

# **SecDevice 10.0.0**

## **Configuration Guide**

**November, 2024**

# Table of Contents

<b>Overview of SecDevice .....</b>	<b>14</b>
Overview .....	15
Features and Benefits .....	15
SecDevice Appliance .....	17
<b>Deployment and Topologies .....</b>	<b>18</b>
Overview .....	19
Zone Deployment Topologies .....	20
Proactive Mitigation (Asymmetric Proactive TPS Deployment Mode) .....	21
Reactive Mitigation with TPS Standalone Detector .....	22
Reactive Mitigation with Third Party Detector .....	24
Connectivity Between SecDevice and TPS .....	25
Open TCP and UDP Ports on SecDevice .....	26
<b>Network Object-based Detection .....</b>	<b>28</b>
Victim IP Identification vs. Network Object-based Detection .....	28
End-to-End Workflow .....	29
<b>Victim IP Identification .....</b>	<b>31</b>
Histogram Indicators .....	31
End-to-End Workflow .....	32
<b>Overview of Protected Objects .....</b>	<b>35</b>
Protected Destination .....	36
Protected Zone .....	36
Source Entries .....	37
Difference Between Protected Destination and Protected Zones .....	38
<b>Initial Setup of SecDevice .....</b>	<b>40</b>
Setup for New SecDevice Owners .....	41
Assign an IP Address to the Management Interface (eth0) .....	42
Enter Basic Network Settings from the Getting Started Wizard .....	43

Enter a License to Activate SecDevice .....	44
Setup for Existing SecDevice Owners .....	46
Consoleadmin .....	46
Backup .....	49
Backup using CLI .....	50
Backup Using GUI .....	52
Backup Setup .....	52
Periodic Backup Setup .....	53
Backup Log .....	54
List of Configuration Files Backed Up .....	54
Restore .....	56
Data Management .....	57
Licensing .....	57
<b>Device Management .....</b>	<b>60</b>
Add Devices .....	61
Configure sFlow .....	61
Device Syslogs .....	62
Configure Detection .....	62
Creating a Device Group .....	64
TPS Required Configuration .....	65
<b>Protected Object - Network Objects .....</b>	<b>67</b>
Prerequisites .....	67
Manage a Network Object .....	68
Creating a Network Object .....	70
<b>Protected Zone Configuration .....</b>	<b>74</b>
Manage a Zone .....	75
Create a Zone .....	77
Performing Bulk Actions on Zones .....	85
Zone Operational Mode .....	87
Operational Mode - Idle .....	88

Operational Mode - Learning .....	88
Operational Mode - Protect .....	90
Zone Templates .....	92
Zone Profiles .....	93
Zone Config Profile .....	93
Manage a Zone Config Profile .....	94
Configure Zone Config Profile .....	95
Zone Service Protection Profile .....	99
Manage a Zone Service Protection Profile .....	99
Configure Zone Service Protection Profile .....	100
Zone Operational Policy .....	107
Manage a Zone Operational Policy .....	107
Configure a Zone Operational Policy .....	108
<b>Attack Detection .....</b>	<b>115</b>
Determining Attack Types .....	116
Zone Incident .....	119
Create a New Incident (Zone) .....	124
Stop a Zone Incident .....	125
Dst Entry Incident .....	126
Creating a new incident .....	128
Configuring Automatic Start and Stop Mitigation for Zones .....	130
<b>Attack Mitigation .....</b>	<b>132</b>
Overview .....	133
Zone Mitigation .....	133
Zero-day Attack Protection .....	133
Zone Mitigation Console .....	135
Graph .....	136
Summary .....	137
Summary .....	137
Live Indicators .....	138

Top Sources .....	139
Top Destination .....	140
Incident Logs .....	141
Zone Alerts .....	142
Flowspec .....	142
BGP Route .....	143
Discovered Services .....	144
Countermeasures .....	145
Global Statistics .....	148
Zone and Zone Services Manual Mode .....	148
Zone Service .....	149
Dst Entry Mitigation .....	153
BGP FlowSpec .....	160
Create a BGP Flowspec .....	163
BGP Route .....	168
Create a BGP Route .....	170
Create a Cloud Mitigation Route .....	172
Initiate Cloud Mitigation .....	173
BGP Route Map .....	174
Create a BGP Route Map .....	175
End of Mitigation .....	177
Remotely Triggered Black Hole .....	177
Cloud Mitigation .....	179
Prerequisite .....	180
Create a Cloud Mitigation Rule .....	180
<b>Monitoring &amp; Reporting .....</b>	<b>182</b>
Reports .....	183
Understanding the Types of Reports .....	183
Viewing the Reports .....	186
Scheduling a Report .....	187

Create a Report Schedule .....	188
Configuring the Report Settings .....	192
<b>Charts .....</b>	<b>194</b>
Zone Charts .....	195
Destination Charts .....	196
Device Charts .....	198
Zone Statistics .....	198
Destination Statistics .....	199
IP Visibility .....	200
Network Object .....	201
Zone .....	201
Packet Capture .....	202
Jobs .....	203
Capture Template .....	207
Capture Policy .....	207
Logging .....	208
Device Logs .....	208
SecDevice Logs .....	209
Events .....	210
<b>Dashboard .....</b>	<b>213</b>
Dashboard Overview .....	214
Threat Protection Services Objects .....	215
Service Protection Status .....	215
Total Mitigator Traffic .....	215
Top Sources .....	216
Current Device Health .....	216
High Traffic Destinations .....	216
Top Attacked Destinations .....	217
Alerts .....	217
Configure Alerts .....	217

System .....	218
Dashboard Customization .....	219
<b>Protected Object - Destination Entries .....</b>	<b>221</b>
Using Search .....	223
Creating a Dst Entry .....	223
<b>Protected Object - Source Entries .....</b>	<b>225</b>
Using Search .....	226
Creating a Source Entry .....	226
<b>Device Management Operations .....</b>	<b>228</b>
Device List .....	229
Device Groups .....	233
Default Credentials .....	235
Creating the Default Credentials .....	235
Updating the Default Credentials .....	237
Deleted Devices .....	238
Device Upgrade .....	239
Uploading an Image .....	239
Upgrading a Device .....	241
Device Configs .....	242
Config Backups .....	245
Device Settings .....	252
Connection .....	253
Device Rescan .....	254
Health Monitor Settings .....	254
sFlow .....	255
Statistics Display .....	256
SSL Management .....	256
SSL Management Local SSL Certs .....	257
SSL Management Device SSL Certs .....	259
CLI / File Objects .....	260

CLI Config Snippets .....	261
A10 Threat Intel .....	263
CLI / File Objects .....	263
Class-Lists .....	264
Source Based Policy .....	266
Configure a Source Based Policy .....	267
Domain-Lists .....	267
Domain Group .....	269
IP Filtering Policy .....	269
Adding a Rule for IP Filtering Policy .....	270
Other System Settings .....	271
Debugging and Support .....	273
<b>TPS Zone Templates .....</b>	<b>274</b>
TCP .....	275
Manage a TCP Template .....	275
Configure a TCP Template .....	276
UDP .....	283
Manage a UDP Template .....	284
Configure a UDP Template .....	285
DNS .....	288
Manage a DNS Template .....	289
Configure a DNS Template .....	290
QUIC .....	295
Manage a QUIC Template .....	296
Configure an QUIC Template .....	297
HTTP .....	298
Manage an HTTP .....	298
Configure an HTTP Template .....	299
General .....	300
Rate Limiting .....	304

Malformed HTTP .....	305
Filter .....	306
SLL-L4 .....	307
Manage an SLL-L4 Template .....	308
Configure an SSL-L4 Template .....	309
ICMP-v4/v6 .....	311
Manage an ICMP-v4/v6 Template .....	311
Configure an ICMP-v4/v6 Template .....	313
IP Proto .....	314
Manage an IP Proto Template .....	315
Configure an IP Proto Template .....	316
Encapsulation .....	317
Manage an Encapsulation Template .....	317
Configure an Encapsulation Template .....	318
SIP .....	319
Manage an SIP Template .....	319
Configure an SIP Template .....	320
Source Port TCP Template .....	323
Manage a Source Port TCP Template .....	323
Configure a Source Port TCP Template .....	324
Source Port UDP Template .....	325
Manage a Source Port UDP Template .....	325
Configure a Source Port UDP Template .....	327
<b>TPS DST Entry Templates .....</b>	<b>329</b>
<b>TPS Other Objects .....</b>	<b>330</b>
GLID .....	331
Configure GLID .....	332
Action Lists .....	334
Logging Template .....	336
Configure a Logging Template .....	337

Violation Actions .....	338
Configure a Violation Action .....	339
Scripts .....	340
<b>Administration .....</b>	<b>343</b>
Scheduler .....	344
Job Execution Results .....	346
Settings .....	347
Network .....	348
Access Management .....	349
Route .....	350
Clock .....	351
Licensing .....	352
SNMP .....	353
Notification .....	356
Notification Events .....	357
Notification Settings .....	358
External Logging .....	359
TPS .....	361
Call Home SERT .....	362
Settings .....	362
Download History .....	363
Web Certificate .....	364
Geo Location .....	364
User Management .....	365
Users .....	367
Roles .....	367
Privileges .....	368
External Authentication Role Mapping .....	368
Privilege Levels for RADIUS and TACACS+ .....	369
RADIUS Configuration .....	369

Setup RADIUS Users .....	370
TACACS Configuration .....	372
LDAP Configuration .....	373
LDAP Authentication .....	374
Authentication Sequence .....	374
Maintenance .....	375
Reboot .....	375
Upgrade .....	375
Backup .....	376
Data Management .....	376
Tech Support .....	376
SecDevice Monitor .....	377
<b>High Availability (HA) .....</b>	<b>379</b>
Prerequisites .....	381
High Availability Setup .....	383
HA Setup Overview .....	384
View High Availability .....	386
Disable High Availability .....	387
Upgrade SecDevice High Availability Pair .....	388
Troubleshoot Common High Availability Issues .....	388
<b>SecDevice + Detector (SecDevice Combo) .....</b>	<b>391</b>
SecDevice Combo Overview .....	392
SecDevice Combo Specifications .....	392
Internal Detector Set Up for SecDevice Combo .....	394
Verify the SecDevice Mode .....	394
Access the Internal TPS Detector .....	395
Configure the TPS Detector .....	396
Upgrading the Internal TPS .....	397
Changing SecDevice Mode .....	397
Using the Detector in an SecDevice + Detector Form Factor .....	399

<b>Troubleshooting .....</b>	<b>400</b>
Recovering from High Availability Failure Events .....	400
Confirming Scheduled Reports .....	401
Failed Report Generation .....	401
Recovering from High Availability Failure Events .....	401
HA Setup Failure .....	401
HA Failure Due to Data Corruption .....	401
Undetected Data Corruption .....	401

# Overview of SecDevice

---

This chapter provides an overview of SecDevice.

The following topics are covered:

<a href="#"><u>Overview</u></a> .....	15
<a href="#"><u>Features and Benefits</u></a> .....	15
<a href="#"><u>SecDevice Appliance</u></a> .....	17

## Overview

The A10 SecDevice® management system is an appliance integrated with the Thunder TPS® (Threat Protection System) for DDoS protection. SecDevice provides centralized management of TPS devices and policies, orchestrates detection and mitigation of DDoS attacks, and delivers a single-pane-of-glass view of the generated reports across all managed Thunder TPS appliances.

SecDevice enables organizations to configure, monitor, and comprehensively analyze their Thunder TPS deployments to view DDoS attacks. System administrators can view DDoS attacks in real-time and enforce policy-centric workflows to granularly regulate traffic and block suspicious activity.

SecDevice provides real-time dashboards that are easy-to-follow and help administrators to monitor the health of protected services and devices, view active incidents, illustrate overall traffic and blocked attacks across geographic locations, identify attack trends, and address compliance risk, and so on.

