ]) indicate the current value of the attrib specified.

### Set All System Information Using Interactive Mode

- 1 Type the following command:

```
set sys
```

The system returns prompts for information. Default values are listed in brackets. To use the default value, press Enter.

- 2 The system prompts you to set the value for the **contact** attrib:

```
System contact (sys.contact=[Customer Contact]) = Brit
```

- 3 Type a value for the **location** attrib and press Enter:

```
System location (sys.location=[First floor lab]) =
```

- 4 Type a value for name attribute and press Enter:

```
System name (sys.name=[sms25]) =
```

- 5 The system returns the following confirmation message:

```
Result: Success
```

```
System contact      (sys.contact  ) = Brit
System location     (sys.location ) = First floor lab
System name         (sys.name      ) = sms25
System serial number (sys.serialNum) = X-SMA-ST-SMS25-0001
```

## Remote Paths

Several commands accept remote paths as input. The remote paths specify a resource on an external server that can be accessed by the SMS server. Remote files that can be specified as input to an operation may be accessed using the HTTP, HTTPS, FTP, NFS, or SMB (Samba) protocols.

Remote directories that are used for saving SMS-based files to a remote server can be accessed through the NFS or SMB protocols. Files are always mounted with read-only access. Directories are mounted read-only when possible.

Remote paths are specified as a single string value. The details for each protocol are listed in the following sections. In each example, items in italics are variables. When using the path syntax, you must replace them with the appropriate values for your paths. Items in brackets ([ ]) are optional.

## FTP

You can use the following formats for the FTP protocol:

- Complete specification—`ftp://[username:password@]server[:port]/directory/filename`
- Anonymous FTP—`ftp://server/directory/filename`
- Specifying a user name and password—`ftp://username:password@server/directory/filename`
- FTP Examples:

```
ftp://10.11.12.13/pub/sms-0.0-0.500.pkg
ftp://steve:password@10.11.12.13/pub/sms-0.0-0.500.pkg
```

## HTTP and HTTPS

You can use the following format for the HTTP and HTTPS protocols:

- Complete specification—`http://[username:password@]server[:port]/directory/filename` or `https://[username:password@]server[:port]/directory/filename`
- HTTP Example:

```
http://www.servername.com:8000/files/sms-0.0-0.500.pkg
```

## NFS

You can use the following formats for the NFS protocol:

- Remote directory specification—`server:/exportedDirectory`
- Remote file specification—`server:/exportedDirectory/filename`
- NFS Example:

```
nfsserver.domain.com:/public/upgrades/sms-0.0-0.500.pkg
```

## SMB (Samba)

You can use the following formats for the SMB protocol:

- Remote file specification—`//server/sharename/directory/filename`
- Complete specification—`//server/sharename[/directory][/filename] [-o option-list]`

Options can be provided to the SMB mount operation by appending them to the end of the mount point value, and using a space character to separate the values. Options might include the username, password, and workgroup. Options can be joined together using a comma as a separator.

- SMB Example:

```
//winbox/pub/sms.pkg -o workgroup=mydomn,username=steve,password=ps111
```



# The help Command

The **help** command returns documentation about the specified command, object, or attribute.

## Syntax

```

help
help --full
help --attrs
help object.attr
help --cmds
help cmd
help --objs
help object
help --background
help background
help --topic
help topic

```



**Note** In the **help** command syntax, you can use the question mark (?) interchangeably with the word “help.” For example, you could type the following to view documentation about all commands:

```
? --cmds
```

## Description

The **help** command is a non-interactive, read command that returns documentation about a command, object, or attribute that you specify.

## Objects and Attributes

The following objects and attributes can be used with the **help** command:

Table A - 1: Help Commands

Command	Description
<code>help --full</code>	Lists all commands, objects, and attributes
<code>help -- attrs</code>	Lists all attributes
<code>help --objs</code>	Lists all objects, or collections of attributes
<code>help --cmds</code>	Lists all commands
<code>help --background</code>	Lists background topics

## Example

To see documentation about the **sys** object, type **help sys**. The system returns the following results:

```

sys: System information
System information can be viewed and updates using the "sys"
object.

Read-write:
name, contact, location

Read-only:
serialNum

```

# Command Reference

The following table lists each command available in the SMS CLI. See the sections that follow for more detailed information about each command.

Table A - 2: SMS Commands

Command	Type	Page
<a href="#">clear</a>	non-interactive, read/write	page 498
<a href="#">cls</a>	non-interactive, read/write	page 498
<a href="#">console</a>	non-interactive, read	page 498
<a href="#">date</a>	non-interactive, read/write	page 498
<a href="#">delete</a>	non-interactive, read/write	page 498
<a href="#">diags</a>	non-interactive, read	page 499
<a href="#">dir</a>	non-interactive, read	page 499
<a href="#">dns</a>	interactive, write	page 499
<a href="#">exit</a>	non-interactive, write	page 499
<a href="#">ftp</a>	non-interactive, write	page 499
<a href="#">get</a>	non- interactive, read	page 500
<a href="#">help</a>	non- interactive, read	page 500
<a href="#">ifconfig</a>	non-interactive, read	page 501
<a href="#">ipconfig</a>	non-interactive, read	page 501
<a href="#">kbdcfg</a>	interactive, write	page 501
<a href="#">key</a>	non-interactive, read/write	page 501
<a href="#">list</a>	non-interactive, read	page 502
<a href="#">monitor</a>	non-interactive, read/write	page 502

Table A - 2: SMS Commands

Command	Type	Page
<a href="#">more</a>	interactive, read	page 502
<a href="#">nic</a>	interactive, read/write	page 502
<a href="#">notify</a>	interactive, read/write	page 503
<a href="#">ntp</a>	interactive, read/write	page 503
<a href="#">getpasswd</a>	non-interactive, read	page 503
<a href="#">quit</a>	non-interactive, write	page 504
<a href="#">reboot</a>	non-interactive, write	page 505
<a href="#">recover</a>	interactive, write	page 505
<a href="#">resolve</a>	non-interactive, read	page 505
<a href="#">restart</a>	non-interactive, write	page 505
<a href="#">reverse</a>	non-interactive, write	page 505
<a href="#">scp</a>	non-interactive, write	page 506
<a href="#">set</a>	interactive/non-interactive, write	page 506
<a href="#">setup</a>	interactive, write	page 507
<a href="#">shutdown</a>	non-interactive, write	page 507
<a href="#">snmp</a>	interactive, write	page 507
<a href="#">snmpget</a>	non-interactive, write	page 507
<a href="#">snmpwalk</a>	non-interactive, read/write	page 508
<a href="#">time</a>	non-interactive, read	page 508
<a href="#">tmc</a>	interactive, read/write	page 508
<a href="#">traceroute</a>	non-interactive, read	page 508
<a href="#">update</a>	interactive, write	page 510
<a href="#">users</a>	interactive, write	page 510
<a href="#">version</a>	non-interactive, read	page 510
<a href="#">vi</a>	non-interactive, read	page 510
<a href="#">view</a>	non-interactive, read/write	page 511
<a href="#">web</a>	interactive, read/write	page 511
<a href="#">who</a>	non-interactive, read	page 512

## clear

Clears the screen.

### Usage

clear

### Aliases

cls

## cls

Clears the screen.

### Usage

cls

### Aliases

clear

## console

The **console** command shows a list of messages that have been sent to the console since the last reboot.

### Usage

console

## date

Displays and sets the system time. Without a parameter, **date** will return the current system date and time. The parameter allows a new date to be specified.

### Usage

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

### Related Objects

time

## delete

Deletes user files. User files are archived and exported files generated from the database contents.

### Usage

delete *file* [...]

### Related Commands

dir, view, vi

## diags

Runs diagnostic tests and checks system health.

### Usage

health (*object*)

## dir

Returns a listing of files contained in the user directory.

### Usage

dir

### Related Commands

delete, view, vi

## dns

The **dns** command interactively prompts for DNS (Domain Name Service) settings used to resolve host names to IP address values. To clear server values, use a period (.). The *dns* object contains default domain name, DNS search list, and DNS server information.

### Usage

dns

### Related Commands

nic, ntp

### Related Objects

dns

## exit

Closes the session.

### Usage

exit

### Aliases

quit, Ctrl-D

## ftp

The FTP (File Transfer Protocol) client is used to move files to and from the SMS server's user directory. The contents of the user directory can be listed with the **dir** command. Files can be viewed with the **view** command, and deleted with the **delete** command.

## Usage

```
ftp [hostName|hostAddress]
```

After starting the ftp client, issue the command **cd /tmp**.

## Caveats

The **dir/delete/view** commands all operate over the contents of the user directory (**/tmp**). The **cd** or change-directory command is disabled from the shell for reasons of security. In order for the **ftp** program to see, and have access to the contents of the user directory, it is important to first change the local directory with the command **lcd /tmp**. After this point, files can be copied both to and from the SMS server.

## Related Commands

dir, view, delete, vi

# get

Retrieves the value of one or more attribs or a list of attribs contained within an object.

## Usage

```
get <attrib|object> [...]
```

The **get** command can use any read-write or read-only attrib. See [“Attribs and Objects” on page 512](#) for a list of attribs.

## Related Commands

list, set

# help

Returns background information on various topics and command syntax.

## Usage

```
help [--full | --attribs | --cmds | --objs | --background | topic]
```

## Alias

?

## Options

<b>--full</b>	lists all commands, objects and attribs
<b>--attribs</b>	lists all attribs
<b>--objs</b>	lists all objects (collections of attribs)
<b>--cmds</b>	lists all commands (default)
<b>--background</b>	lists background topics

## ifconfig

Displays the network settings for the box. **ifconfig** is an alias for the command **get net**, which displays the values of the attribs contained in the net object. To change the values, use the **set net** command. See [“Network Changes” on page 506](#).

### Usage

ifconfig

### Aliases

get net, ipconfig

### Related Objects

net

## ipconfig

Displays the network settings for the box. **ipconfig** is an alias for the command **get net**, which displays the values of the attribs contained in the net object. To change the values, use the **set net** command. See [“Network Changes” on page 506](#).

### Usage

ipconfig

### Aliases

get net, ifconfig

### Related Objects

net

## kbdcfg

Loads the kernel keymap for the console. This is useful if the console is using a non-QWERTY keyboard. This command leads you through the configuration of a new keyboard layout.



**WARNING:** Do not use this option if you are using a standard QWERTY keyboard. Setting your keyboard layout to a value with which you are not familiar could render your system inaccessible.

### See also

kbd.layout (attrib)

## key

The **key** command is used to update the license key for the server.

### Usage

key

### Aliases

license

### Related Objects

license

## list

Lists the objects or the attribs contained in an object.

### Usage

list [*object* | *object.attrib*] [...]

If no arguments are specified, **list** will return all defined objects. If an object is specified, **list** will return all attribs contained within the object. If an attrib is specified, **list** will confirm the attrib by listing the attrib in the response.