With the introduction of One DDoS, SecDevice can perform complete automation of DDoS defense, starting from auto-discovery of destination IP addresses and services to continuous baselining of the traffic, distributed detection of DDoS attacks, and automatic mitigation of the attacks.

The SecDevice management system can integrate with third-party DDoS detection systems. When the third-party DDoS detection systems detect attacks, a DDoS attack incident can be created dynamically using northbound RESTful APIs (aGAPI).

## Features and Benefits

SecDevice provides centralized management, monitoring, alerting, reporting, and detecting of global DDoS attacks and defenses.

Table 1 : Features and Benefits of SecDevice

<b>Benefits</b>	<b>Description</b>
Real-time DDOS	<ul style="list-style-type: none"><li>• Empowers enterprises and service providers to surgically distinguish DDoS attackers from valid users</li></ul>

<b>Benefits</b>	<b>Description</b>
Defense Management System	<ul style="list-style-type: none"> <li>Provides a global view to rapidly identify and remediate attacks, and ensures that policies are consistently enforced from a central point</li> <li>Provides the ability to configure, monitor, and comprehensively analyze the Thunder TPS deployments to view DDoS attacks in real time, and drill down to see the details of connections handled by an individual</li> <li>Manages multiple Thunder TPS deployments — across geographic locations — to streamline operations and lower IT operational costs</li> <li>Provides an optional integrated DDoS detector module that supports tightly integrated interworking of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management and robust reporting</li> </ul>
Stops DDoS Attacks	<ul style="list-style-type: none"> <li>Aggregates data from all managed Thunder TPS deployments, providing a rich set of telemetry data to monitor and defeat DDoS attacks</li> <li>Illustrates attacks through a live dashboard and applies all the advanced Thunder TPS features through mitigation templates or creates custom countermeasures instantly</li> <li>Provides an ability to apply policies that can regulate traffic and block suspicious activity</li> </ul>
Simplify Management	<ul style="list-style-type: none"> <li>Streamlines device management, even for organizations with multiple Thunder TPS appliances</li> <li>Manages upgrade software, SSL certificates, and backup and restore configuration files for all of appliances</li> <li>Consolidates all management tasks in one location, making it easy for administrators to apply consistent policies across all devices</li> </ul>
Automatic Service Discovery	<ul style="list-style-type: none"> <li>Auto-discovers services and performs continuous protocol-specific indicator threshold computation for adaptive mitigation.</li> </ul>
Automated	<ul style="list-style-type: none"> <li>Provides fully automated attack detection and mitigation with</li> </ul>

<b>Benefits</b>	<b>Description</b>
Detection and Mitigation	minimal operator intervention.
Maximize IT Agility	<ul style="list-style-type: none"><li>Helps to quickly provision changes, identify issues and roll back configurations when necessary</li></ul>
Report on Attacks and Network Activity	<ul style="list-style-type: none"><li>Offers a variety of summaries, detailed incident reports and real-time dashboards that enable organizations to track security events, identify attack trends and address compliance risk</li><li>Provides a rich set of reports that illustrate overall traffic and blocked attacks by protocol</li></ul>

## SecDevice Appliance

SecDevice is available as an appliance in three different form factors— Physical, Virtual, and SecDevice + Detector combination Physical.

For detailed information about system requirements, see *SecDevice Software Installation Guide*.

For detailed information about SecDevice combo, see [SecDevice + Detector \(SecDevice Combo\)](#)

# Deployment and Topologies

---

This section provides an overview of Detection and the topologies supported for SecDevice. It also provides details about management connectivity between SecDevice and TPS and the list of open ports available for SecDevice.

The following topics are covered:

<a href="#"><u>Overview</u></a>	19
<a href="#"><u>Zone Deployment Topologies</u></a>	20
<a href="#"><u>Connectivity Between SecDevice and TPS</u></a>	25
<a href="#"><u>Open TCP and UDP Ports on SecDevice</u></a>	26

## Overview

The following section provides a high level overview of the steps involved in DDoS mitigation using SecDevice:

1. **Initial setup of SecDevice.** For installation, licensing, and initial setup, refer to [Initial Setup of SecDevice](#).
2. **Initial setup of TPS devices** – Certain configuration steps such as configuring the management interface, DDoS inside and outside interface, interface to export statistics through sFlow to SecDevice, sFlow/NetFlow collector interface in the case of a standalone detector, BGP related configuration have to be done on the TPS devices and upstream router depending on the required topology. Subsequently, all operations can be done solely through SecDevice.
3. **Add TPS devices to SecDevice** – After initial setup of TPS devices is done, add them under SecDevice management and optionally specify the TPS devices that will act as standalone detectors. For more information, see [Add Devices](#).
4. **Create protected objects** – The user may choose destination entry or zone based configuration to protect their services. Note that TPS based detection is supported only for zones and the steps described here are primarily applicable to zone based mitigation. With zone based configuration, a traffic baseline can also be learned to build more accurate threshold rates or ratios for zone mitigation services. You can also perform continuous learning of traffic baseline to determine protocol specific indicator thresholds. For more information, see [Protected Zone Configuration](#).
5. **Create network objects** – The users can choose network object-based detection workflow to detect DDoS attacks on their networks. The TPS standalone detector can automatically detect, profile, and identify attacks at any level of the network object, including active IP subnets, hosts, and services layers. For more information, see [Protected Object - Network Objects](#).
6. **Attack Detection** - An A10 TPS detector or a third party detector examines the traffic using sFlow or NetFlow from the ingress router and compares it against user configured traffic thresholds for each service. For more information, refer to [Attack Detection](#).

7. **Create Incident** - When a threshold is exceeded, the detector informs SecDevice, which creates an incident to act as a trouble ticket for managing the mitigation of the attack and subsequently generating relevant reports. For more information, refer to [Zone Incident](#).
8. **Attack Mitigation** - The user can either manually start mitigation for incidents or have SecDevice automatically start mitigation. As part of mitigation, SecDevice configures the TPS device to send BGP route announcements to divert the traffic for services under attack through the mitigation devices which clean traffic as per configured mitigation rules. For more information, see [Attack Mitigation](#).
9. **End of Mitigation** - The TPS mitigation device will send zone level based escalation and deescalation notifications based on inbound traffic for the service and mitigation rules configured. Once all mitigation devices report to have deescalated to level 0, the user can either manually stop the mitigation or have SecDevice automatically stop it. As part of stopping mitigation, the previously configured BGP route announcement for the service is unconfigured from the mitigator and an incident report is generated. For more information, see [End of Mitigation](#).

## Zone Deployment Topologies

The SecDevice device is used to manage Organization devices that are running A10's Advanced Core Operating System (ACOS).

eth0 of SecDevice appliance is used as the management interface.

The management traffic includes REST API communication between SecDevice and TPS, and syslog messages from TPS to SecDevice.

TPS uses sFlow to send statistics to SecDevice which is used to plot the service graphs. sFlow can be sent through management interface from TPS 3.2.2-P5 or later. **However, it is highly recommended to use the SecDevice data interface to receive sFlow traffic. eth1 (or ethn) is SecDevice's data port(s).**

See [TPS Required Configuration](#) for details on TPS CLI configuration required for communication between TPS and SecDevice.

SecDevice offers the following types of deployment for DDoS mitigation to meet different customer needs:

- [Proactive Mitigation \(Asymmetric Proactive TPS Deployment Mode\)](#)

Deployment with mitigation devices only

- [Reactive Mitigation with TPS Standalone Detector](#)

Deployment with a TPS standalone detector and mitigation devices.

- [Reactive Mitigation with Third Party Detector](#)

Deployment with a third party detector device and mitigation devices.

## Proactive Mitigation (Asymmetric Proactive TPS Deployment Mode)

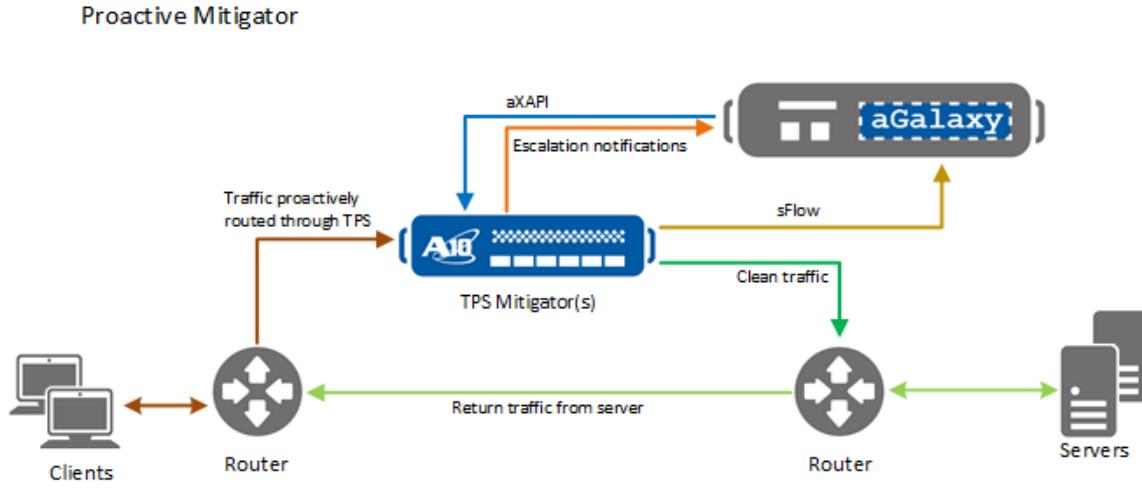
In this deployment, inbound traffic flows through the mitigator(s) at all times. As a proactive solution, the deployment is typically asymmetric. SecDevice is used to configure and monitor zones on TPS mitigator devices.

When inbound traffic exceeds a configured threshold for any zone services, the escalation level will rise to the next configured level. At this point, the mitigator will signal SecDevice through an aGAPI callback. SecDevice will then create an incident and mitigation occurs.

Note: Since traffic flows through the mitigator at all times, the mitigator should first be configured for learning through the operational mode configuration. The learnt parameters will then be pushed back to the mitigator to be used for monitoring.

[Figure 1](#) shows how SecDevice reacts and applies this TPS solution.

Figure 1 : SecDevice Zone Proactive Mitigation

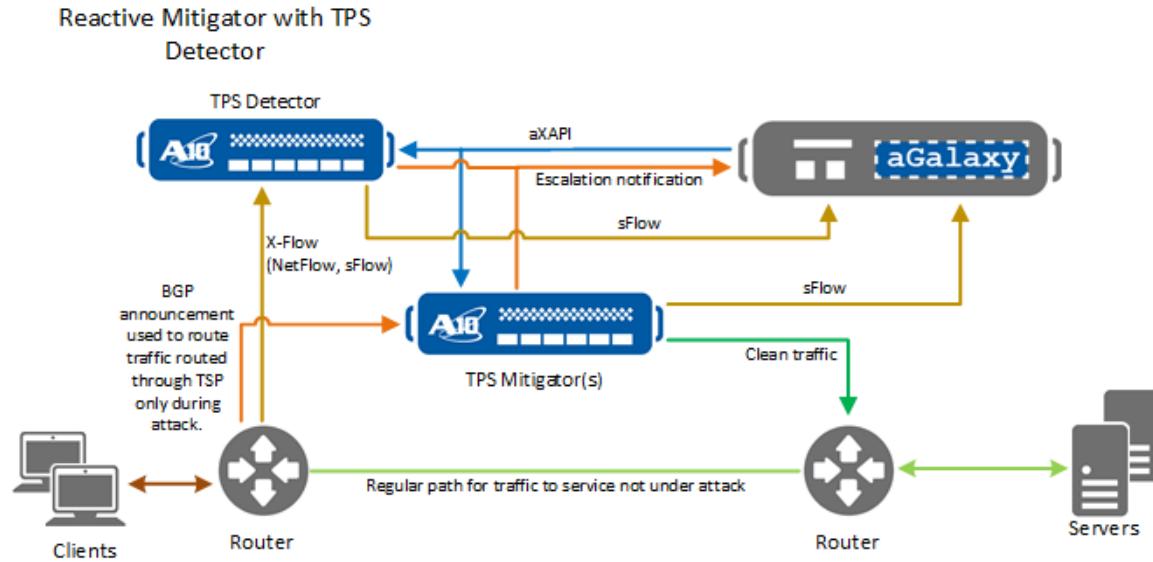


## Reactive Mitigation with TPS Standalone Detector

This reactive asymmetric deployment uses SecDevice to configure and monitor zones and mitigate attacks using Organization TPS standalone detector to detect attacks and TPS mitigator(s) to scrub traffic during attack. The detector can initially be used to learn the traffic baseline for the zone service and then monitor based on the learnt baseline. The detector monitors services using sFlow or NetFlow traffic received from the ingress router(s). Zone traffic is only sent to the mitigator(s) when an attack occurs and mitigation is required.

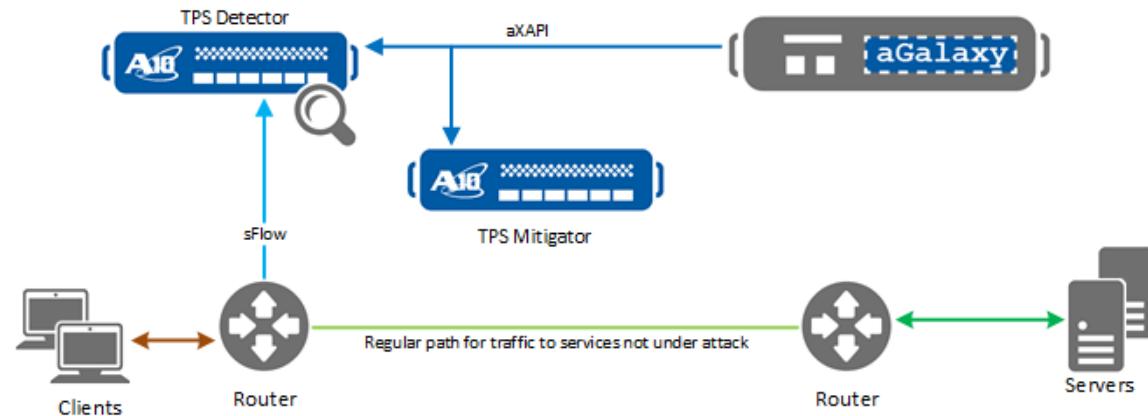
For this deployment, a zone is configured on SecDevice and the zone and zone service list is pushed to both the detector and mitigator(s). Next, the operational mode can be set to learn using the detector. SecDevice then receives the maximum thresholds for the services during the learning period. The user is allowed to edit the thresholds. When completed, the zone service thresholds are pushed to the detector for monitoring. The thresholds are also pushed to the mitigators, but no traffic will flow through them until an incident is triggered. Upon detection of an attack, the detector signals SecDevice through a REST API callback. SecDevice then creates incidents and optionally starts mitigation using the mitigator(s). [Figure 2](#) shows how SecDevice reacts and applies this TPS solution.

Figure 2 : SecDevice Zone Mitigation TPS Mitigator enabled



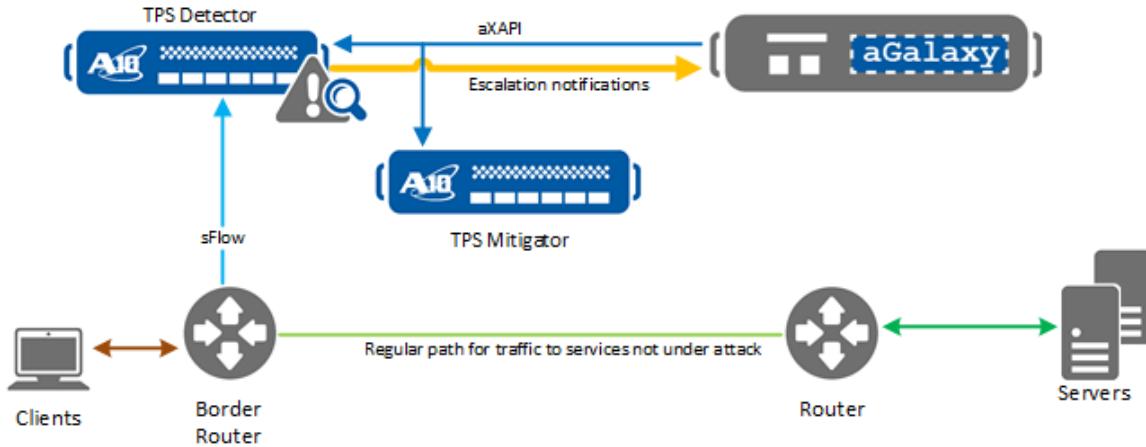
This deployment example uses a reactive mitigator with a detector solution. [Figure 3](#) shows the collection of traffic data through sFlow and communication pathway between the detector, mitigator and SecDevice.

Figure 3 : SecDevice Zone Mitigation Initial Deployment Topology



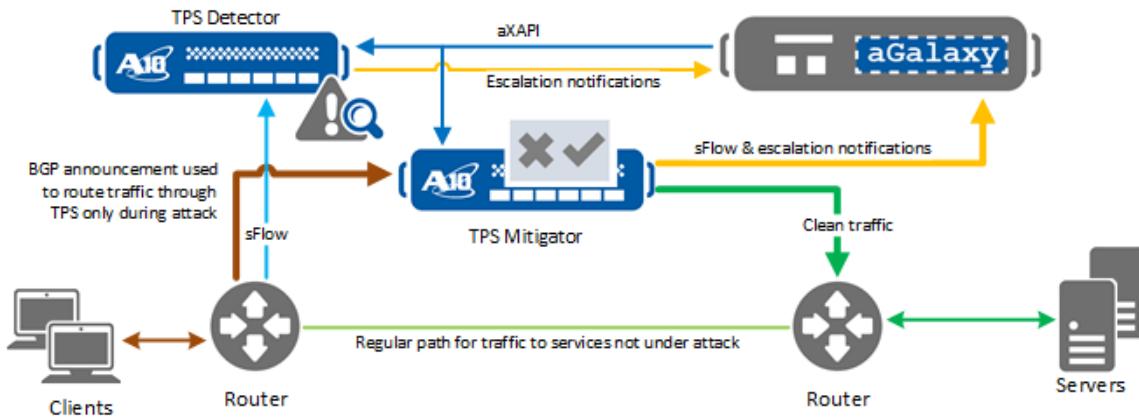
When an attack is detected, an escalation notification is sent to SecDevice. SecDevice creates an incident and the mitigator filters traffic, as shown in [Figure 4](#).

Figure 4 : SecDevice Zone Mitigation Escalation Step 1



[Figure 5](#) shows how SecDevice reacts and applies the TPS solution. sFlow is routed to the mitigator which communicates with SecDevice and also filters traffic based on mitigation policies.

Figure 5 : SecDevice Zone Mitigation Escalation Step 2



## Reactive Mitigation with Third Party Detector

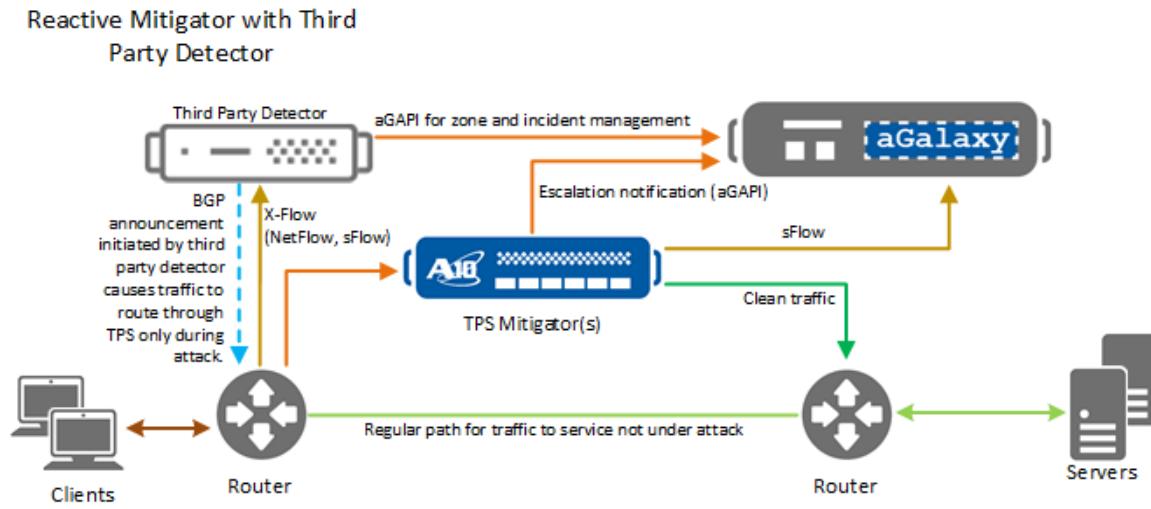
This reactive asymmetric deployment uses SecDevice to configure and monitor zones on TPS mitigator(s) and a third party device is used to detect attacks. Zone traffic is only sent to the mitigator(s) when an attack occurs and mitigation is required.

When an attack occurs, incidents are triggered in one of the following ways:

- The third party detector, through aGAPI, signals SecDevice to create an incident.
- The user manually creates an incident.
- The third party detector uses BGP signaling to route traffic through the TPS mitigator(s). If the attack traffic exceeds the configured threshold levels on any zone services, the TPS mitigator(s) will signal SecDevice through REST API notification callback. When SecDevice receives the escalation notification, SecDevice will create an incident for actual mitigation to occur.

[Figure 6](#) shows how SecDevice reacts and applies the TPS solution.

Figure 6 : SecDevice Zone Mitigation with Third Party Detector



## Connectivity Between SecDevice and TPS

SecDevice communicates with TPS using aXAPI (ACOS REST API). The following communication occurs from a TPS device to SecDevice:

- SYSLOG—sends system logs to SecDevice
- DDoS notification—sends notification using aGAPI (SecDevice REST API)
- sFlow—sends traffic statistics to SecDevice
- SCP—includes files such as backup, class-lists, and others

Typically, all REST API communication, Syslog, and SCP happen over the management network. To send sFlow statistics, it is recommended to use a separate data

interface on the TPS device that is connected to an interface other than eth0 on SecDevice.

The following connectivity options are supported:

1. (Not Recommended) In the following example, the management network is used for aGAPI, aXAPI, SYSLOG, SCP, sFlow. This approach can be used for small-scale set ups only.

Table 2 : Using Management Network Only

<b>SecDevice</b>	<b>TPS</b>	<b>Used For</b>
eth0	Management	aGAPI, aXAPI, SYSLOG, SCP, sFlow

2. (Recommended) In the following example, the management network is used for aGAPI, aXAPI, SYSLOG, and SCP. A data interface such as eth3 that is connected to a different network is used for sFlow configurations.

<b>SecDevice</b>	<b>TPS</b>	<b>Used For</b>
eth0	Management	aGAPI, aXAPI, SYSLOG, SCP
eth2	eth3	sFlow Configurations

3. In the following example, the TPS management interface is not used for any communication. Only the data interfaces such as eth2 is used for aGAPI, aXAPI, SYSLOG, and SCP and eth3 is used for sFlow configurations.