### Related Objects

See [“Attribs and Objects” on page 512](#) for a list of objects and attribs you can use with the **list** command.

### See Also

get, set

## monitor

Shows utilization and uptime information every 5 seconds (by default).

### Usage

monitor [*delay*]

where *delay* is the number of seconds between polls.

### Related Objects

health

## more

Command to list output one screen at a time.

## nic

Ethernet 10/100Mbps interface management. Interactively prompts for configuration of the SMS server network settings. The bottom-most (NIC1) is enabled by default and is the recommended connection to the management network.

### Usage

nic



**Related Commands**

dns, ntp

## notify

The **notify** command is used to manage the SMS notification service. The command interactively prompts for SMTP e-mail addresses and SNMPv1 traps to a remote trap server.

**Usage**

notify

**Related Objects**

smtp, snmp

**Related Commands**

snmp

## ntp

The **ntp** command is used to manage the NTP (Network Time Protocol) client that synchronizes the SMS server time with a list of specified servers. NTP is enabled by default and is configured with a list of Stratum 1 servers available on the internet. The list of servers can be customized to installation requirements. The SMS server can also act as a NTP server for your devices. The agent can be disabled, but the server cannot. To clear server values, use a period (.).

**Usage**

ntp

**Related Objects**

svc

**Related Commands**

snmp

## getpasswd

Changes the password for the current user.

The security level and restrictions for entering user names and passwords. The default setting is 2 from the following options:

**Table A - 3: Security Levels**

Level	Description
Level 0	User names cannot have spaces in it. Passwords are unrestricted.
Level 1	User names must be at least 6 characters long without spaces. Passwords must be at least 8.

Table A - 3: Security Levels

Level	Description
Level 2	Includes Level 1 restrictions and requires the following: <ul style="list-style-type: none"> <li>• 2 alphabetic characters</li> <li>• 1 numeric character,</li> <li>• 1 non-alphanumeric character (special characters such as ! ? and *)</li> </ul>

### Usage

getpasswd

## ping

**ping** checks network connectivity by sending a ICMP request to the specified destination, and then checking on an echoed response.

### Usage

ping [-options] *hostNameOrAddress*

### Options

**-c count** Stop after sending *count* packets.

**-i wait** Wait *wait* seconds between sending each packet. The default is to wait for one second between each packet.

**-n** Numeric output only. No attempt will be made to lookup symbolic names for host addresses.

**-q** Quiet output. Nothing is displayed except the summary lines at startup time and when finished.

**-r** Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.

**-s packetsize** Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

**-v** Verbose output

## quit

Closes the session.

### Usage

quit

### Aliases

exit

Ctrl-D

## reboot

Reboot the system. The **--force** option will reboot the system without prompting for confirmation. The cancel options aborts an in-progress reboot.

### Usage

```
reboot [--force] [cancel]
```

## recover

Database recovery operation. The **recover** command verifies the SMS database and suggests actions to restore the database back to health.

### Usage

```
recover
```

### See Also

database

### Related Attributes

health.db-valid

## resolve

Resolves a hostname to an IP address using the DNS settings. If the name cannot be resolved, it is returned **as-is**.

### Usage

```
resolve <hostname>
```

### See Also

reverse

## restart

Restart the network stack. The **--force** option will restart the network stack without prompting for confirmation.

### Usage

```
restart [--force]
```

## reverse

Performs a reverse-lookup on an IP address or a relative hostname using the DNS settings. If the value cannot be resolved, it is returned **as-is**.

### Usage

```
reverse <ip-address|hostname>
```

## See Also

resolve

## scp

Secure Copy (remote file copy program)

**scp** copies files between hosts on a network. The **scp** program installed on the SMS supports **scp** when initiated from outside of the SMS only. Attempts to issue the **scp** program from within the CLI will return an error.

## Caveats

The error message “PRNG is not seeded” is returned if **scp** is attempted from the SMS CLI.

## set

Assigns values to one or more attribs or to a list of attribs contained within an object. The list may be a one or more attrib names, object names, or attrib/object pairs. To accept the current or default value, type the return key. To clear a String or IP Address value, enter a period (.), and then the return key.

The **set** command can use any read-write or write-only attrib. See [“Attribs and Objects” on page 512](#) for more information. For information on set net, see [“net and net2” on page 520](#).

## Usage

```
set <attrib|object|attrib=value> [...]
```

## Related Commands

list, get

## Network Changes

If you need to change the IP address and gateway for the SMS server, you must complete the following procedure:

- 1 Change the IP address by entering the command:

```
set net.ipaddr = smsipaddr
```

where **smsipaddr** is the new IP address.

- 2 Change the gateway by entering the command:

```
set net.gateway = gateway
```

where **gateway** is the IP address of the new gateway.

- 3 Restart the network stack by entering the command:

```
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 when 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.

## setup

Initial setup wizard for providing essential configuration settings for the SMS server. Non-essential values can be configured with other commands.

The **setup** command is automatically invoked with the first CLI logon session. It is repeated with each new logon session until the entire setup procedure is finally completed. To repeat the procedure, execute the **setup** command at any time.

### Usage

```
setup
```

## shutdown

Shutdown and power-off the system. To restart the system, physically press the **POWER** button on the front of the unit. The **--force** option will reboot the system without prompting for confirmation. The **cancel** option aborts an in-progress shutdown operation.

### Usage

```
shutdown [--force] [cancel]
```

## snmp

The **snmp** command is used to manage the SNMP (Simple Network Management Protocol) values. SNMP is disabled by default and provided SNMPv1 read-only access. The **get** community name is configurable.

### Usage

```
snmp
```

## snmpget

**snmpget** will request a single OID from the specified agent.

### Usage

```
snmpget hostNameOrAddress communityName OID
```

### See Also

```
snmpget
```

## snmpwalk

**snmpwalk** will traverse the SNMP MIB of the agent running at the specified address. If the address OID is not provided, the walk will begin at the first OID, if the community name is not provided, walk with use **public** and if the *hostNameOrAddress* is not provided, walk will use localhost.

### Usage

```
snmpwalk [hostNameOrAddress [communityName [OID]]]
```

### See Also

snmpget

## time

The **time** command runs the specified program command with the given arguments. When the command finishes, **time** writes a message to standard output giving timing statistics about this program run. These statistics consist of the elapsed real time between invocation and termination, the user CPU time, and the system CPU time.

### Usage

```
time <command> [arguments..]
```

## tmc

Displays the TMC port settings for the box. **tmc** is an alias for the command **get tmc**, which displays the current TMC port value. To change the values, use the **set tmc** command. The **tmc** command supports the alternate TMC port feature. *The port number must be 443 or 4043.*

For V 2.5.1 and above, fresh installed systems use port 443 as the default. Upgrades to V 2.5.1 and below use 4043 as the default port.

### Usage

```
get tmc
set tmc <4043 | 443>
```

### Related commands

get, set

## traceroute

This program attempts to trace the route an IP packet would follow to some internet host by launching UDP probe packets with a small **t**tl (time to live) then listening for an ICMP **time exceeded** reply from a gateway. We start our probes with a **t**tl of one and increase by one until we get an ICMP **port unreachable** (which means we got to *host*) or hit a **max** (which defaults to 30 hops and can be changed with the **-m** flag). Three probes (change with **-q** flag) are sent at each **t**tl setting and a line is printed showing the **t**tl, address of the gateway and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a five second timeout interval (changed with the **-w** flag), an asterisk (\*) is printed for that probe.

## Usage