<b>SecDevice</b>	<b>TPS</b>	<b>Used For</b>
eth0	eth2	aGAPI, aXAPI, SYSLOG, SCP
eth2	eth3	sFlow Configurations

## Open TCP and UDP Ports on SecDevice

The following are the TCP and UDP ports that are currently open on SecDevice:

<b>Protocol</b>	<b>Port</b>	<b>Direction</b>	<b>Description</b>
ICMP	N/A	Both	Accessibility to check for responses on network
TCP	22	Both	SSH (SCP of the device configuration backup, upgrades, class-lists, and so on.)
UDP	123	Out	Time synchronization (recommended)
TCP	80	In	Web UI access
UDP	161	In	SNMP statistics and inventory polling
UDP	162	In	Receive SNMP traps from managed devices
TCP	443	In	Web UI access
TCP	443	Out	HTTPS access outbound required to communicate with the TPS devices (AXAPI)
UDP	514	In	ACCEPT SYSLOG messages from managed devices and any source IP added in Administration >> Settings >> Access Management
UDP	6343	In	ACCEPT sFlow data containing metrics from managed devices
TCP	7788	Both	DRBD synchronization (SecDevice HA)
UDP	7800	Both	Pacemaker for cluster messaging (SecDevice HA)
UDP	9996	In	Accept NetFlow Data; Used by detector in the SecDevice + Detector combo appliance

# Network Object-based Detection

---

Network Object-based Detection is supported on TPS Standalone Detector 6.0.2 and later releases. Network Object-based detection provides automated network discovery and attack detection using Netflow telemetry. The TPS standalone detector uses a simplified IP network configuration and automatically detects, profiles, and identifies attacks at any level of the network object, including active IP subnets, hosts, and services layers. Network Object-based Detection supports IPv4 and Netflow v9 and v10 for traffic monitoring.

For detailed information about Network Object-based Detection, see *DDoS Mitigation Guide*.

The following topics are covered:

<a href="#"><u>Victim IP Identification vs. Network Object-based Detection</u></a>	.....	28
<a href="#"><u>End-to-End Workflow</u></a>	.....	29

## Victim IP Identification vs. Network Object-based Detection

You can use either Victim IP Identification or Network Object-based Detection to discover anomalies.

**Victim IP Identification:** Provides zone-based and host attack detection, attack detection using auto-baseline and profiling from traffic indicators and histogram packet classifications, and auto-detection of attacks for IP addresses.

For more details, see [Victim IP Identification](#).

**Network Object-based Detection:** Provides Network Object-based detection and network, subnet, and host attack detection. It auto-discovers and breaks down the network hierarchy, determining active subnets and hosts within the network object. After the network hierarchy discovery, auto-baseline and profiling for victim identification occur at the subnet, host, and per-host service layers, based solely on the network object.

## End-to-End Workflow

The TPS standalone detector uses a simplified IP network configuration and automatically detects, profiles, and identifies attacks at any level of the network object, including active IP subnets, hosts, and services layers. Network object-based detection supports IPv4 networks and Netflow v9 and v10 for traffic monitoring.

For detailed information on how the TPS detector performs network object-based detection and victim service identification, see *DDoS Mitigation Guide*.

The following section describes the automated orchestration and end-to-end workflow using SecDevice:

1. Create a network object with an IPv4 address and with a netmask range from /8 to /16. The TPS detector auto-discovers active subnets, hosts, and services from the network object.

To create a network object, go to **Configurations >> Protected Objects >> Network Objects**. Within the network object, specify the static packet rate, percentage, or per mille threshold to detect and break down a network object into IPv4 subnets. You can also set the percentage threshold to breakdown the service of an IP address based on the services configured under Zone Config Profile. For detailed information on creating a network object, see [Protected Object - Network Objects](#).

When associating a Zone Operational Policy with the network object, it is important to ensure that Zone Oper Policy has the Victim IP option selected under BGP routes. For details on creating a Zone Oper Policy, see [Zone Operational Policy](#).

2. Once the network object is created, the operational mode is set to Learning mode by default. The TPS detector baselines traffic during normal traffic patterns to learn thresholds. After the initial learning period, traffic is continuously monitored for anomalies using network and histogram indicators.
3. When a DDoS attack is detected, a new zone is automatically created with the name format: <network object name\_attack IP subnet>. For example, netobj10\_10\_1\_0\_0\_24. For more information about viewing the newly created zone, see

[\*\*Protected Zone Configuration\*\*](#). The new zone contains the attacked IP address along with the Zone Config Profile and Zone Operational Policy defined for the network object. The zone is then deployed to the TPS mitigator.

4. SecDevice creates a BGP route to redirect the traffic from the attacked IP addresses to the mitigator. The new zone created for the network object is pushed to the TPS mitigator, and the mitigation status is changed to Mitigation. To view the BGP routes created for the attacked IP subnets, go to **Configurations >> BGP >> Route**. For more details on BGP Routes, see [BGP Route](#).
5. When TPS mitigator escalates, TPS notifies SecDevice, and an Incident is generated for the zone associated with the network object. To check the status of the zone incident, go to **Mitigation >> Zone Incident**. For additional information about zone incidents, see [Zone Incident](#).
6. Go to **Monitoring >> logging >> SecDevice Audit Logs** to view all the logs related to IP Anomaly attack detection. For information on SecDevice Audit Logs, see [Monitoring & Reporting](#).
7. If another attack is detected on an IP address that is within the same subnet, the network object zone is updated to include another attacked IP address and the same process of mitigation continues until the attack is stopped.
8. Once the traffic anomaly stops, the TPS detector sends IP Anomaly cleared notification to SecDevice and the following actions are performed:
  - SecDevice removes the BGP Route from the TPS mitigator for the attacked IP address.
  - If it is the last attacked IP address on the network object, SecDevice stops any on-going incidents and the network object is removed from the TPS device.
  - A report is generated for the protected network object. Go to **Monitoring >> Reporting >> Reports >> Reports**, download the report, and under Detector Logs section you can find the detailed information about the IP Anomaly attack.

# Victim IP Identification

---

Victim IP Identification feature is supported on TPS Standalone Detector 6.0.0-P2 and later releases. The feature helps to detect the threshold violations on a per-IP address basis. It uses traffic indicators and packet classification histograms to identify the specific IP address that is under attack within the protected zone and pushes the zone to the mitigator for mitigation. For detailed information about Victim IP Identification feature, see *DDoS Mitigation Guide* for Threat Protection System.

Victim IP Identification provides the following:

- Automatically discover the IP addresses and services such as port and protocol to be monitored.
- Auto-detects specific IP addresses under given subnet that are under attack and redirects the affected traffic to the TPS mitigator for mitigation.
- Perform continuous learning of traffic baseline to determine protocol-specific indicator thresholds.
- Auto-detect DDoS attacks by computing anomalies based on values derived from the indicators.
- Allow the highest accuracy and the shortest time to mitigation.

The traffic indicators help profile network traffic and detect a potential DDoS attack that occurs for the protected zone when the traffic exceeds one of the thresholds. You can set the thresholds for Port Other TCP and Port Other UDP manually.

## Histogram Indicators

Histogram indicators use packet classifications for packets that target zone IP addresses. When victim IP Identification feature is enabled with histogram indicators, histogram thresholds use adaptive auto-learning.

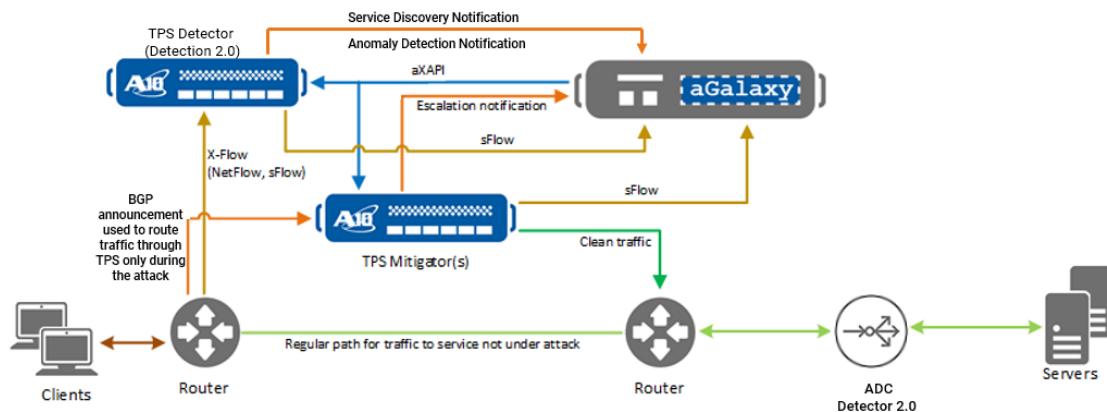
For more details on histogram indicators, see *DDoS Mitigation Guide*.

## End-to-End Workflow

[Figure 7](#) illustrates the end-to-end workflow of DDoS attack and mitigation using Dynamic Baseline Detection. In this deployment example, there are two detectors--TPS standalone and Thunder ADC. The sFlow or NetFlow information from the traffic is sent from the ingress router to the TPS standalone detector. The traffic from the router is also forwarded to the ADC detector.

Figure 7 : : Detector 2.0 Deployment and Workflow

### Reactive Deployment



The following section describes the end-to-end workflow of Dynamic Baseline Detection:

- Adding Devices**—In this deployment example, more than one TPS mitigator is added to SecDevice. The TPS standalone, ADC, or CGN devices can be added as detectors.
- Discovering Services**—A detector examines network traffic and automatically discovers services such as IP addresses, ports, and protocols in the network. The TPS standalone and ADC detectors report IP addresses, ports, and protocols to SecDevice whereas CGN reports only IP addresses. The detector sends information about discovered entities to SecDevice. Once SecDevice receives that information, they are listed under Configuration >> Auto Discovery >> Discovered Entities. For information on viewing discovered entities information, refer to [Auto Discovery](#).

3. **Creating Zones and Zone Services**—For each discovered entities, a zone can be created automatically or manually based on how a detector is configured under Devices >> Devices List >> Details >> Configure Detection. For information on configuring detector, refer to [Setting Up a Detector](#).

If SecDevice is setup to auto-create a zone, the zone and zone service is created automatically. The zone creation policy provides the configuration details required for auto-creating a zone. For information on configuring detector, refer to . Similarly, the zone service creation policy provides the configuration details required for auto-creating a zone service. For information on configuring detector, refer to [Configuring a Zone Service Creation Policy](#).

4. **Detecting a DDoS attack**—Dynamic Baseline Detection applies machine learning algorithms to continuously baseline the traffic and detect an anomaly due to a DDoS attack. The detector notifies SecDevice of the anomaly along with the thresholds SecDevice should use while configuring the zone service in the mitigator. For more information, refer to [Attack Detection](#).

If SecDevice is setup to create an incident automatically, SecDevice creates an incident when anomaly detected notification is received from the detector.

5. **Mitigating a DDoS attack**—SecDevice can start the mitigation manually or automatically based on how the zones in the Zone Operational Policy are configured for auto-start mitigation. At the time of mitigation, the mitigator sends BGP route announcements to divert the traffic for services under attack through the mitigation devices.

During mitigation, the mitigator exports service statistics to SecDevice through sFlow. The mitigator captures dropped packets and analyzes the attack pattern by applying machine learning techniques. The Berkely Packet Filter (BPF) pattern computed is dynamically applied to the attacked service. For more information, refer to [Attack Mitigation](#).

6. **End of Mitigation**—When the attack stops, the detector sends an anomaly cleared notification to SecDevice. Once all mitigation devices report to have de-escalated to level 0, the mitigation is stopped. The mitigation can be stopped manually or automatically based on the Zone Operational Policy configuration. A Zone Operational Policy can also be configured to remove the zone from TPS after the mitigation is stopped. The previously configured BGP route announcement

for the service is also unconfigured from the mitigator and a zone incident report is generated. For more information, refer to [End of Mitigation](#).

# Overview of Protected Objects

---

A protected object is an IP address or IP address/subnet that is either the attacker you want to stop, or the target (servers) you want to protect. Either or both can be defined as a protected object ([Static DDoS \(Protected Objects\)](#)).

IP addresses or subnets defined in one object cannot be re-used in any other object.

The following topics are covered:

<a href="#"><u>Protected Destination</u></a> .....	36
<a href="#"><u>Protected Zone</u></a> .....	36
<a href="#"><u>Source Entries</u></a> .....	37
<a href="#"><u>Difference Between Protected Destination and Protected Zones</u></a> .....	38

## Protected Destination

Protected destination (potential target) objects can be defined using the following:

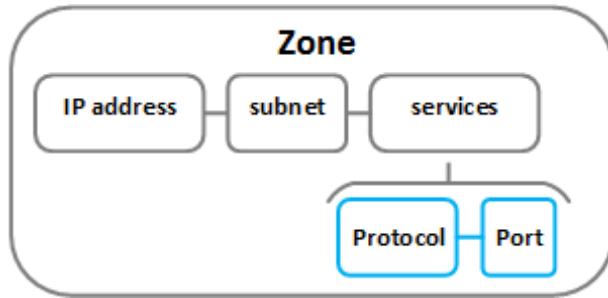
- Host (defining a specific host, also known as a “protected IP”)
- Subnet (defining a specific subnet, also known as a “protected subnet”)
- Default (all traffic not matching either the specified host or subnet)

## Protected Zone

A protected zone is an object comprised of a group of IP addresses and/or subnets, and ports and protocols that provide a service and are protected as a single entity.

[Figure 8](#) shows these basic elements.

Figure 8 : Zone composition



TPS can build a typical traffic rate threshold baseline to facilitate traffic rate limits by examining traffic rate for a zone profile for a set period of time. This is done by configuring “learning” in operational mode. Afterwards, operational mode is used to monitor traffic. See [Zone Operational Mode](#) for more information.

When suspicious behavior occurs, it is possible you may not want to take immediate drastic actions which could be detrimental to the quality of service (QOS) for customers. To address this concern, zones can be configured with escalation levels (up to 5) that allow you to fine tune mitigation actions to be responsive to traffic conditions.

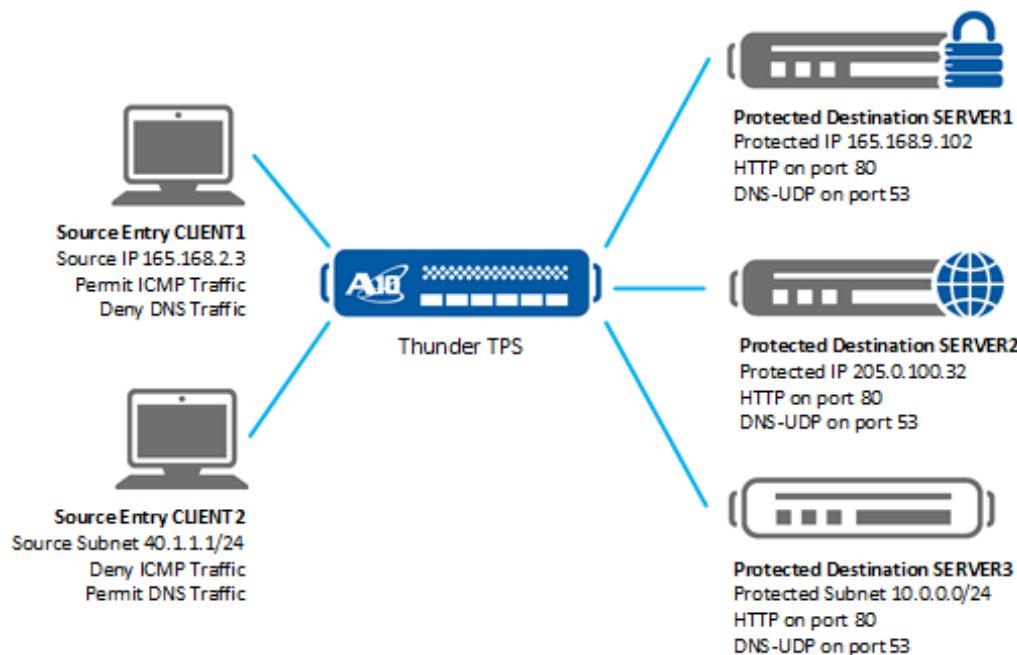
Detection and mitigation, the two primary actions for DDoS mitigation can be handled by one device. When the detector identifies a risk that needs to be mitigated, it creates an incident. Depending on your network, a one device solution may or may not be optimal. An offering of the various types of deployments using SecDevice for device management is shown in [Deployment and Topologies](#).

## Source Entries

Source (potential attacker) objects can be defined using the following:

- Host (defining a specific host, also known as a “source IP”)
- Subnet (defining a specific subnet, also known as a “source subnet”)
- Geographic location (defining a specific geographic location)
- Default (all other traffic not matching the specified host, subnet, or geographic location)

Figure 9 : Static DDoS (Protected Objects)

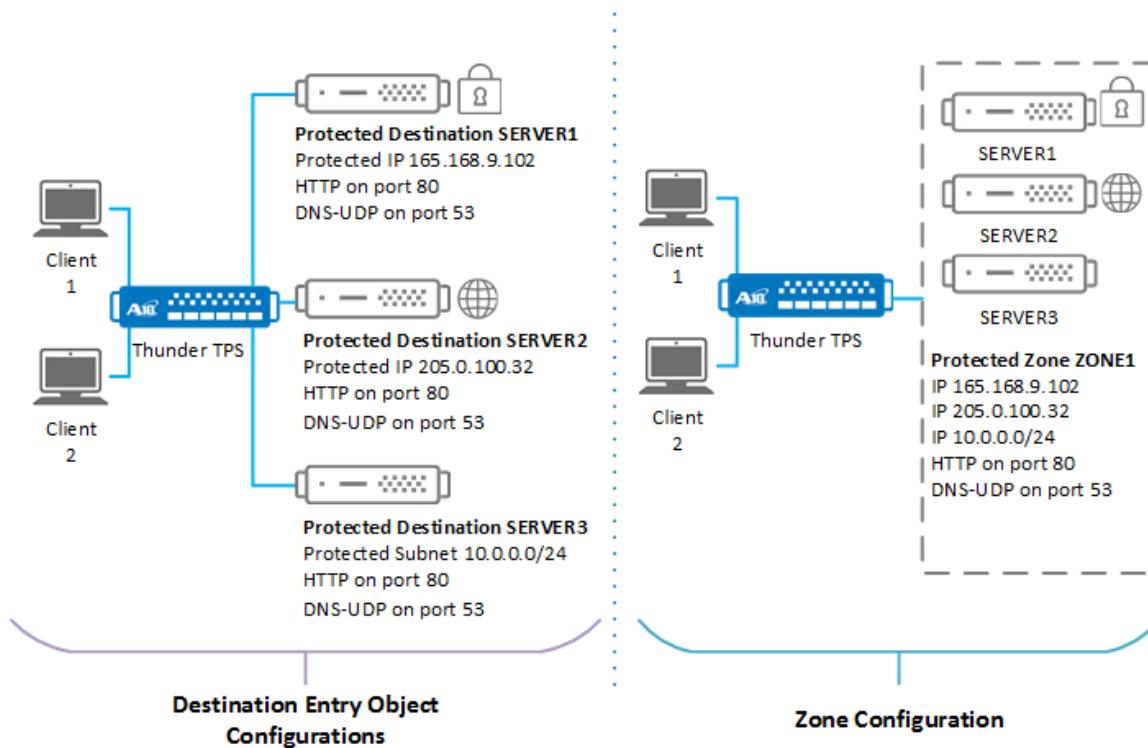


## Difference Between Protected Destination and Protected Zones

Destination differs from a Zone as a projected object in some of the following ways:

- Zones offer mitigation that can be configured to respond to traffic patterns and automatically increase or decrease the mitigation levels as desired.
- Many of the configured objects for zones can be applied to other zones without additional configuration.
- Zones are handled as a group of IPs and/or subnets collectively, providing a service that is protected as a single entity. [Figure 10](#) illustrates the conceptual difference between protected destination entry configuration and zone configuration.
- Automatic learning of traffic pattern is available only for protected zones.

Figure 10 : Destination Entry vs. Zone configuration



What ties a zone together is its profile. After this has been created, zone based templates (TCP, UDP, DNS, HTTP, QUIC, SSL-L4, ICMPv4, ICMPv6, IP Proto,

Encapsulation, Logging, Violation Actions, and SIP) can be created and then bound to the zone profile.

This is different from destination entry configuration in that destination entries have TCP, UDP, Other, HTTP, DNS, ICMPv4, ICMPv6 SSL-L4 and GLID templates that can be configured, but must be bound to the protected destination object through a mitigation template.

While Zones and Destination Entries seem to share common templates, such as TCP, UDP, DNS, etc..., these templates are not interchangeable between Zone and Destination Entries with the exception of GLID templates.

# Initial Setup of SecDevice

---

The Organization SecDevice application enables you to manage multiple Organization devices from a single workstation. The network administrator uses a browser to access the SecDevice device. The administrator can use the SecDevice's GUI interface to manage the Organization devices in the network.

For initial setup of SecDevice virtual appliance, refer to *SecDevice Software Installation Guide*.

The following topics are covered:

<a href="#"><u>Setup for New SecDevice Owners</u></a> .....	41
<a href="#"><u>Setup for Existing SecDevice Owners</u></a> .....	46
<a href="#"><u>Consoleadmin</u></a> .....	46
<a href="#"><u>Backup</u></a> .....	49
<a href="#"><u>Restore</u></a> .....	56
<a href="#"><u>Data Management</u></a> .....	57
<a href="#"><u>Licensing</u></a> .....	57

## Setup for New SecDevice Owners

Before you can use SecDevice for the first time, you must perform the following simple tasks:

- [Assign an IP Address to the Management Interface \(eth0\)](#)
- [Enter Basic Network Settings from the Getting Started Wizard](#)
- [Consoleadmin](#)

A new SecDevice owner must perform a basic setup of SecDevice, configure sFlow and SNMP, and add devices, templates, and configurations to the ACOS appliances.

Perform the following steps to get a new SecDevice owners up and running as soon as possible.

- Configure [sFlow](#)

Configure sFlow to allow SecDevice to collect data from devices.

- Configure [SNMP](#) (Optional)

Configure SNMP to set up the management system.

- Add Devices

Add devices for SecDevice to manage. Refer to [Add Devices](#).

- Add TPS required configuration. [TPS Required Configuration](#)

Add the templates and configurations in this section to your managed ACOS appliances to enable certain SecDevice management features.

Should you need to do any editing after performing the steps above, editing of initial configuration settings can be done through the following:

- [Network](#)

Edit the Hostname, the IPv4 or IPv6 default gateway and interfaces.

- [Route](#)

Configure the static route to SecDevice

- [Clock](#)

Configure the date and time for SecDevice. NTP servers can be configured for this purpose.

- [SNMP](#)

Apply a base license or license add-on

## Assign an IP Address to the Management Interface (eth0)

---

The SecDevice 5000 hardware ships with a default IP assigned to the management interface (eth0). This management interface is not accessible through a web browser until you have assigned a new IP via the **consoleadmin** menu. Therefore, before you can access the GUI wizard shown in [Enter Basic Network Settings from the Getting Started Wizard](#), you must establish an SSH session and set the “eth0” management interface to the IP address of your choice.

Perform the following steps to assign an IP to the management interface:

1. Access SecDevice using a console Telnet session.
2. Log in to the SecDevice console with the following credentials (user: **consoleadmin** / password: **a10**)
3. From here you can configure the network settings.
4. Select menu option <7> Setup Network to change the IP assigned to **eth0**.
5. Next, select menu option <2> Network Interfaces.
6. Next, select menu option <1> **eth0**.
7. Follow the prompts to continue assigning the IP address of your choice to the management interface (**eth0**).
8. You can check your configurations by select option <6> **Show network**.

The output from this will list the IP assigned to the management interface. The output should indicate that the management interface (eth0) has the value of the

new IP you just assigned, and it should no longer show the factory-assigned default IP address (172.31.31.31).