```
traceroute [-dFIrvx] [-f first_ttl] [-g gateway][-i iface] [-m max_ttl] [-p port] [-q queries]
[-s src_addr] [-t tos] [-w waittime] [-z pausesecs] host
```

## Options

- f** Set the initial time-to-live used in the first outgoing probe packet.
- F** Set the **don't fragment** bit.
- d** Enable socket level debugging.
- g** Specify a loose source route gateway (8 maximum).
- i** Specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the **-s** flag for another way to do this.)
- I** Use ICMP ECHO instead of UDP datagrams.
- m** Set the max time-to-live (max number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
- n** Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).
- p** Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT\_UNREACHABLE message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.
- r** Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed).
- s** Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in outgoing probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on. If the IP address is not one of this machine's
- t** Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. (If you are not running 4.4bsd, this may be academic since the normal network services like telnet and ftp don't let you control the TOS). Not all values of TOS are legal or meaningful - see the IP spec for definitions. Useful values are probably '-t 16' (low delay) and '-t 8' (high throughput).
- v** Use Verbose output. Received ICMP packets other than TIME\_EXCEEDED and UNREACHABLE values are listed.
- w** Set the time (in seconds) to wait for a response to a probe (default five seconds).

## update

This procedure leads you through upgrading SMS server software:

- 1 Acquire the latest upgrade package from the TMC web site.
- 2 Save it to a local HTTP or FTP server that can be accessed by the SMS server.
- 3 Provide the URL to this downloaded file. After the package is transferred and installed, the **update** procedure prompts for a reboot.

The **database** command prompts for a reboot, which is required for the operations to take effect.

### Usage

update

### Aliases

ctl.upgrade-source

## users

Lists and manages the SMS user accounts. You can create new users and assign passwords, roles, and disable settings.

### Usage

users

### Related Object

pwd

## version

Displays the system and component versions.

### Usage

version

### Related Objects

sw

## vi

**vi** is a text editor that is comparable to Vi. It can be used to edit all kinds of plain text. It is especially useful for editing programs. While running **vi**, a lot of help can be obtained from the on-line help system, with the **:help** command.

### Usage

vi [*options*] [*file ...*]



## Caveats

**/tmp** and its contents are the only files and directories that the SuperUser has permission to modify. When accessing files you must specify the complete path name (for example: **vi /tmp/FileName.txt**). After seven days without modification, files in this directory is removed.

## Options

The options may be given in any order, before or after filenames. Options without an argument can be combined after a single dash.

- +*[num]*** For the first file the cursor will be positioned on line *num*. If *num* is missing, the cursor will be positioned on the last line.
- +/*{pat}*** For the first file the cursor will be positioned on the first occurrence of *{pat}*. See “:help search-pattern” for the available search patterns.
- h** Give a bit of help about the command line arguments and options. After this, Vi exits.
- m** Modifying files is disabled. Resets the **write** option, so that writing files is not possible.
- n** No swap file will be used. Recovery after a crash will be impossible. Handy if you want to edit a file on a very slow medium (e.g. floppy). Can also be done with **:set uc=0**. Can be undone with **:set uc=200**.
- R** Read-only mode. The read-only option will be set. You can still edit the buffer, but will be prevented from accidentally overwriting a file. If you do want to overwrite a file, add an exclamation mark to the Ex command, as in **:w!**. The **-R** option also implies the **-n** option (see below). The read-only option can be reset with **:set noro**. See **:help ‘read-only’**.
- r {file}** Recovery mode. The swap file is used to recover a crashed editing session. The swap file is a file with the same filename as the text file with **.swp** appended. See **:help recovery**.
- Denotes the end of the options. Arguments after this will be handled as a file name. This can be used to edit a filename that starts with a dash (-).
- help** Give a help message and exit, just like **-h**.
- version** Print version information and exit.

## See Also

ftp, dir, delete, view

## view

Command to view the contents of the directory. Internal help is available by typing a question mark (?).

## See Also

delete, dir, ftp, vi

## web

HTTP/HTTPS (Hyper-Text Transfer Protocol) management.

Interactively prompts for configuration of web server settings. The HTTP and HTTPS services can be separately enabled through the **web** command. Additionally, a single password can be assigned to the content to limit access to reports, archived data, documentation and client downloads. The user name used for access is **web** and the password is assigned with the **web** command.

The HTTP protocol is not secure and transmits data and passwords in the clear. It is recommended that HTTP be disabled.

### Usage

web

### See Also

snmp

## who

Displays a list of CLI users, where and when the users originated.

### Usage

who

### See Also

health.who

# Attribs and Objects

This section briefly describes each object and attrib used by the SMS CLI. For more detailed information about each element, see the individual commands described in [“Command Reference” on page 496](#).

## Attrib Types

The following table describes each type of attrib that you can view or edit in the CLI.

Table A - 4: CLI Attrib Types

Type	Definition
Bool	Boolean. Value can be <b>true</b> or <b>false</b> .
String [#]	String Can have a maximum size of #.
Password	String Uses asterisk (*) to mask out the value as it is entered.
IPaddr	IP address Uses dotted notation.
Name [#]	String Can contain alpha-numeric characters with a maximum size of #.

# Object Reference

The following objects are available in the SMS CLI:

- [“cli” on page 513](#)
- [“ctl” on page 514](#)
- [“db” on page 514](#)
- [“dns” on page 499](#)
- [“high availability” on page 516](#)
- [“health” on page 517](#)
- [“kbd” on page 518](#)
- [“license” on page 519](#)
- [“net and net2” on page 520](#)
- [“ntp” on page 521](#)
- [“pkg” on page 523](#)
- [“route” on page 525](#)
- [“snmp” on page 526](#)
- [“svc” on page 526](#)
- [“sw” on page 528](#)
- [“sys” on page 529](#)
- [“time” on page 530](#)

See the following sections for more detailed information about each object and its attribs.

## cli

Collection of CLI-related attribs. The attribs are used to adjust CLI behavior, including the inactivity timeout value.

Table A - 5: cli Attribs

Attrib	Description	Type	Access	Range
cli.sessionTimeout	Attribute used to control the auto-logout time. By adjusting the value, you can control the number of minutes before the CLI will automatically log out due to inactivity. You can set the value to 0 to disable the timeout function. If you change the time by 1 minute or more, the SMS server restarts. Example: set cli.sessionTimeout=30	Int	read-write	0-32000

## ctl

Collection of system control operations. The attribs contained in **ctl** can be used to reboot or shutdown the system, or access the upgrade capability. See [“Remote Paths” on page 493](#) for more information about entering path names for attribs that require them.

Table A - 6: ctl Attribs

Attrib	Description	Type	Access	Range
ctl.power-off	Setting the <b>ctl.power-off</b> attrib to the value of <b>true</b> will cause the system to shutdown and power-off. To restart the system, it is necessary to physically press the <b>Power</b> button on the front panel of the box.	Bool	write-only	0
ctl.reboot	Setting the <b>ctl.reboot</b> attrib to the value of <b>true</b> will cause the system to reboot. The operation will be immediate with no warning given to other users using the client or the CLI.	Bool	write-only	0
ctl.reboot-needed	Returns the state of the system, indicating whether there are pending configuration settings that require a reboot to apply those changes.	Bool	read-only	0
ctl.upgrade-source	Setting the <b>ctl.upgrade-source</b> attrib to a string representing a URL will cause the system to retrieve and apply the update package to the system. Normally, a reboot will be required for the update to become effective. The URL can reference the http, https or ftp protocols. Example: set ctl.upgrade-source=http://www.tippingpoint.com/SMS-UPDATE-1.0.pkg	String	write-only	5-128

## db

Collection of database control operations. The attribs contained in **db** can be used to backup, restore or re-initialize the system database. See [“Remote Paths” on page 493](#) for more information about entering path names for attribs that require them.

On startup, the sequence performed is (1) if requested, backup the database, (2) if requested, restore the database, (3) if requested, reinit the database, (4) if needed, migrate the database. Therefore, within a single restart, a current database can be saved to a remote system, and a new database can replace the old one. To clear a current value, set the attrib to a period (.).

## Related Commands

database

Table A - 7: db Attribs

Attrib	Description	Type	Access	Range
db.attackCount	Displays the number of attack records stored in the database.	Int	read-only	0
db.check	Verifies the integrity of the database.			
db.export-files	Files to be saved and transported to a remote system can be stored in the export directory. To transfer the entire contents of the export directory this attrib must be provided with the name of a Samba (SMB) mount point. The destination mount point must be writable by the SMS server. SMB can be secured by providing an access list on the server that prevents all machines <i>except</i> for the SMS server to access it. The export directory can be cleared by setting the <b>db.clear-export</b> attrib. Example: set db.export-files=server:/export/directory	String	write-only	4-132
db.initTime	The time that the database was re-initialized.	String	read-only	0-32
db.reinit	Setting the <b>db.reinit</b> attrib to <b>true</b> will schedule the database to be cleared upon system startup the next time the system is rebooted.	Bool	read-write	0

## dns

The **dns** object contains default domain name, DNS search list and DNS server information.

## Related Objects

nic, ntp

Table A - 8: dns Attribs

Attrib	Description	Type	Access	Range
dns.domain	Default DNS domain used to resolve hostnames. If a fully-qualified hostname is not provided, the domain is appended to the hostname and the result is passed for resolution.	Name	read-write	2-64
dns.search	DNS domain search list used to resolve hostnames. If a fully-qualified hostname is not provided, each member of the search list is appended to the hostname and the result is passed for resolution.	String	read-write	2-128

Table A - 8: dns Attribs

Attrib	Description	Type	Access	Range
dns.server1 dns.server2 dns.server3	Attribs used to specify name resolution servers. The value must be a dotted IP address, and the first entry ( <b>dns.server1</b> ) will be assigned a preferred role. To clear this value, use a period (.).	IPaddr	read-write	7-15

## high availability

Collection of system High Availability (HA) attribs. The attribs are used to retrieve HA information.

Table A - 9: ha Attribs

Attrib	Description	Type	Access	Range
ha.status	Attribute returning the status of HA. The status messages include the following: <ul style="list-style-type: none"> <li>• Disabled: High Availability is not configured.</li> <li>• Enabled</li> <li>• Error: The system could not determine local status.</li> <li>• Error: Unable to communicate with peer.</li> <li>• Error: Peer system state is invalid.</li> <li>• Error: Configuration out of sync with peer.</li> <li>• Error: Peer system failure.</li> <li>• Configured: Synchronization required.</li> <li>• Configured: Attempting synchronization.</li> <li>• Configured: Synchronizing</li> <li>• Degraded: Peer takeover pending.</li> <li>• Degraded: Unable to communicate with peer.</li> <li>• Degraded: Synchronization required.</li> <li>• Degraded: Peer system failure</li> </ul>	String	read-only	
ha.disable	Attribute that disables HA.	String		
ha.configured	Attribute returning the status of the HA configuration.		read-only	

## health

Collection of system health-related attribs. The attribs are used to retrieve system health information, including utilization values, and system uptime statistics.

Table A - 10: health Attribs

Attrib	Description	Type	Access	Range
health.cpu-util	Attribute returning the CPU (Processor) utilization. 0% represents a near-idle system, and 100% is fully-utilized.	String	read-only	2-4
health.db-valid	Attribute reporting the status of the database. If <b>true</b> , then the database is considered valid and fully operational, if <b>false</b> , the system should be restarted, and other corrective steps taken.	String	read-only	1-32
health.diskIo	Disk I/O statistics. <ul style="list-style-type: none"> <li>• blocks-read</li> <li>• blocks-written</li> </ul>	String	read-only	0-128
health.disk-util	Attribute returning the disk system utilization. As disk utilization approaches 100%, database management operations should be performed to reduce disk usage.	String	read-only	2-4
health.loadAvg	CPU load statistics. <ul style="list-style-type: none"> <li>• load-avg-1min</li> <li>• load-avg-5min</li> <li>• load-avg-15min</li> <li>• runnable-processes/total-processes</li> <li>• current-pid</li> </ul>	String	read-only	0-128
health.memInfo	Physical memory statistics. <ul style="list-style-type: none"> <li>• total</li> <li>• used</li> <li>• free</li> <li>• shared</li> <li>• buffers</li> <li>• cached</li> </ul>	String	read-only	0-128
health.mem-util	Attribute returning the memory (RAM) utilization. 0% represents a near-idle system, and 100% is fully-utilized.	String	read-only	2-4
health.net-valid	Attribute reporting the status of the communication paths to the TMC and each of the configured devices. The message will indicate the nature of the problem. Usually, the problem can be addressed by confirming that the network settings permit the SMS to communicate with <a href="https://tmc.tippingpoint.com">https://tmc.tippingpoint.com</a> , available through the internet.			

Table A - 10: health Attribs

Attrib	Description	Type	Access	Range
health.swapInfo	Swap memory statistics. <ul style="list-style-type: none"> <li>• total</li> <li>• used</li> <li>• free</li> </ul>	String	read-only	0-128
health.swapIo	Swap I/O statistics. <ul style="list-style-type: none"> <li>• blocks-read</li> <li>• blocks-written</li> </ul>	String	read-only	0-128
health.sys-valid	Attribute reporting the status of the SMS server application. If <b>true</b> , then the system is considered valid and fully operational, if <b>false</b> , the system should be restarted, and other corrective steps taken.	String	read-only	1-32
health.uptime	Attribute reporting the amount of time since the last system boot.	String	read-only	2-56
health.who	Attribute reporting a list of currently logged-in users. Pipe ( ) characters are used in place of carriage-return characters.	String	read-only	0-1024

## kbd

Keyboard related attribute.



**WARNING:** Do not use this option if you are using a standard QWERTY keyboard. Setting your keyboard layout to a value with which you are not familiar could render your system inaccessible.

### Related Command

kbdcfg

Table A - 11: key Attrib

Attrib	Description	Type	Access	Range
kbd.layout	Specifies the console keyboard layout. Usage: <code>set kbd.layout=&lt;keyboard designation&gt;</code> Example setting: <code>fr</code> for French keyboard layout. The default setting is <code>kbd.layout=us</code>	String	read-write	0-64



The following console keyboard layouts are available:

```

This procedure will lead you through setting the
layout for your keyboard. The following layouts
are available:

ANSI-dvorak      dvorak-l      it-ibm        se-fi-lat6
applkey         dvorak-r      it2           se-ir209
azerty          emacs         jp106         se-lat6
backspace       emacs2        keypad        se-latin1
be-latin1       es            la-latin1     sg
bg-cp1251       es-cp850     lt            sg-latin1
bg-cp855        et            lt.baltic    sg-latin1-lk450
bg_bds-cp1251  et-nodeadkeys  lt.l4        sk-prog-qwerty
bg_bds-utf8     euro         mk            sk-prog-qwertz
bg_pho-cp1251  euro1        mk-cp1251    sk-qwerty
bg_pho-utf8     euro2        mk-utf       sk-qwertz
br-abnt         fi           mk0          slovene
br-abnt2        fi-latin1    n1           sr-cy
br-latin1-abnt2  fi-latin9   n12          sv-latin1
br-latin1-us    fi-old       no           tr_f-latin5
by              fr           no-latin1    tr_q-latin5
cf              fr-latin0    pc110        tralt
croat           fr-latin1    pl           trf
ctrl            fr-latin9    pl2          trq
cz              fr-old       pt           ua
cz-cp1250       fr-pc        pt-latin1    ua-utf
cz-lat2         fr_CH        pt-latin9    ua-utf-ws
cz-lat2-prog    fr_CH-latin1  ro_win       ua-ws
cz-us-qwertz    gr           ru           uk
de              gr-pc        ru-cp1251    unicode
de-latin1       hu           ru-ms        us
de-latin1-nodeadkeys  hu101       ru-yawerty   us-acentos
de_CH-latin1    il           ru1          wangbe
defkeymap       il-heb       ru2          wangbe2
defkeymap_V1.0  il-phonetic  ru3          windowkeys
dk              is-latin1    ru4

```

## license

License information for the SMS server. The license is used to control the number of managed devices supported by the server.

### Related Command

key

Table A - 12: license Attribs

Attrib	Description	Type	Access	Range
license.count	Returns the number of devices that the license key permits for this server.	Int	read-only	0-1000
license.date	Returns the date that the current license key was installed.	String	read-only	0-32
license.desc	Returns the license key description.	String	read-only	0-64
license.key	Sets or returns the current SMS server license key.	String	read-write	32
license.reset	Resets the current SMS server license key.			

## net and net2

Collection of network-related attribs. The attribs are used to configure the two Ethernet 10/100 interfaces for access to the local network. The secondary interface is the upper 10/100 RJ-45 connector.

Unless identified as a net-only attrib, each attrib listed as **net.\*** listed below can use the prefix **net** or **net2** to specify the correct Ethernet 10/100 interface.

### Related Commands

ifconfig, ipconfig

### Related Objects

dns

Table A - 13: net and net2 Attribs

Attrib	Description	Type	Access	Range
net.gateway	Attribute used to provide the gateway (default route) value. To clear this value, use a period (.). Applies only the net object. When you modify this value using the <b>set</b> command, you must issue the <b>set net.restart=yes</b> command to save and employ the changes. When you employ this command, the CLI may not reflect the change with a confirmation message. See <a href="#">“Network Changes” on page 506</a> .	IPaddr	read-write	0
net.hwaddr	Attribute used to return the Hardware / MAC (Media Access Control) address for the Ethernet 10/100 interface.	String	read-only	17
net.ifc-enable	Attrib used to enable/disable the NIC. Normally, this should not be done. To enable the NIC set the value to <b>true</b> , to disable the value should be set to <b>false</b> .	Bool	read-write	0
net.ipaddr	Attribute used to view and change the IP address for the Ethernet 10/100 interface. To clear this value, use a period (.). When you modify this value using the <b>set</b> command, you must issue the <b>set net.restart=yes</b> command to save and employ the changes. When you employ this command, the CLI may not reflect the change with a confirmation message. See <a href="#">“Network Changes” on page 506</a> .	IPaddr	read-write	0
net.mask	Attribute used to provide the subnet mask value. To clear this value, use a period (.).	IPaddr	read-write	0
net.ready	Returns "true" if the primary network interface is configured and ready.			

Table A - 13: net and net2 Attribs

Attrib	Description	Type	Access	Range
net.restart	Attribute used restart the Ethernet 10/100 interface with the current network settings. Set to <b>true</b> to restart immediately. ( <b>false</b> has no effect.) Warning: restarting the network interface may cause connections to be lost, including SMS client sessions, and remote CLI sessions. Applies only the net object.	Bool	write-only	0
net.speed	Attribute used to view and change the network speed setting for the Ethernet 10/100/1000 interface. Valid values are: 10, 100, or 1000 Mb/s.	String	read-write	2-4
net.duplex	Attribute used to view and change the duplex setting for the Ethernet 10/100/1000 interface. Valid values are: half or full.	String	read-write	4
net.autoneg	Attribute used to view, and enable/disable auto-negotiation for the Ethernet 10/100/1000 interface. Valid values are: yes or no.	Bool	read-write	0

## ntp

Collection of NTP (Network Time Protocol) settings used to synchronize the system time with a remote time server. NTP allows machines within a network to be synchronized on a common time.

### Related Objects

svc, snmp

Table A - 14: ntp Attribs

Attrib	Description	Type	Access	Range
ntp.server1 ntp.server2 ntp.server3	Attribs used to specify a list of NTP time servers. The value may be a dotted IP address or a hostname. The first entry ( <b>ntp.server1</b> ) will be assigned the preferred time server role. The preferred time server is also used as a step ticker, which adjusts the time immediately upon system boot. To clear this value, use a period (.).	IPaddr	read-write	0

Table A - 14: ntp Attribs

Attrib	Description	Type	Access	Range
ntp.auth-enable	<p>Attrib used to enable/disable the NTP authentication. It allows the NTP client to verify that the server is known and trusted and not an intruder intending to masquerade as that server. We only support NTP V3 (symmetric key) authentication.</p> <p>To enable the NTP authentication, set the value to <code>yes</code>, and a key id and key value should be provided with the <code>ntp.auth-keyId</code> and <code>ntp.auth-keyValue</code> attribs.</p> <p>To disable the value, set it to <code>no</code>.</p> <p>Example: <code>set ntp.auth-enable=yes</code></p>	Bool	read-write	0
ntp.auth-keyId	<p>The ID of key which is used to authenticate NTP server if the NTP authentication is enabled. The ID has to exist in <code>/etc/ntp/keys</code> before you set this value. To clear this value, use a period (<code>.</code>).</p> <p>Example: <code>set ntp.auth-keyId=1</code></p>	Int	read-write	1-65535
ntp.auth-keyValue	<p>The value of key which is used to authenticate NTP server if the NTP authentication is enabled. The key has to exist in <code>/etc/ntp/keys</code> before you set this value. To clear this value, use a period (<code>.</code>).</p> <p>Example: <code>set ntp.auth-keyValue=test</code></p>	String	read-write	1-255

## pkg

Collection of attribs used to control package management.

### Related Object

tmc (object)

Table A - 15: license Attribs

Attrib	Description	Type	Access	Range
auto-download	controls whether new packages available at the TMC are automatically downloaded. Email will be generated to notify the administrator of the action (if configured).	Bool	read-write	0
auto-install	controls whether the SMS database is updated with the newly downloaded package.	Bool	read-write	0
auto-distrib	controls whether the new package will be distributed to the managed devices.	Bool	read-write	0
tmc-poll-rate	controls the frequency of the check for new TMC packages.	Int	read-write	0-9999
proxy-tmc	controls whether a HTTP proxy server is used to make TMC connections.	Bool	read-write	0
tmc-proxy-host	controls which proxy server to use to make TMC connections.	String	read-write	1-128
tmc-proxy-port	controls which proxy server port to use to make TMC connections.	Int	read-write	1-65535
proxy-tmc-authenticate	controls whether authentication is required with the HTTP proxy server.	Bool	read-write	0

## pwd

Collection of password-related attribs. The attribs are used to confirm the **SuperUser** password and enable the service mode used by support personnel. For information about managing users including, user groups, passwords, and security levels, see [“General Administration” on page 437](#).

### Related Command

users

Table A - 16: pwd Attribs

Attrib	Description	Type	Access	Range
pwd.group-adduser	Used to add a user to a group.		write-only	
pwd.group-deluser	Used to remove a user from a group.		write-only	
pwd.group-list	Used to list all groups, or groups with users.		read-only	
pwd.level	Attribute used to set the security level for the password.			
pwd.service-enable	Attribute used to enable/disable the service mode password for the system. To protect customer security, the service mode is deactivated at the factory, to enable the service mode account, the customer must log on as <b>SuperUser</b> and set this attrib to <b>true</b> . After service mode is enabled, a service professional can log onto the system in with a secret password. To disable the service mode, set the attrib to <b>false</b> . To clear this value, use a period (.). Example: set pwd.service-enable=false	Bool	read-write	0
pwd.user-add	Used to add a user.		write-only	
pwd.user-age	Attribute used to set the maximum age for a password.			
pwd.user-del	Used to delete a user.		write-only	
pwd.user-desc	Attribute used to describe the user account.			
pwd.user-email	Attribute used for the user account's email address.			
pwd.user-expires	Attribute used to enable password expiration.			
pwd.user-expiredays	Attribute used to set the amount of days to check the account for expiration.		read-only	
pwd.user-info	Attribute used to list the user accounts.		read-only	
pwd.user-pager	Attribute used to include the user account's pager number.			
pwd.user-phone	Attribute used to include the user account's phone number.			

Table A - 16: pwd Attribs

Attrib	Description	Type	Access	Range
pwd.user-pwd	Attribute used for the user account's password.		read-only	
pwd.user-state	Attribute for the state for the user ID.			
pwd.user-verify				
pwd.SuperUserConfirm	Used to confirm a password value assigned to the <b>SuperUser</b> account. Returns Success if the password matches, otherwise an error. Causes a SMS logon message to be sent to the audit log.	Password	write-only	8-32
pwd.web	Used to assign a password to the HTTP/HTTPS-accessible content. This single password allows access to the user manuals, the client software, reports, and archived attack data. To clear the password and permit unrestricted access to the web server, set the value to a '.' character.	Password	write-only	8-32

## route

Collection of network-related attribs. The attribs are used to configure the Ethernet 10/100 interface for access to the local network.

### Related Objects

net

### Related Commands

ifconfig, ipconfig

Table A - 17: route Attribs

Attrib	Description	Type	Access	Range
route.add	Attribute used to add a static route to the IP routing table. Usage: <code>route.add &lt;destination&gt; &lt;mask&gt; &lt;gateway&gt;</code>			
route.del	Attribute used to delete a static route from the IP routing table. Usage: <code>route.del &lt;destination&gt; &lt;mask&gt; &lt;gateway&gt;</code>			
route.info	Attribute used to list all routes in the IP routing table.	String	read-only	0-1024

## smtp

Collection of SMTP (Simple Mail Transfer Protocol) -related attribs. The attribs are used to configure the smtp service.

Table A - 18: smtp Attribs

Attrib	Description	Type	Access	Range
smtp.notify-list	List of e-mail addresses used to deliver notification messages when a notifiable event occurs. The list should be one or more e-mail addresses separated by comma or semicolons.			

## snmp

Collection of SNMP (Simple Network Management Protocol) -related attribs. The attribs are used to configure the snmp service.

### Related Objects

svc

### Related Commands

ntp, web

Table A - 19: snmp Attribs

Attrib	Description	Type	Access	Range
snmp.get-community	Attrib used to specify the <b>get</b> community name for the system over the SNMP protocol. Read access is available to the SMS system, but write access is disabled in this release.	String	read-write	1-32
snmp.trap-community	Attrib used to specify the community name used to send system traps. For traps to be sent, a snmp.trap-dest must be set. Independent of the trap settings, the snmp agent can be enabled with the svc.snmp-enable attrib.			
snmp.trap-dest	Attrib used to specify the destination for system traps. For traps to be sent, a snmp.trap-dest must be set. If the snmp.trap-community is not specified, "public" is used. Independent of trap generation, the snmp agent may be disabled with the svc.snmp-enable attrib.			

## SVC

Collection of attribs used to enable various services that execute within the system. While the system implements an internal firewall to protect against attacks, further security can be implemented by disabling unneeded services.



## Related Commands

ntp, snmp, pwd

Table A - 20: svc Attribs

Attrib	Description	Type	Access	Range
svc.http-enable	Attribute used to enable/disable the HTTP (HTTP protocol) service. The HTTP service is used to download the SMS client during the installation process and download other files. The service is configured to prevent CGI and other active server processing. Once the client is downloaded, the service can be disabled until an updated client is available. HTTP and HTTPS can be enabled separately. To enable HTTP, set the <b>svc.http-enable</b> attrib to <b>true</b> . To disable, set to <b>false</b> . Example: set svc.http-enable=true	Bool	read-write	0
svc.https-enable	Attribute used to enable/disable the HTTPS (Secure HTTP protocol) service. The HTTPS service is used to download the SMS client during the installation process. The service is configured to prevent CGI and other active server processing. Once the client is downloaded, the service can be disabled until an updated client is available. To enable HTTPS, set the <b>svc.https-enable</b> attrib to <b>true</b> . To disable, set to <b>false</b> .	Bool	read-write	0
svc.ping-enable	Attribute used to enable/disable incoming ping support. Responding to pings can be considered a security weakness for systems. When disabled, the SMS will not respond to ICMP Echo Requests. Example: set svc.ping-enable=true			
svc.ntp-enable	Attrib used to enable/disable the NTP (Network Time Protocol) client. The NTP client can be used to synchronize system time with a list of remote time servers. To enable the NTP client, set the value to <b>true</b> , and a list of servers should be provided with the <b>ntp.server1 (...)</b> attribs. To disable the value should be set to <b>false</b> . Example: set svc.ntp-enable=true	Bool	read-write	0
svc.snmp-enable	Attribute used to enable/disable the SNMP (Simple Network Management Protocol) agent. The SNMP service provides limited, read-only management support to a remote SNMP manager. To enable SNMP, set the <b>svc.snmp-enable</b> attrib to <b>true</b> . To disable, set to <b>false</b> . The community name for get requests can be set with the <b>snmp.get-community</b> attrib. Example: set svc.snmp-enable=true	Bool	read-write	0

Table A - 20: svc Attribs

Attrib	Description	Type	Access	Range
svc.ssh-enable	Attribute used to enable/disable the SSH (Secure Shell) service. The SSH service is used to provide secured, remote CLI (Command Line Interface) access to the system. If SSH is disabled, the CLI can still be accessed by connecting a terminal or a keyboard/monitor to the chassis. The SMS server supports SSH protocol version 2. To enable SSH, set the <b>svc.ssh-enable</b> attrib to <b>true</b> . To disable, set to <b>false</b> . Example: set svc.ssh-enable=true	Bool	read-write	0
svc.telnet-enable	Attribute used to enable/disable the Telnet service. The Telnet service is used to provide remote CLI (Command Line Interface) access to the system. If Telnet is disabled, the CLI can still be accessed by connecting a terminal or a keyboard monitor to the chassis, or by using the SSH service. To enable Telnet, set the <b>svc.telnet-enable</b> attrib to <b>true</b> . To disable, set to <b>false</b> . Example: set svc.telnet-enable=true	Bool	read-write	0
svc.tmc-poll-rate	The SMS polls the TMC at regular intervals (factory default is 30 minutes). Communication is attempted over TCP port 443 to the host " <a href="https://tmc.tippingpoint.com">https://tmc.tippingpoint.com</a> ". The poll rate can be adjusted by providing the svc.tmc-poll-rate attrib with a new value and then rebooting the SMS. Assigning the attrib the value of '0' will disable polling. (This setting may be desirable when the SMS is behind a firewall which prevents outbound communication with the TMC.)			

## SW

Collection of software versioning attribs. The attribs are used to report the system software version, and to list the software packages and their individual versions.

Table A - 21: sw Attribs

Attrib	Description	Type	Access	Range
sw.components	Returns a list of installed software packages and their versions.	String	read-only	0-1024
sw.version	Attribute returning the system software version.	String	read-only	1-32

## sys

Collection of system-related attribs. The attribs retain system values, including the system name, location and contact.

Table A - 22: sys Attribs

Attrib	Description	Type	Access	Range
sys.contact	Attribute holding the system contact. Normally, this file contains the name and/or address of the administrator of this system.	String	read-write	0-64
sys.location	Attribute holding the system location. Normally, this field contains the physical location of the system.	String	read-write	0-64
sys.name	Attribute holding the system name. The system name must be set. It will be used in system prompts, and will be registered with dynamic name servers if DHCP is enabled.	Name	read-write	1-32
sys.serialNum	Attribute returning the unique \${PRODUCT} system serial number. Provide this serial number in interactions with support professionals.	String	read-only	20

## time

Collection of system time attribs. The attribs are used to configure the local time zone and the current system time.

### See Also:

ntp

Table A - 23: time Attribs

Attrib	Description	Type	Access	Range
time.dateTime	Displays the current system time in a readable format.	String	read-only	32
time.setTime	Displays and sets the current system time. The date and time is specified in the format: [MMDDhhmm[[CC]YY][.ss]]	String	read-write	32
time.setTimeZone	Displays and sets the current local time zone. Time zones can be represented in several forms, but preferred is a three-letter zone, followed by a time offset from GMT, and another three-letter zone for the daylight savings time. Examples: EST5EDT, America/Newark, CST6CDT, America/Chicago, MST7MDT, America/Denver, PST8PDT, America/Los_Angeles set time.setTimeZone=America/New_York set time.setTimeZone=CST6CDT	String	read-write	2-48

# B Open Source Licenses

*TippingPoint's TippingPoint software uses some open source components. Many open source license agreements require user documentation to contain notification that the open source software is included in the product.*

## Open Source Software in SMS

The following open source software used by the SMS requires that the full text of the license be published with the user documentation:

- [Apache License](#) — Primarily for the log4j (logging) and SOAP technologies
- [JDOM License](#) — Primarily for Xerces (XML driver) and jdom (XML handling)
- [Gnu Public License \(GPL\)](#) — Primarily for the following:
  - *RedHat 9.0 distribution (all of the pieces that make up RedHat, including Etherreal, UCD SNMP, and so on)*
  - *MySQL*
  - *mysql-connector (JDBC mysql driver)*
  - *dbConnectionBroker (database connection broker)*



**Note** The TippingPoint (TP) license for the SMS was included in the contents of your SMS box. To request additional copies of the license, contact TippingPoint customer service.

## Apache License

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see < <http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

## JDOM License

Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name “JDOM” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [license@jdom.org](mailto:license@jdom.org).
4. Products derived from this software may not be called “JDOM”, nor may “JDOM” appear in their name, without prior written permission from the JDOM Project Management ([pm@jdom.org](mailto:pm@jdom.org)). In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: “This product includes software developed by the JDOM Project (<http://www.jdom.org/>).” Alternatively, the acknowledgment may be graphical using the logos available at <http://www.jdom.org/images/logos>.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin ([brett@jdom.org](mailto:brett@jdom.org)) and Jason Hunter ([jhunter@jdom.org](mailto:jhunter@jdom.org)). For more information on the JDOM Project, please see <http://www.jdom.org/>.

## Gnu Public License (GPL)

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION



0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients'

exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## END OF TERMS AND CONDITIONS

### Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy <name of author>
```