9. After you have verified that the network settings are correct, press Enter to proceed.
10. When you have finished verifying that you correctly assigned the new IP to management interface “eth0”, launch a Web browser and enter the new IP of the management interface in the URL field.
11. You will be asked to enter your log in credentials for the SecDevice device (**admin / a10**).

The **Getting Started** wizard appears. Now you can proceed to [Enter Basic Network Settings from the Getting Started Wizard .](#))

## Enter Basic Network Settings from the Getting Started Wizard

---

Upon first launching SecDevice, the Getting Started page appears. The Getting Started page is a brief wizard that walks you through configuration of basic device settings, such as configuring the IPv4 or IPv6 address, adding an NTP server, setting the system clock, choosing a timezone, as well as setting up the list of device IPs to be discovered.

1. When the Getting Started page first appears, enter the Hostname and default gateway (IPv4 or v6).
2. Configure the NTP servers, if desired.
3. On the Eth0 settings on the right side of the window, specify whether DHCP should be used. If not, then manually enter the IPv4 or IPv6 IP address, as well as the netmask.
4. Click Save to save your initial network configurations.
5. Click **Enter License** to license your device.

---

**NOTE:** You can later update these basic network configurations by navigating to Administration >> Settings and clicking on the appropriate option.

---

## Enter a License to Activate SecDevice

Before you can use the SecDevice system, a device management license must be installed to activate the software. Optionally, a TPS management add-on license can also be installed afterwards for advanced TPS management features. Applying a license can be done through the GUI or through [Consoleadmin](#).

For new SecDevice setting up SecDevice through the Getting Started Wizard, [Figure 11](#) appears.

For existing SecDevice users, go to **Administration >> Settings** and click **Licensing**, and [Initial License Screen](#) appears.

Figure 11 : Initial License Screen

The screenshot shows the 'Initial License Screen' for aGalaxy! Version 3.0.4. The top navigation bar includes 'Getting Started' and 'X'. The main content area has a heading 'Licensing'. Below it, a note says: 'To license your aGalaxy instance go to the [License Manager](#) and get a license for your aGalaxy instance. This aGalaxy's instance UUID and any additional licensing information is listed below. Use the forms at the bottom of this page to input the license text or upload a license file.' A text input field is labeled 'Enter or paste license text into the area below:' with a placeholder 'Paste license text here'. A 'Submit' button is located to the right of the input field. Below the input field, there is a section for uploading a license file with a 'Choose File' button, a 'No file chosen' message, and an 'Upload' button. At the bottom, the 'UUID' is listed as 'e18fbc9c-acec-4134-9a34-9daf61734db6' with a 'Back' button to its right.

1. Go to the License Manager at the following URL:

<https://glm.a10networks.com/>

If not already available, create your account on Organization' License Manager, then sign in.

2. Copy the UUID, which appears at the bottom of the Licensing window. (See [Figure](#)

[11.\)](#)

---

**NOTE:** Note: Be careful to avoid selecting any extra spaces when copying the UUID.

---

3. Paste the UUID text into the License Manager in the appropriate field. The license manager will generate your license token.
4. Return to SecDevice's License page (**Administration>> Settings** and click on **Licensing**) and enter the license using one of the following methods:
  - Copy/Paste—Copy the text of the license (created by the License Manager) and paste it into the blank field.  
Then, click **Submit**.
  - Upload text file—if you saved the license as a text file, you can upload the text file by clicking the **Browse** button, navigating to the text file, and then clicking the **Upload** button. (See [Administration >> Setting >> Licensing](#).) Then, click **Submit**.
5. You can now begin using the SecDevice device to manage your Organization devices.

The base license for SecDevice enables device management functions such as inventorying ACOS devices, performing device upgrades, and backup and restoration of configuration files to devices such as startup configuration, SSL certificates, and class lists.

Starting the release 3.2.2, SecDevice provides enhanced Threat Protection System (TPS) management capabilities and allows for centralized management of device configurations and mitigation against threats. To enable these TPS features, in addition to the base license, an add-on TPS license needs to be procured from the same A10 License Manager. Once this license is installed, the TPS features will become available.

6. Repeat steps 6-9 to update SecDevice with an add-on TPS license.

## Setup for Existing SecDevice Owners

Existing SecDevice owners may wish to review some of the “[Setup for New SecDevice Owners](#)” steps to ensure their existing SecDevice configuration is not missing an important criteria for operation. Perform the following:

- Upgrading SecDevice

To upgrade your SecDevice, see the *SecDevice Release Notes*.

---

**NOTE:** If you are configuring a new SecDevice, refer to the installation guide for the software or hardware installation instructions. For a device upgrade through SecDevice, see the instructions in [Device Upgrade](#).

---

If you have an SecDevice running Threat Protection System (TPS) services, such as mitigation, ensure all mitigations are stopped on any existing incidents prior to performing an upgrade.

- [Enter a License to Activate SecDevice](#)

Refer to this section for applying a base license or an add-on license.

## Consoleadmin

Consoleadmin provides the following functions:

- Change Password - Changes the password for your consoleadmin account.
- Enable support login - Allows support login.
- Disable support login - Removes the ability to have any support accounts.
- Show support login status - Checks whether support login status is enabled or disabled.
- Show services status - Displays the status of various services on SecDevice.
- Show network - Shows the current network configuration.
- Setup Network - Allows you to set up or change network settings.

- Restart SecDevice services - SecDevice will reload services, but data will not be cleared.
- Reboot - SecDevice will clear its data and restart.
- Shutdown - SecDevice will be powered down.
- Upgrade/Backup/Restore/DB Migration- Select to choose one of the following functions:
  - SecDevice Upgrade - Upgrades SecDevice to the next version. For more information about upgrading SecDevice, see SecDevice Release Notes.

---

**NOTE:** SecDevice does not support software downgrade to a previous version.

---

---

**NOTE:** Stop mitigation on all incidents before the upgrade.

---

- SecDevice [Backup](#) - Backs up your existing SecDevice configuration
- SecDevice [Restore](#) - Restores a prior SecDevice backup configuration.
- List current backups - Lists all the current backups
- DB Migrations — SecDevice migrates some data internally among different databases for storage and data retrieval optimization. When there is a large amount of data, the migration might take a very long time and increase the upgrade time. Hence, SecDevice skips the migration and displays a warning message indicating the DB migration is not complete. The user can retrigger the migrations at a later date.:.

---

**NOTE:** Some DB migrations have not completed yet. Please check them under "<11> Upgrade/Backup/Restore/DB Migrations" -> "5 - DB Migrations" menu item.

---

- Switch SecDevice mode - Toggle SecDevice so it functions in one of the following modes:
  - Normal mode - SecDevice runs only as an SecDevice appliance (default).
  - SecDevice+Detector Combo mode - SecDevice functions as both a TPS Detector and an SecDevice appliance.

- Licensing

- SecDevice License - Provide your SecDevice license to enable SecDevice features.

To obtain the device UUID and acquire GLM license:

1. Obtain the UUID for the SecDevice model
2. Acquire your GLM License
3. Provide the License here

To obtain the device UUID and acquire a GLM license information, see Global License Manager guide pertaining to Perpetual Licenses.

- Internal Detector Device License - Provide your detector device license to enable virtual TPS instance.

---

**NOTE:** This is only available on the SecDevice 5000 model.

---

- Reset - Resets SecDevice.

1. Reset user 'admin' to default setting - Allows administrator to reset the user's password to 'a10' (the default value).
2. Reset HA to standalone mode - Configures existing HA setup to operate as a standalone device.
3. Clear ES recovery translog - Attempts recovery of search indexer when performance degradation is caused by index issues.
4. Reset Syslogs - Clears all syslogs on SecDevice. This includes all SLB syslogs, WAF syslogs in addition to device syslogs. This action should not be performed except under the advice of Organization Support.
5. Reset Audit Logs - Clears all audit logs on SecDevice.
6. Reset HBase/Open TSDB - Do not use unless under guidance from A10 support. It will delete all Open TSDB data.
7. Reset Web Certificate - Resets web certificate file when access to GUI is denied.
8. Reset Corosync Resource State - Resets Corosync resource state for recovering the state of out-of-sync HA setup. This option is applicable for HA setups only. Contact TAC before using this option.

9. Reset TPS Zones - Allows administrator to easily delete all the zones in SecDevice database.
  10. Reset Custom Iptables - Under **Access Management** tab in SecDevice, administrator is able to add Iptable rules to block network access from the specific host. This resets the rule if user gets locked out.
  11. Reset Everything! - This will reset SecDevice back to its original factory settings.
- Troubleshooting Options—Provides various tech support options.
    1. Get Techsupport Archive—Allows you to access techsupport archive.
    2. Query TSDB for Zone Incident—Allows you to query TSDB for zone incident.
    3. Ping from SecDevice—Allows you to ping from SecDevice.
    4. Packet capture on SecDevice—Allows you to download pcap via URL enhancement.
    5. Install Verification—Allows you to perform install verification.
  - Quit

## Backup

SecDevice enables you to back up the configuration files by saving them from the database and storing them in the **/a10data/backup** folder or the remote server. You can use the backup file to recover SecDevice database configuration files in case of system failure. You can also use the configuration files to maintain consistent configuration across multiple SecDevice devices. Hence, it becomes prerequisite to backup the SecDevice configuration files.

In addition to triggering backups on a need basis, you can schedule a periodic backup every 12 hours, daily, weekly, and monthly. Periodic backups create directories under **/a10data/backup** with “\_p” as the suffix. For example, 20190617\_330024\_p.

You can securely copy the backup configuration files to a remote server by selecting the **Enable SCP after backup** option in both Backup Setup and Periodic Backup Setup. For the Backup Setup, the original backup files are deleted from the backup

directory. However, for the Periodic Backup Setup, the original files are not deleted immediately. In order to delete the old backup files, you must set up the number of backup rotations using Consoleadmin. For more information about setting up the backup rotation, see [Consoleadmin](#). For example, if you setup 5 rotations, the files older than the past five backup files are deleted.

SecDevice backup files are encrypted. Use the Restore option under consoleadmin to decrypt the backup files and use them for recovering the SecDevice configuration. For more information about the Restore option, see [Restore](#).

You can perform the backup configuration of SecDevice using the CLI or GUI. In this section, the following topics are covered:

- [Backup using CLI](#)
- [Backup Using GUI](#)

## Backup using CLI

---

To perform a backup of SecDevice, log in through the CLI as consoleadmin and perform the following steps:

1. Enter **11** for Upgrade/Backup/Restore and press [Enter] to enter Maintenance Menu.

2. From Maintenance Menu, enter “2” to select SecDevice Backup. The following options are displayed:

- a. Configuration only (RECOMMENDED)

Saves all information listed under Devices (Device List, Device Groups, Device Default Credentials, Deleted Device List).

- b. Configuration with sFlow data

Saves all information under Configurations (Config Backups, Local Configs, and Device Upgrade).

- c. Configuration with syslog and audit log data

Saves local information for TPS which comprises of local SLB objects, local templates, and local SNAT pool information.

- d. Configuration with sFlow, syslog, and audit log data

Saves the following:

- System settings (General, Clock, Connection, Health Monitor, Web and sFlow)
- Scheduler
- Job Execution Results
- User Management
- Email

- e. Configuration with periodic backup

Saves all information listed under Devices (Device List, Device Groups, Device Default Credentials, Deleted Device List).

Choose the following options:

- Option 1—Enables or disables the periodic backup.
- Option 2—Allows you to edit the backup time interval. You can choose every 12 hours, daily, weekly, or monthly.
- Option 3—Enables or Disables Secure Copy Protocol (SCP) to securely transfer backup files to the remote server.
- Option 4—Allows you to configure the host.

It is strongly recommended to use Backup option 1. The length of time taken to perform a backup for options 2, 3, and 4 is substantially high due to the amount of data available for backup.