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.
```

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ``show w'` and ``show c'`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
<signature of Ty Coon>, 1 April 1989
```

```
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.



# C Troubleshooting

*The SMS is a complex system. If you cannot find the information you are seeking in this manual, please contact your TippingPoint customer support representative.*

## Overview

This section includes the following topics:

- [“Log On Error Messages” on page 541](#)
- [“Password Recovery” on page 541](#)
- [“Password Recovery” on page 541](#)
- [“IPS Port Out-of-Service” on page 543](#)
- [“SMS Error Messages” on page 543](#)

## Log On Error Messages

To recover from error messages that occur in the Log On dialog box, see the following items:

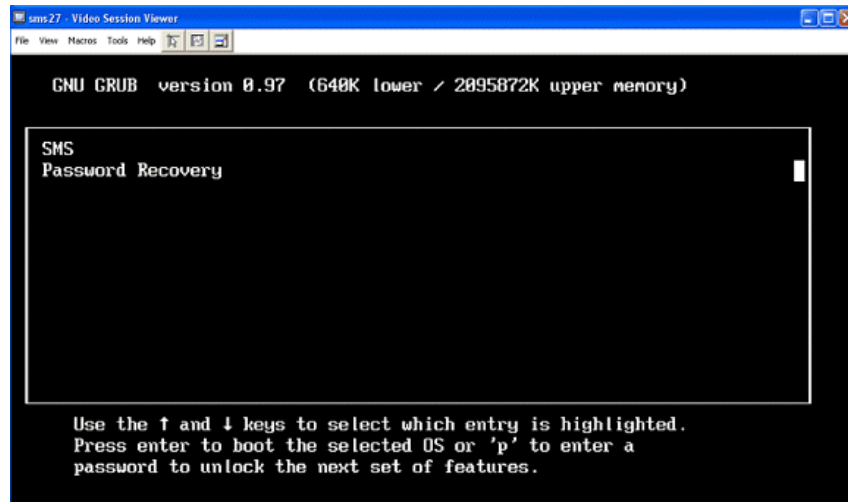
- If you see the error message **Connect Failed**, verify that you have entered the correct IP address or fully qualified host name for the server. You might also need to verify that the server is properly connected to the network and that the network is up.
- If you see the error message **Can't authenticate! Retype and try again**, verify that you have typed the correct username and password.

## Password Recovery

If you need to recover your password, the SMS provides an automated recovery mechanism.

- 1 Attach a console to the SMS.
- 2 Reboot and watch for the **GNU GRUB** menu that displays after the **Grub:** prompt.

- 3 When the prompt displays, press the **Esc** key.
- 4 Select the **Password Recover** option and press **Enter**.



When the SMS completes the boot sequence, the factory SuperUser account is reactivated and the password is the serial number of your SMS.

## Network Changes

If you need to change the IP address and gateway for the SMS server, you must complete the following procedure:

- 1 Change the IP address by entering the command:

```
set net.ipaddr = smsipaddr
```

where ***smsipaddr*** is the new IP address.

- 2 Change the gateway by entering the command:

```
set net.gateway = gateway
```

where ***gateway*** is the IP address of the new gateway.

- 3 Restart the network stack by entering the command:

```
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 when 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 [“set” on page 506](#).



## 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.

To resolve this issue, do the following:

- 1 Display the Devices screen.
- 2 On 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. The options disables.
- 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 details the 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 the 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 message, please 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** TippingPoint suggests modifying and distributing smaller amounts of filters, using Category Settings, and Shared Settings to help improve performance and distribution of profiles. See [“IPS Profile Filters” on page 189](#) and [“Traffic Management Filters” on page 230](#).

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, TippingPoint recommends using the Category Settings for a category of filters. The Category Settings affect action set changes across all filters for a category. See [Chapter 6, “Profiles”](#).

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, TippingPoint recommends 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 [Chapter 6, “Profiles”](#) and [“Traffic Management Filters” on page 230](#).

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 device has 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** TippingPoint suggests modifying and distributing smaller amounts of filters, using Category Settings, and Shared Settings to help improve performance and distribution of profiles. See [Chapter 6, “Profiles”](#) and [“Traffic Management Filters” on page 230](#).

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.





# X-Family Remote Deployment

*The SMS provides a method to add and manage remote X-Family devices over a secure VPN tunnel.*

## Overview

This section includes the following topics:

- [“Example Deployment” on page 548](#)
- [“Setup” on page 550](#)
- [“Device Management” on page 554](#)
- [“Device Recovery” on page 554](#)

The SMS provides a method to acquire and manage remote X-Family devices over a secure VPN tunnel. This method is based on using the serial number for X-Family devices and a VPN configuration file to setup the connection. The X-Family device is added to the SMS in the offline mode and uses the device serial number rather than the IP address. A VPN configuration file of X-Family CLI commands must also be added to the SMS offline device setup. When the configuration file is downloaded to the device, a site-to-site VPN between a local SMS and the remote X-Family device is established.



**Note:** If an X-Family device is in Fully Transparent mode (i.e. it has only one virtual interface - the external one) Offline Device Acquisition will not work.

At the beginning of this device acquisition process the remote device is identified on the SMS **All Devices** screen by the serial number. When the process is complete (approximately two minutes), the serial number is removed and the device name appears on the SMS **All Devices** screen. The SMS can then manage the device.

The following setup requirements apply:

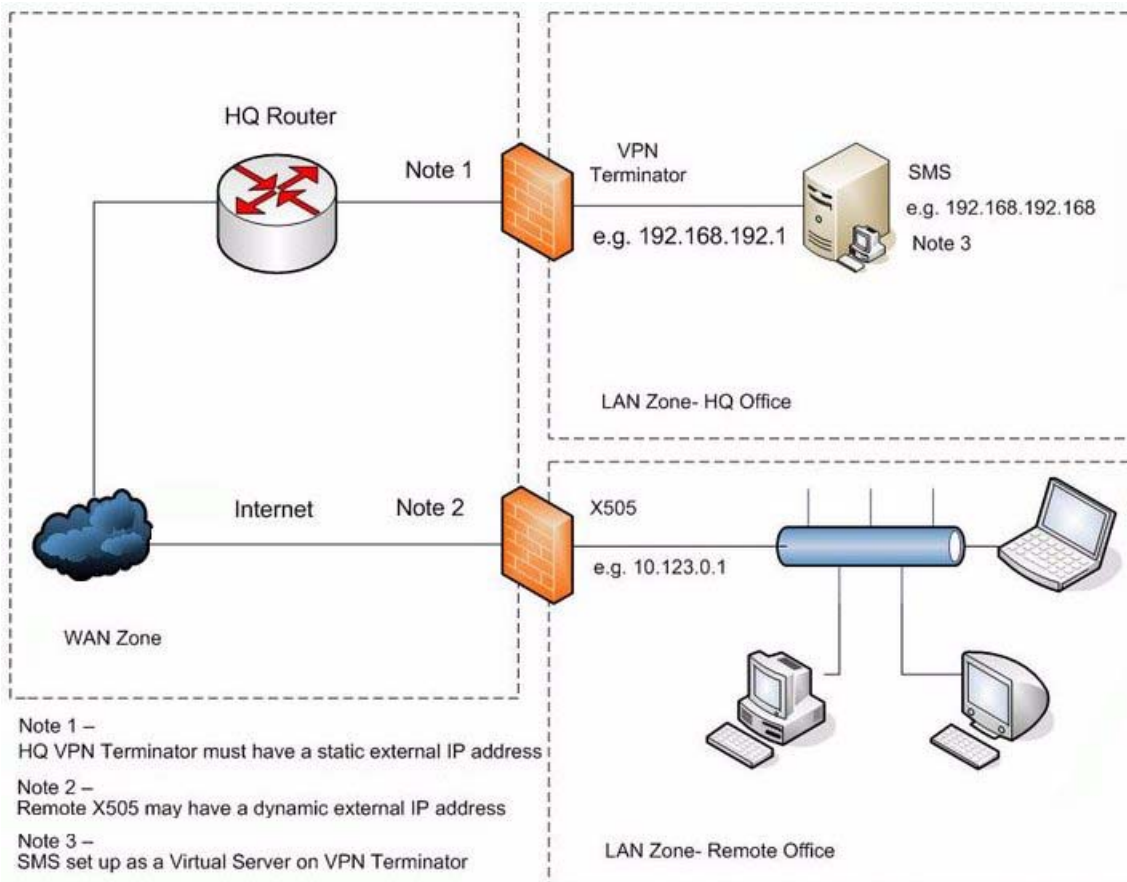
- **SMS Setup**— X-Family devices must be added offline using serial numbers. Setup must also include a VPN configuration file to establish the required VPN between the X-Family and the SMS. [“Device Management” on page 554.](#)
- **VPN Terminator Setup** — VPN Terminator (to which SMS is connected) must meet specific configuration requirements. See [“VPN Terminator Setup” on page 553.](#)
- **X-Family Device Setup** —SMS configuration must be enabled with the X-Family CLI `setup` command or the `conf t sms` command. See [“VPN Terminator Setup” on page 553.](#)

## Example Deployment

The following figure represents an example remote deployment where:

- Central headquarters site (HQ Office) has the SMS and a VPN Terminator.
- One remote site (Remote Office) has the X-Family device that is acquired using the “phone home” technique.
- VPN Terminator may or may not be an X-Family device.  
If the VPN Terminator is an X-Family device, the SMS can acquire and manage the device using the normal online method.

Figure E - 1: Device - New Device: Remote Acquisition Configuration



## How It Works

Remote deployment of X-Family devices includes the following items:

- [“Device Acquisition” on page 549](#)
- [“Remote Management” on page 549](#)

### Device Acquisition

The SMS sees the remote X-Family device “phoning home” (using SSL over TCP Port 10043) and recognizes the serial number. The VPN CLI commands file is downloaded and run on the acquired device to set up the other end of the site-to-site VPN tunnel. The SMS then switches over to managing the remote device using the remote device's internal IP address (over the VPN tunnel). For more information, see [“VPN Configuration File” on page 550](#)

### Remote Management

Remote X-Family devices that are accessed via the internet are managed through an IPSec (or GRE/ IPSec) tunnel between the HQ where the SMS is located and the remote X-Family device. The tunnel,

which may also be used for regular data traffic, provides a secure connection for the device to communicate with the SMS over the Public Internet. The tunnel does not come up until the initial configuration file has been downloaded over a temporary https connection



**Note** If you use a VPN tunnel for device acquisition, this tunnel can also be used for other data. Any additional VPN tunnels that are set up on the device must not interfere with this tunnel (by editing the underlying IKE proposal or by using the same local and remote subnets).

## Setup

This section contains the following topics:

- [Device Management](#)
- [VPN Terminator Setup](#)
- [VPN Terminator Setup](#)

## SMS Setup

X-Family devices must be added using the offline feature. The SMS setup requires the following items:

- [X-Family Device Serial Numbers](#)
- [VPN Configuration File](#) — file containing a number of X-Family CLI commands that is downloaded to the remote device to setup the remote end of the VPN tunnel.

For SMS Setup instructions, see “[Configure SMS for Remote X-Family Device Acquisition and Management](#)” on page 552

## X-Family Device Serial Numbers

Serial numbers are issued for all registered factory units. The X-Family serial number can be found in the following ways:

- In the Local Security Manager (LSM), on the System Summary page.
- Through the X-Family CLI, using the `show version` command.
- On the bar code sticker, located on the bottom of the device.

## VPN Configuration File

A configuration file is a text file that resides on your network and contains one device CLI command per line. The file is downloaded to the remote device to set up the remote end of the VPN tunnel. For information about X-Family CLI commands, see the TippingPoint X-Family documentation.

## Sample VPN Configuration File

The following sample VPN configuration file, `vpn_config_site_xyz.txt`, has the minimum set of commands that are needed to set up one end of an aggressive mode VPN tunnel.



```

conf t vpn ike local-id domain site_xyz
conf t vpn ike proposal DES-SHA1-PSK aggressive-mode enable
conf t vpn ike proposal DES-SHA1-PSK local-id-type domain
conf t vpn ike proposal DES-SHA1-PSK peer-id-type domain
conf t vpn ike proposal DES-SHA1-PSK auto-connect enable
conf t vpn ipsec add sms
conf t vpn ipsec sa sms key ike proposal DES-SHA1-PSK shared-secret
<shared-secret> peer-id hq
conf t vpn ipsec sa sms peer <vpn_terminator_ext_ip>
conf t vpn ipsec sa sms tunnel remote subnet
<vpn_terminator_internal_subnet> netmask 255.255.255.0
conf t vpn ipsec sa sms tunnel local subnet <site_xyz_internal_subnet>
netmask 255.255.255.0
conf t vpn ipsec sa sms tunnel enable
conf t vpn ipsec sa sms enable
conf t vpn ipsec enable

```

### Important Notes:

- The remote device must be set to the factory defaults.
- The order of the commands is important. For example, the Default SA must not be enabled before the shared-secret has been set because this would result in an error running the config file and the VPN would never come up.
- The central site domain (**hq** in the sample) must be used as the peer-id at all the remote sites but the local-id (**site\_xyz** in the sample) should be unique at each remote site.
- Each remote device needs a unique local subnet which must be different from the internal subnet on the VPN Terminator.
- Each remote device needs a unique local-id which must be different from the local-id on the VPN Terminator.