When the backup file is created successfully, the following message appears:

Successfully created backup files. Press [Enter] to continue.

3. Press [Enter]. The following instructions are displayed:

- a. Enter the remote host where the backup file will be exported to. You must provide the IP address of the remote host and hit [Enter]
- b. Enter the user name on the remote host. You must provide the user name account and hit [Enter]

- c. Enter a destination directory on the remote host location. (The directory must exist). Enter the destination directory. An example would be “/tmp/agalaxy\_backups”.
- d. After completing steps a-c, the SecDevice backup process is done.

## Backup Using GUI

---

You can either trigger backups on a need basis or you can schedule a periodic backup. This section covers the following:

- [Backup Setup](#)
- [Periodic Backup Setup](#)
- [Backup Log](#)
- [List of Configuration Files Backed Up](#)

### Backup Setup

To trigger the backup configuration:

1. Select the appropriate SecDevice backup options from the list:
  - Configuration
  - Incidents
  - Reports
  - Packet Capture
  - Audit Logs
  - Alerts
  - Events
  - Device Logs
  - sFlow

For detailed information about the list of configuration files backed up for each option, see [List of Configuration Files Backed Up](#).

2. To securely transfer the backup files using SCP, select **Enable SCP to remote path after backup**.
3. In the **Host** field, enter the name of the host from where you want to copy the files.
4. In the **Username** field, enter the user name of the host.
5. In the **Password** field, enter the password of the host.
6. In the **Copy to Directory Path** field, enter the path to the directory where you want the files to be copied.
7. (Optional) Click **Test the SSH connection** to test the connection before transferring the files.
8. Click Start Backup to start copying the files to the specified directory path.

## Periodic Backup Setup

To setup the periodic backup:

1. Select **Enable Periodic Backups of Configuration Only** check box.
2. From the Periodic backup time interval drop-down list, select one of the following options:
  - every 12 hours
  - daily
  - weekly
  - monthly
3. By default, the Numbers of backup rotation is setup to 5. You will find information about the disk space of the past average periodic backup and usage for periodic backup.
4. To securely transfer the backup files using SCP, select **Enable SCP to remote path after backup** and enter the appropriate information.
5. (Optional) Click **Test the SSH connection** to test the connection before transferring the files.
6. Click Start Backup to start copying the files to the specified directory path.

## Backup Log

The backup log shows the success messages when the backup of SecDevice configuration files are saved successfully. It also shows any error messages detected at the time of the backup or the periodic backup.

For example,

```
2019-05-16 01:59:00,708 INFO Datetime didn't match periodic configuration,
option = 4
```

```
2019-05-16 02:00:00,439 INFO Periodic backup start
```

## List of Configuration Files Backed Up

[Table 6](#) lists the options and description of the type of configuration backup saved:

Table 6 : Backup Options and Description

Options	Description
Configuration only (RECOMMENDED)	Lite Configuration backup
Configuration with sFlow data	Full Configuration backup, tsdb
Configuration with syslog and audit log data	Full Configuration backup, elasticsearch
Configuration with sFlow, syslog, and audit log data	Full Configuration backup, tsdb, elasticsearch
Configuration with periodic backup	Lite Configuration backup

provides the list of configuration files backed up for the Full Configuration backup and the Lite Configuration backup:

Table 7 : List of Files Backed Up for Full Configuration and Lite Configuration

Files	Path (Defined in agalaxy_share/backup/agalaxy_backup.py)	Full Configuration Backup	Lite Configuration Backup
Release file	/etc/agalaxy/build/Release	Yes	Yes
External device configuration	/a10/agalaxy/device_configuration/device_configuration	Yes	Yes

Table 7 : List of Files Backed Up for Full Configuration and Lite Configuration

Files	Path (Defined in agalaxy_share/backup/agalaxy_backup.py)	Full Configuration Backup	Lite Configuration Backup
External file blob	/a10/agalaxy/device_configuration/file_blob	Yes	Yes
Upgrade image	/a10/agalaxy/device_upgrade/image	Yes	Yes
Saved alert configuration	/a10/agalaxy/saved_alert_configuration.conf	Yes	Yes
Network interface	/etc/network/interfaces	Yes	No
DNS settings	/etc/resolvconf/resolv.conf.d/tail	Yes	No
System settings configuration	/a10/agalaxy/system	Yes	Yes
Device connectivity settings	/a10/agalaxy/inventory/discovery_list.conf	Yes	Yes
Backup configuration	/a10/agalaxy/share/backup.conf	Yes	Yes

[Table 8](#) provides the list of configuration files backed up in mariadb databases for Full Configuration backup and the Lite Configuration backup:

Table 8 : List of Files Backed Up for Full Configuration and Lite Configuration

Files	Full Configuration Backup	Lite Configuration Backup
aGalaxyUI	Yes	Yes
adc	Yes	Yes
agapi	Yes	Yes

Table 8 : List of Files Backed Up for Full Configuration and Lite Configuration

Files	Full Configuration Backup	Lite Configuration Backup
alarm	Yes	Yes
basicinv	Yes	No
callhome	Yes	No
device_configuration	Yes	Yes
device_upgrade	Yes	Yes
event	Yes	Yes
information_schema	Yes	No
keystone	Yes	Yes
mail	Yes	Yes
mysql	No	No
packet_capture	Yes	No
performance_schema	No	No
reports	Yes	No
scheduler	Yes	Yes
stats_manager	Yes	Yes
tps	Yes	Yes
tps2	Yes	Yes
tps_incident	Yes	Yes

## Restore

Performing a restore operation will result in service being down during the process.

Before restoring a backup to SecDevice, ensure the following:

- The current SecDevice must have the same license type.
- The current SecDevice must have a license quota that is equal to, or greater than the backup.
- The current SecDevice must have the same release version as the backup.

## Data Management

Data Management allows you to clean up alerts, audit logs, device logs, and events. It shows the size of “other” files to maintain sufficient disk space on /a10data. To ensure optimal performance, it is recommended to delete unnecessary files and keep only the required number of files.

Data Management provides a list of major categories and the disk space used by each category. On clicking a category, you can further view sections of each category broken down by date and the disk space used. You can either delete a section that is consuming more space or perform disk rotation. Disk rotation helps to retain the latest files and remove the old files.

To perform data rotation:

1. Go to **Administration >> Maintenance >> Data Management**.
2. Select **Data Rotation**.
3. In **Keep the latest**, enter the number of months of data files to be maintained in the system. You can enter from 1 to 60 months. For example, if you specify 12 months, the files older than 12 months are deleted from the system.

---

**NOTE:** For Audit and Device logs from earlier releases (SecDevice 5.0.6 and earlier), the data rotation is performed based on the size.

---

## Licensing

Before you can use SecDevice, you must enter a license to activate the software. To get the license, you must copy the UUID from the SecDevice Licensing page, create an account with A10’s license manager, enter the UUID into the license manager, and this will create your license. Then, upload this license into SecDevice’s Licensing page.

To access this page, navigate to Administration >> Setting and click on Licensing.

1. Create or access your account on Organization' License Manager at the following URL:

[https://glm.a10networks.com/wizard/glm\\_welcome/create\\_account](https://glm.a10networks.com/wizard/glm_welcome/create_account)

- If you already have an account, click **Log into Your Account**.
- If you do not have an account, click **Register an Account**.

---

<b>NOTE:</b>	An account should have been created for you, so confirm before creating one.
--------------	--

---

2. Once you have set up an account, copy the UUID (see bottom of [Administration >> Setting >> Licensing](#) below) and paste the UUID into the License Manager. The license manager will generate your license token.

---

<b>NOTE:</b>	Take care not to include any extra spaces when inputting this value.
--------------	--

---

3. Return to SecDevice's License page by navigating as follows: Select **Administration >> Settings and click on Licensing**.

### Administration >> Setting >> Licensing

1. Click the License Manager link and go to your account. (This is required to obtain a license token.)

UUID 00cf204a-520a-4323-a23e-555a8ff23594

2. Copy the UUID here and enter it into the License Manager.

3. Once the License Manager creates the license token, upload it here.

4. Enter the license. There are two ways to do so:

- Upload text file—If the license is saved as a text file, you can click the **Browse** button, navigate to the text file, and then click the **Upload** button.
- Copy/Paste—Copy the text of the license and paste it into the blank field.

Then, click **Submit** button.

---

**NOTE:** Only mitigators count against the Max Devices License Limit. The detectors are not counted.

---

5. Click **Submit**.

# Device Management

---

Devices that act as a Detector or TPS Mitigation devices must be set up under SecDevice management.

The following topics are covered:

<a href="#"><u>Add Devices</u></a> .....	61
<a href="#"><u>Configure sFlow</u></a> .....	61
<a href="#"><u>Device Syslogs</u></a> .....	62
<a href="#"><u>Configure Detection</u></a> .....	62
<a href="#"><u>Creating a Device Group</u></a> .....	64
<a href="#"><u>TPS Required Configuration</u></a> .....	65

## Add Devices

Perform the following steps to add devices.

1. Log in to SecDevice.
2. Go to **Devices >> Device List**. The Device List page displays a list of ACOS devices that are currently being managed by SecDevice.
3. Click **Add Devices**. The Add Device page is displayed.
4. In the IP Address field, enter the IP address or host name.
5. In the Username IP field, enter the username for accessing the device.
6. In the Password field, enter the password associated with the username.
7. From the Designate Device as drop-down list, select the options to designate the device as a mitigator or a detector.

---

**NOTE:** Only mitigators count against the Max Devices License Limit. The detectors are not counted.

---

8. Click **Submit**.

## Configure sFlow

The sFlow page allows you to set up SecDevice as an sFlow collector, with the managed devices sampling random packets and sending statistics in an sFlow datagram to SecDevice for analysis.

Go to **Devices >> Device Settings**, and click on sFlow.

To configure sFlow, do the following:

1. Click the sFlow Collector IP icon and select the IP address to be used as an sFlow collector in the Pick an IP window, or enter an IP address manually in the sFlow Collector IP field.

2. Enter the Polling Interval value for sFlow collection.
3. Click **Save** to finish.

**NOTE:** When an sFlow's IP is changed, it is updated to all managed devices. In order to remove the configuration, input 0.0.0.0 in the sFlow Collector IP field, as 0.0.0.0 is recognized to push SecDevice's management interface address (for example, eth0's IPv4 address) to devices as the sFlow collector IP.

---

## Device Syslogs

A managed device is configured to send control plane syslogs to SecDevice when it is first discovered. Once configured, SecDevice acts as an external syslog receiver for ACOS devices.

## Configure Detection

To configure a detector, do the following:

1. Go to **Devices >> Device List**.
2. For the TPS device that you wish to configure as a detector, under **Actions**, click **Details** and select **Configure Detection**.

Figure 12 : Configure Detection

The screenshot shows the 'Configure Detection' interface. At the top, there's a breadcrumb navigation: Devices >> Device List >> Configure Detection. Below it, the 'General Settings' section displays the device name as 'vThunder164 ( 10.16.27.164 )' and the 'Detector Type' as 'Unified Detector'. The 'Detector xFlow Settings' section contains fields for 'sFlow Receiving Port' (1-65535), 'NetFlow Receiving Port' (1-65535), 'Detection Window Size' (15), and 'Initial Learning Interval' (1-168 (in hours)). A table titled 'Remote Agents' lists two entries: 'edge-router-cisco-asr1k' with IP 17.17.17.36 and 'edge-router-ax2600' with IP 17.17.17.8. Both rows have checkboxes for 'sFlow' and 'Netflow' checked, and a sampling rate of 1. There are 'Cancel' and 'Submit' buttons at the bottom.

## General Settings

Under General Settings, the name of the device and detector type is displayed by default.

## Detector xFlow Settings

Table 9 : Information on Detector xFlow Settings

Field	Purpose
<b>sFlow Receiving Port</b>	Enter a port that is used to receive the sFlow traffic which needs to be monitored.
<b>NetFlow Receiving Port</b>	Enter a port that is used to receive NetFlow traffic which needs to be monitored.
<b>Detection Window Size</b>	Enter an xFlow sample receiving interval.

Table 9 : Information on Detector xFlow Settings

Field	Purpose
Initial Learning Interval	Enter an initial learning period to understand the traffic patterns.

- Add the Remote Agents information to determine the routers from where xFlow samples are sent. Click + and add the following information:

Table 10 : Information on Remote Agents

Field	Purpose
Agent name	Enter the name of the router. For example, edge-router-ax2500.
IP Address	Enter the IP address of the router.
sFlow	Select the flow technology that the detector supports.
Netflow	Select the flow technology that the detector supports.
<b>Netflow Sampling Rate</b>	If Netflow is selected as the flow technology, set the sampling rate of packets. For example, if the sampling rate is 1, every packet is sampled for the detection process.

- Click **Submit**.

## Creating a Device Group

Using Device Groups, you can create a mitigator group or a detector group.

To create a device group:

- From the **Devices >> Device Groups** page, click + Create to create a device group.
- In the **Group Name** box, enter a name of the device group.
- From Device(s), select the devices with which you want to create a device group.
- In the Description box, enter a description for the device group.
- From the Use device-group as: drop-down list, select the appropriate option.
- Click **Submit**.

## TPS Required Configuration

When the device is added to SecDevice, SecDevice pushes the following configuration to TPS to receive sFlow, escalation and de-escalation notifications, and syslogs:

```
ddos protection enable
```

```
!
```

```
ddos notification-template notify-agalaxy
```

```
api
```

```
host-ipv4-address x.x.x.x <-- SecDevice mgmt interface address to receive notifications
```

```
relative-uri /agapi/v1/ddos/notification/
```

```
authentication
```

```
relative-login-uri /agapi/auth/login/
```

```
relative-logoff-uri /agapi/auth/logout/
```

```
auth-username _notifyadmin
```

```
auth-password encrypted
```

```
ycS3t8e49gTaxCXkOddHtp4yitlBAGyDPBCMuNXbAOc8Ely41dsA5zwQjLjV2wDn
```

```
!
```

```
ddos notification-template-common
```

```
default-template notify-agalaxy
```

```
!
```

```
logging host x.x.x.x use-mgmt-port <-- SecDevice mgmt interface address to receive syslog
```

```
!
```

```
route-map A10-SET-NEXT-HOP permit 1
```

```
!
```

```
sflow setting counter-polling-interval 15  
sflow setting local-collection disable  
sflow collector ip x.x.x.x 6343 use-mgmt-port <-- SecDevice mgmt interface address to receive sflow  
sflow collector ip x.x.x.x 6343 <-- SecDevice data interface address to receive sflow  
sflow agent address y.y.y.y <-- set sFlow packet source IP = TPS mgmt interface address  
sflow polling ddos enable  
sflow polling ddos enable-anomaly-stats
```

---

**NOTE:** For 3.2.1-P1 devices, instead of `sflow polling ddos enable`, enter the following command: `sflow polling ddos enable 3_0-compatibility`

---

For TPS 3.2.2-P2 and up, SecDevice configures “a10-proprietary-polling” under an sflow collector entry as follows:

```
sflow collector ip x.x.x.x 6343 <-- SecDevice data interface address to receive sflow  
customized-setting export  
a10-proprietary-polling
```

# Protected Object - Network Objects

---

Network Object-based Detection is supported on TPS Standalone Detector 6.0.2 and later releases. Network Object-based Detection provides automated network discovery and attack detection using Netflow telemetry. The TPS standalone detector uses a simplified IP network configuration and automatically detects, profiles, and identifies attacks at any level of the network object, including active IP subnets, hosts, and services layers. Network Object-based Detection supports IPv4 and Netflow v9 and v10 for traffic monitoring.

Network Object-based Detection provides the following:

- Auto-discovers active subnets, hosts, and services from the network object.
- The network object address for IPv4 can use /8 to /31 netmask range and detect subnets in the subnet masks /16, /24, and /32 for hosts.

For detailed information about Network Object-based Detection, see *DDoS Mitigation Guide*.

The following topics are covered:

<a href="#">Prerequisites</a> .....	67
<a href="#">Manage a Network Object</a> .....	68
<a href="#">Creating a Network Object</a> .....	70

## Prerequisites

To create a new Network Object, make sure that you have completed the following steps:

- Create a Detector Group and a Mitigator Group.

To know how to create a Detector Group and a Mitigator Group, see [Device Groups](#).

- Configure a Zone Config Profile. It is recommended to configure Port Other TCP

and Port Other UDP indicators. The thresholds mentioned in the protection profile for these services are used for mitigation.

To know how to create a Zone Config Profile, see [Zone Config Profile](#).

- Configure a Zone Operational Policy and select the Victim IP option under BGP Routes to detect the threshold violations on a per-IP address basis.

To know how to create Zone Operational Policy, see [Zone Operational Policy](#).

## Manage a Network Object

Perform the following steps to access the Network Object page:

- Go to **Configurations >> Protected Objects >> Network Objects**.
- (Optional) Click to perform any of the following actions:

Action	Purpose
Reset	Resets the search filter on the network objects.
Refresh	Refreshes the information displayed for the Network Object page.
+Add New	Configures a new Network Object.
Bulk Actions	Allows you to perform actions on multiple zones at once, see <a href="#">Performing Bulk Actions on Zones</a> .

Table 12 : Describes the network object page configuration.

Column heading	Description
Name	Displays the name of the network object.
IP/Subnet	Displays the IP address and subnet information of the network object.
Detector Group	Displays the device or device set that acts as a detector or a detector group for the network object.
Oper. Mode	Displays the operational mode the network object is under currently (Idle, Learn, Protect). To edit the Oper. Mode, click the edit icon and select the appropriate option. For more information on Oper. Mode,

Column heading	Description
	<p>see <a href="#">Zone Operational Mode</a>.</p> <ul style="list-style-type: none"> <li>• <b>Idle</b>—Click the icon to set Operational Mode to Idle, where CPU resources are not utilized for a network object.</li> <li>• <b>Learn</b>—Click the icon to set Operational Mode to Learn, where traffic baseline values will be established for a network object that can be used to create thresholds.</li> <li>• <b>Protect</b>—Click the icon to set Operational Mode to Monitor, to enable detection.</li> </ul> <p>A confirmation message is displayed, click OK to change the Oper. Mode. The Oper. Mode is updated accordingly.</p>
<b>Oper. Status</b>	<p>Displays the operational status of the network object. The status can be as follows:</p> <ul style="list-style-type: none"> <li>• <b>OK</b>—Indicates the status is normal.</li> <li>• <b>Unknown</b>—Indicates the status cannot be determined at the current time.</li> <li>• <b>Out of Sync</b>—Indicates the changes on SecDevice are not yet synchronized with the device(s).</li> <li>• <b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the network object(s).</li> <li>• <b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the network object(s).</li> </ul>
<b>Actions</b>	<p>Click the link in the Actions column to perform any of the following :</p> <ul style="list-style-type: none"> <li>• <b>Edit</b>—Allows you to modify one of the previously-configured detection network object.</li> <li>• <b>Sync to Device</b>—Allows you to push the current network object configuration (along with profile configuration, oper policy configuration, and associated BGP objects) to the device group. Once the network object is pushed successfully to the device group, the status is updated. Go to <b>Administration &gt;&gt; Scheduler</b></li> </ul>

Column heading	Description
	<p>or <b>Job Execution Results</b> to view the job execution status and results.</p> <ul style="list-style-type: none"> <li>• <b>Delete</b>—Allows you to delete the current network object.</li> </ul>

Network Objects can be searched based on the network object name or IP address. The search can be filtered based on the following.

- Detector Group
- Mitigation Group
- Mitigation Status
- Oper. Status

## Creating a Network Object

Perform the following steps to create a new Network Object:

1. Navigate to **Configurations > Protected Objects > Network Objects**.
2. On the **Network Objects** page, click **+Add New**.
3. In the **Network Object Name** field, enter a network object name.
4. In the **IP Address** field, enter IP addresses.

You can add only up to 10 IPv4 subnets in the range of /8 to /31 networks for detection.

5. In the **Mitigation** section, specify the type of zone for mitigation.
  - **Use Pre-configured Zones:** By selecting Pre-configured Zones option for Victim IP Mitigation Zone, SecDevice will try to match the anomaly detected IP/subnet with pre-configured zone's IP list. When SecDevice receives anomaly detection notification from the Detector, SecDevice searches for the zone with the closest match for the victim IP/subnet and deploys that zone to the mitigator in addition to configuring the BGP route for the victim IP/subnet to start mitigation. If SecDevice does not find a matching zone, it logs a message and

skips mitigation.

---

**NOTE:** The Victim IP option must be enabled under Zone Operational Policy to apply Use Pre-configured Zones.

---

- **Dynamically Create Zones:** By selecting Dynamically Create Zones option for Victim IP Mitigation Zone, SecDevice dynamically creates a zone using anomaly detected IP and deploys it to the mitigator group. SecDevice also configures BGP route for the anomaly detected IP/subnet. For this option to work, Zone Config Profile, Zone Operational Policy, and Mitigator Group must be specified. SecDevice will use these options to configure the zone.

---

**NOTE:** The Victim IP option must be enabled under Zone Operational Policy to apply Dynamically Create Zones.

---

- **No Mitigation (Detection Only):** When No Mitigation (Detection Only) is selected for Victim IP Mitigation Zone, SecDevice only logs the anomaly detected notifications from the detector and takes no mitigation action.

6. In the **Detection** section, select a detector group.
7. In the **Top K Destination** section, enter the top-k destination between 1-100.
8. In the **Sort By** section, select either **Max peak** or **Average** rate for the IP detection.
9. In the **Auto Discovery Configuration** section, select the thresholds for auto breakdown, service breakdown, and other fields. However, they are optional.
  - For **Auto Breakdown Threshold Type**, select one of the following options: Relative Percentage or Static Packet Rate.
    - **Relative Percentage:** When Relative Percentage is selected, the detection mechanism used by the TPS detector breaks down the subnets based on specified percentage in the **Percentage of Each Subnet Layer** and **Permil of Network Object** fields.
    - **Percentage of Each Subnet Layer:** Specify 1 per 1000 value for **Percentage of Each Subnet Layer**. The default value is 10.

- **Permit of Network Object:** Specify a value between 1 – 999 for **Permit of Network Object**. The default value is 1.
  - **Static Packet Rate:** When Static Packet Rate is selected, the detection mechanism used by the TPS detector uses the value specified in the “Packet Rate” field to break down the subnets in the network object into /16, /24, /32 netmask subnets.
  - Under **Service Breakdown Threshold Local Percentage**, enter the percentage threshold to break down the service of an IP address. This service breakdown from IP addresses to services starts with the detection of general protocols such as **TCP other**, **UDP other**, or **ICMP**.
- Select the **Enable Service Port Discovery** checkbox to enable the TPS detector to do service discovery.
  - Select the **Enable Source Port Discovery** checkbox to enable the TPS detector to do source discovery.
10. Under **Threshold Configuration**, configure the detection scope for network object and subnetworks. The anomalies are discovered based on the packet rate (pps) and bit rate (bps) thresholds.
  11. In the **Histogram** section, select either **Observe**, **Monitor**, or **Off** for the histogram thresholds. Histogram indicators use packet classifications for packets that target network objects such as subnets, hosts (IP addresses), and services. Histogram indicators profile traffic at all levels of the network object to learn traffic flow patterns and thresholds.
  12. In the **Threshold Sensitivity** section, select sensitivity level for the incoming traffic as **Low**, **Medium**, or **High**. If this threshold is not required, you can keep this option as **Off**.
  13. In the **Flooding Multiplier** field, set a value between 2-10.
  14. For the **Detection