Table E - 1: VPN Configuration Files - Definitions

Term	Definition
<shared-secret>	Shared secret that is used by all remote devices to communicate to the central site. (8 characters minimum)
<vpn_terminator_ext_ip>	Static host IP Address of the external interface of the VPN Terminator device.
<vpn_terminator_internal_subnet>	Subnet address (for example, 192.168.192.0 for a /24 subnet) of the internal interface on the VPN Terminator that contains the SMS.
<site_xyz_internal_subnet>	Subnet address (for example, 10.10.10.0 for a /24 subnet) of the internal interface on the remote device that will be installed at site xyz.

## Configure SMS for Remote X-Family Device Acquisition and Management

1. From the SMS **Device** navigation pane, select **All Devices** and do one of the following:

- Click **New**.
- From the menu bar, select **File** —> **New** —> **Device**.

The **Devices - New Device** dialog displays.

Figure E - 2: Device - New Device: Remote Acquisition Configuration

The screenshot shows the 'Devices - New Device' dialog box with the following configuration:

- Device Information**
- IP Address:** [Empty text box]
- Username:** topuser
- Password:** [Masked with asterisks]
- Member of Device Group:** All Devices (dropdown menu)
- Synchronize Device Time with SMS
- Online Device
  - Configure the device
  - Clone an existing device:
- Offline XSeries Device
  - Serial Number: 8UJZ999999999
  - Serial Numbers File: [Empty text box] **Browse...**
  - Use a VPN configuration file
  - VPN Configuration File: vpn\_config\_site\_xyz.bd **Browse...**

Buttons: **OK** and **Cancel**

2. Using the offline option, pre-add one or more X-Family devices.



**Note:** After an offline device is added, it cannot be edited. If incorrect information is specified for the offline device, the offline device will need to be deleted and re-added to the SMS.

3. Designate the VPN configuration file to use. See [“Sample VPN Configuration File” on page 550](#).



**Note:** The VPN Terminator (to which SMS is connected) must be pre-configured. For setup requirements, see [“VPN Terminator Setup” on page 553](#).

## VPN Terminator Setup

The VPN Terminator (to which SMS is connected) must be pre-configured for:

- A Virtual Server for the SMS - mapping an external IP address to the internal IP address of the SMS Server.
- Firewall rules and routing etc. to allow “phone home” messages over TCP Port 10043 from the remote device to reach SMS (before the site-to-site VPN has been set up).
- Other end of the site-to-site VPN tunnel.
- If the VPN Terminator is an X-Family device and is to be managed by the SMS, it must be set up for in-band management.

## X-Family Device Setup

After the SMS and VPN Terminator are set up, the X-Family device or devices must be set up. The X-Family device provides two methods for enabling SMS configuration. Both of these methods are described in detail in the *TippingPoint X-Family Command Line Interface Reference*.

### Using the Command Line Interface Setup Wizard

For the X-Family Device to “phone home” to the relevant SMS Server, the setup wizard must be run by typing the “setup” command on the CLI. You will be prompted to enter the IP address of the SMS device that you want to manage the X-Family device. The X-Family device will then initiate a call to the SMS to trigger the acquisition process.

The Command Line Interface (CLI) setup wizard runs when you first configure your X-Family device with the CLI. It can also be accessed at any time with the `setup` command. When prompted by the wizard, indicate that you want to enable SMS configuration for the X-Family device and enter the IP address of the SMS device that you want to manage the X-Family device. The X-Family device will download the SMS configuration from the specified SMS device.

For more information, refer to “Enabling SMS Configuration” in Chapter 1, “X-Family Startup Configuration”, in the *TippingPoint X-Family Command Line Interface Reference*.

### Using the `conf t sms remote-deploy` Command

At any time, you can enable SMS device management with the `conf t sms remote-deploy` X-Family CLI command. This command sets the ip address for the primary SMS and (optional) secondary SMS. When this command is used to set the addresses, the host attempts to contact the SMS.

The `conf t sms no remote-deploy` command turns off remote deployment.

The following table provides command examples.

Table E - 2: X-Family Remote-Deploy Commands

Command	Example	Description
<code>conf t sms remote-deploy &lt;primary&gt; [secondary</code>	<code>conf t sms remote-deploy 1.1.1.1 2.2.2.2</code>	enables a primary SMS and an optional SMS
<code>conf t sms no remote-deploy</code>	<code>conf t sms no remote-deploy</code>	turns off remote deployment

For more information, refer to Chapter 3, “Command Reference”, in the *TippingPoint X-Family Command Line Interface Reference*.

## Device Management

Manage the X-Family device by bringing the devices online. When each device comes online, it contacts the SMS to download the configuration file to establish the required VPN for SMS management.



**Note:** After the configuration file is downloaded to the device, errors in the configuration file can only be corrected using LSM or by deleting and re-adding the offline device with the correct configuration file. You must then re-run the device setup command to initiate the secure connection again.

The SMS client notification dialog displays messages regarding the status of the secure connection between the device and the SMS. Messages provide information that tells when the device:

- contacts the SMS
- starts processing the configuration file,
- has a configuration error

## Device Recovery

This section provides important information about device recovery when certain network and device events occur.

- [“Network Outage” on page 555](#)
- [“X-Family Reboot” on page 555](#)

## Network Outage

When there are network problems that break the communication between the SMS and the X-Family devices, the following configuration ensures that the device is reacquired by the SMS without user intervention.

- VPN Auto-connect configuration— auto-connect/detect peer options in the IKE proposal ensure that the Phase 1 VPN is established
- No X509 certificates

The heartbeat from the SMS will cause the phase 2 to be established. This entire process may take up to minutes to complete. The SMS will then retrieve the information from the X-Family device in the usual manner.

## X-Family Reboot

If the X-Family device reboots after it has already been configured, the device will phone home to the SMS as usual. The SMS then indicates that there is no new information available. At this point, the X-Family device causes the phase 2 VPN to establish a connection as part of the negotiations for the configuration file (even though one is not downloaded).



**Note:** The Phase 1 VPN is established using the method outline in the Network Outage section.



# F Port Information

*The TippingPoint SMS system requires certain ports to be available for it to perform its tasks. You can make other ports available for optional tasks.*

This section includes the following topics:

- [Required Ports](#)
- [TMC Ports](#)
- [Quarantine Ports](#)
- [HA Ports](#)
- [Optional Ports](#)

# Required Ports

The following table lists and describes the ports that you must make available.

Table F - 1: Required Port Availability

Port	Service	From	To	Description
<b>SMS Client Ports</b>				
10042/TCP	SMS	SMS client	SMS server	GUI management of SMS
22/TCP	SSH	SMS client	SMS server	CLI management of SMS
<b>SMS Server Ports</b>				
943/TCP	HTTPS	SMS server	SMS client	SMS restore
161/UDP	SNMP (agent)	SMS server	IPS	SMS management
4043/TCP	HTTPS	SMS server	IPS	SMS management
<b>SMS Client Browser Ports</b>				
443/TCP	HTTPS	SMS client browser	SMS server	file downloads, such as Client installation, exported reports, web services (if configured)
<b>Device Ports</b>				
8162/UDP	SNMP (trap)	IPS	SMS server	SMS traps
8163/UDP	SNMP (trap)	IPS	SMS server	SMS traps



## TMC Ports

The following table lists and describes the TMC ports that you must make available.

Table F - 2: TMC Port Availability

Port	Service	From	To	Description
<b>Required Ports</b>				
80/TCP	HTTP	SMS server	outbound	Digital Vaccine updates from 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.
443/TCP*	HTTPS	SMS server	TMC	Updates from TMC for New SMS installations, this port is the new default for communication with the TMC.
<b>Optional Ports</b>				
80/TCP	HTTP	SMS server	TMC proxy server	TMC updates (TMC proxy server must be configured using the SMS Client)

## Quarantine Ports

The following tables lists and describes the Quarantine ports that you should make available. These ports are determined by the use of Quarantine on SMS. Quarantine (Actions) Port Availability

Port	Service	From	To	Description
80/TCP	HTTP	SMS server	remote host	Quarantine Web action
23/TCP	telnet	SMS server	external switch	Quarantine Switch Disconnect action
1812/UDP	Radius	External switch	SMS server	Radius proxy (required for Quarantine Switch disconnect action)
25/TCP	SMTP	SMS server	mail server	Quarantine Email action
162/UDP	SNMP	SMS server	remote host	Quarantine SNMP action
162/UDP	SNMP	SMS server	remote host	Quarantine NMS action
514/UDP	syslog	SMS server	syslog server	Quarantine Syslog action

Table F - 3: Quarantine (Triggers) Port Availability

Port	Service	From	To	Description
162/UDP	SNMP	NMS server	SMS server	SNMP traps from an SNMP client or NMS server, such as 3Com Network Directory (3ND) to Quarantine
80/TCP	HTTP	External host	SMS server	Trigger Quarantine/unquarantine via URL, IP correlation lookup, IP or MAC lookup
443/TCP	HTTPS	External host	SMS server	Trigger Quarantine/unquarantine via URL, IP correlation lookup, IP or MAC lookup



**Note** Additional ports may need to be opened if they are defined in a Quarantine Action script.

## HA Ports

The following table lists and describes the High Availability ports that you must make available. In addition to these HA ports, all of the ports listed in [Table F - 1. "Required Port Availability." on page 558](#) must be open for both primary and secondary SMS servers.

Table F - 4: HA Port Availability

Port	Service	From	To	Description
22/TCP	SSH	SMS primary	SMS secondary	Secure remote command execution and file replication
		SMS secondary	SMS primary	
10042/TCP	SMS	SMS primary	SMS secondary	CLI command replication
		SMS secondary	SMS primary	
3306/TCP	MySql	SMS primary	SMS secondary	Database 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	
4444/TCP	RMI	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration
		SMS secondary	SMS primary	

# Optional Ports

The following table lists and describes the optional ports that you can make available.

Table F - 5: Optional Port Availability

Port	Service	From	To	Description
<b>SMS Client Port</b>				
23/TCP	Telnet	SMS client	SMS server	CLI
<b>SMS Client Browser Port</b>				
80/TCP	HTTP	SMS client browser	SMS server	file downloads, such as Client installation, exported reports, web services
<b>SMS Server Ports</b>				
123/UDP	NTP	SMS server	NTP server (time source)	time synchronization from external NTP server
53/TCP/UDP	DNS	SMS server	name server	name resolution
137/TCP/UDP	Samba	SMS server	file server	report export, database backup
138/TCP/UDP				
139/TCP/UDP				
1512/TCP/UDP				
2039/TCP/UDP	NFS	SMS server	file server	report export, database backup
111/TCP/UDP				
369/TCP/UDP				
25/TCP	SMTP	SMS server	Mail server	email notifications, such as IPS events, Quarantine
514/UDP	Syslog	SMS server	Syslog server	SMS audit and syslog
1812/UDP	Radius	SMS server	Radius server	SMS user authentication
<b>Device Ports</b>				
123/TCP	NTP	IPS	SMS server	required only if IPS uses SMS for NTP time synchronization
10043/TCP	SMS provision	X-Family device	SMS server	X-Family remote acquisition
<b>SNMP Client Port</b>				
161/UDP	SNMP	SNMP client	SMS server	To query SMS SNMP MIBs



# Glossary

## action set

An integral part of a filter. It includes instructions that control the system response when it encounters matching traffic. The conditions include the following:

- action — the response of the system
  - *permit* — *allow the data*
  - [rate-limiting](#) — *limit the speed of the transferred data/or only allow data of a certain speed?*
  - *block* — *do not allow the data*
- packet trace — the setting for scanning the packet
  - *priority*
  - *verbosity (depth of the scan)*
  - *bytes to capture of the packet/data*
- contacts — systems to receive an alert

## aggregation period

The length of time during which multiple instances of a specific attack can occur before notification is sent to a contact.

## Application Protection

Pillar of filter types that defend against known and unknown 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. These filters detect specific recognition data to recognize an attempted attack and take specific courses of action that you define when an attempt is detected.

## attack protection filter

Filter that scans for, detects, and blocks malicious attacks that try to locate vulnerable areas in your network security. These filters are part of the [Application Protection](#) pillar of filters.

## attack filter

The method by which the IPS identifies malicious or suspicious traffic. It uses packet-level processing of traffic by comparing 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. In addition, it includes a set of instructions, called an [action set](#), that control the system response when matching traffic is encountered.

## attack filter package

A package that contains new filters developed by the [Threat Management Center \(TMC\)](#). Also called Digital Vaccine.

## attack traffic

Packets traversing a network that match at least one [attack filter](#).

## category setting

The default [action set](#) assigned to a particular category of attack filter. Barring any action set customizations, the system responds to an attack filter according to its category setting. These categories include the following:

- **Application Protection** — Pillar of filter types that defend against known and unknown exploits that target applications and operating systems:
  - [attack protection filter](#) — *Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include the following: [vulnerabilities filters](#) and [exploit filters](#).*
  - [security policy filters](#) — *Detect and block traffic that may or may not be malicious. This traffic may be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to your company's security policies.*
  - [reconnaissance filters](#) — *Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include the following: [probes filters](#) and [sweep/scan filters](#).*
  - [informational filters](#) — *Detect and block classic Intrusion Detection System (IDS) infiltration*
- **Infrastructure Protection** — Pillar of filter types that protect network bandwidth and network infrastructure elements such as routers and firewalls from attack using a combination of filter types:
  - [DDoS filters](#) — *Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system.*
  - *Advanced DDoS* — *Detect and block a wider range of DDoS attacks.*
  - [network equipment filters](#) — *Protect networked equipment from attacks*
  - [traffic normalization filters](#) — *Detect and block abnormal or malicious traffic*

- **Performance Protection** — Pillar of filter types that allow key applications to have prioritized bandwidth access setting that ensure mission critical applications have adequate performance during times of high congestion:
  - [misuse and abuse filters](#) — *Protect the resources and usage of file sharing across networks and personal computers. These filters protect peer-to-peer services.*
  - [traffic management filters](#) — *Protect the network by shielding against IP addresses or permitting only a set of IP addresses*

## Classless Inter-Domain Routing (CIDR)

An address format is similar to an IP address except that it is followed by a slash (/) and a specified number of bits. The number of bits indicates the significant bits in the address. In the following example, the IP source address of a packet must match all 32 bits of the IP address specified:

10.3.4.5/32

## Connection Flood Filters

Filters, used with SYN Proxy enabled, that protect against Established Connection floods. The filter 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.

## CPS Flood Filters

Filters that protect against Connection-Per-Second (CPS) floods. The filter limits the maximum rate at which a client may open connections to a protected server. Each filter includes a threshold setting of the calculated average number of connections per second to allow from a particular client.

## custom filter exceptions

Exclude the IP address from receiving the filter. The IP addresses you enter will not have the filter applied.

## Custom Shield Writer (CSW)

An optional, stand-alone, TippingPoint application that lets you write your own custom filters for use on IPS and SMS devices.

## DDoS filters

Denial of Service filters that detect denial of service attacks. These attacks flood a network with requests, including traditional SYN floods, DNS request floods against nameservers, and attempts to use protected systems as reflectors or amplifiers in attacks against third parties. These filters detect direct flood attacks and attacks hidden within larger packets and requests. These filters are part of the [Infrastructure Protection](#) pillar of filters.

## Digital Vaccine

Downloadable update that includes filters for protecting your network system. These filters provide new signature to protect against researched threats to network security. The [Threat Management Center \(TMC\)](#) researches, creates, and distributes these filter packages from the following Web site: <https://tmc.tippingpoint.com>.

## exploit filters

Filters that protect software from malicious attacks across a network by detecting and blocking the request. 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 are part of the [Application Protection](#) pillar of filters.

## filters

Policy of settings and rules for managing and blocking traffic on a network. Each filter includes an [action set](#) that includes instructions for managing data and a [category setting](#). The TMC assesses each attack filter and assigns it to one of the categories.

## informational filters

Filters that provide a means for classic Intrusion Detection System (IDS) testing. An example of these filters includes Blade signatures. These filters are part of the [Application Protection](#) pillar of filters.

## Infrastructure Protection

Pillar of filter types that protect network bandwidth and network infrastructure elements such as routers and firewalls from attacks. These filters use a combination of traffic normalization, DDoS protection, and application, protocol, and statistical anomaly detection. Infrastructure Protection filters include DDoS, reconnaissance, and traffic normalization filters.

## Intrinsic Network High Availability

Protects network availability or security against failures in the host and network processors. User-configurable to block all or permit all packets when in fallback state.

## Intrusion Prevention System (IPS)

The first active network-defense system that provides true intrusion prevention. Based on breakthrough high-speed security processors, TippingPoint becomes part of the network-infrastructure and scours networks at 2 gigabits per second. Unlike intrusion detection systems, TippingPoint continually cleanses Internet and Intranet traffic, identifying and preventing attacks damage to critical resources occurs, ensuring network integrity and ultimately improving return on investment.

## Local Security Manager (LSM)

A web-based management application that provides on-the-box administration, configuration, and reporting for a single [Intrusion Prevention System \(IPS\)](#).



## misuse and abuse filters

Filters that use the same algorithms as attack filters, but which block peer-to-peer protocol traffic. These protocols are primarily used to share music and video files. They essentially turn a personal computer into a file server which make its resources as well as those of its host network available to the peer-to-peer community. These filters protect peer-to-peer services. These filters are part of the [Performance Protection](#) pillar of filters.

## network discovery

The process by which the TippingPoint system monitors the network for changes in the hosts and services. You can use network discovery information to tune filters.

## network equipment filters

Filters that detect and block the malicious attacks that target equipment accessible through a network. Network attacks can broadly or specifically seek access and data to corrupt on a network. These filters are part of the [Infrastructure Protection](#) pillar of filters.

## notification contacts

Recipients of alert messages. These contacts receive an e-mail alert when a filter with the proper notification contacts settings triggers. Contacts include staff with e-mail accounts and the SMS application.

## 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.

## Performance Protection

Pillar of filter types that allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of high congestion. These filters include misuse and abuse and traffic management filters.

## probes filters

Filters that perform scans for vulnerabilities in the system. These filters protect and block probing attacks, protecting access and evaluating requests. These filters are part of the [Application Protection](#) pillar of filters.

## profile

A package that contains your customizations of attack and peer-to-peer filter packages plus new or changed IP filters, action sets, contacts, or category settings. Profiles is a security package of updates that must be distributed to devices for your customizations to take effect. You can create multiple profiles for customizing what updates and customizations are distributed to devices and segment groups.

## rate-limiting

Setting in an action set that 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.

## reconnaissance filters

Filters that monitor for attacks that perform reconnaissance of the network. These attacks search through your network using various methods to locate vulnerabilities. Once the attack has gathered data by probing your system and scanning your network, it continues with pointed attacks against those vulnerabilities. Reconnaissance filters look for these patterns and alert either the LSM or the SMS when an attack is detected. These filters are part of the [Application Protection](#) pillar of filters.

## Security Management System (SMS)

A Linux management server and Java-based client application for managing multiple devices. It provides coordination across your TippingPoint system for administration, configuration, and monitoring, attack filter customization, centralized distribution of upgrades, and enterprise-wide reporting and trend analysis.

## security policy filters

Filters that 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 requiring deployment knowledge and/or operational policy. The [Threat Management Center \(TMC\)](#) develops these filters. These filters are part of the [Application Protection](#) pillar of filters.

## segment

Similar to a subnet. A segment comprises a group of hosts protected through a licensed pair of ports on an IPS.

## shared settings

Globally affect the settings of associated filters. For detailed information, see [“Traffic Management Filters” on page 230](#). These settings include the following:

- IP Address Restrictions — Limits filter to functions for IP addresses entered on the Global Settings screen. You can create restrictions for Application Protection and Performance Protection pillars.
- Global Exceptions — Limits Application Protection filters from protecting or scanning entered IP addresses. In effect, these filters ignore the entered IP addresses.
- Action Sets — Define the trigger settings that determine when to trigger a filter. These sets provide instructions for filters to react to attacks. See [action set](#).
- Notification Contacts — Define recipients of alert messages. Filters have set notification contacts that receive e-mails of alerts and warnings according to settings. See [notification contacts](#).

## sweep/scan filters

Filters that perform port scans and host sweeps to prevent any malicious code, attacks, and exceeded threshold limits for traffic. Each filter scans a specific type of port and protocol to block attacks against ports and hosts. These filters are part of the [Application Protection](#) pillar of filters.

## SYN Proxy Filters

Filters that protect against SYN floods of the system. As default, the system uses firewalls for blocks. SYN floods 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. In the event of a distributed attack with random spoofed source addresses, SYN Proxy filters temporarily block new connections to the server without interfering with existing connections. This option can be manually enabled to a DDoS filter's settings.

## traffic management filters

Filters that react to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values. These filters are specific to segments, while attack filters can be applied to segments or to your entire TippingPoint system. These filters are part of the [Performance Protection](#) pillar of filters.

## traffic normalization filters

Filters that block network traffic when the traffic is considered malicious. 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. These filters are part of the [Infrastructure Protection](#) pillar of filters.

## Threat Management Center (TMC)

A TippingPoint service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters.

## Threat Suppression Engine (TSE)

Blend of Application-Specific Integrated Circuits (ASICs) and network processors to detect unknown threats and anomalies in your network traffic at ultra-high speeds. The TSE scans and reacts to malicious attacks before they become a problem using the latest updates of operating system and Digital Vaccine packages.

## vulnerabilities filters

Filters that detect and block against vulnerabilities in the network. These filters determine if a vulnerability exists based on traffic requests and reaction by services. These filters are part of the [Application Protection](#) pillar of filters.

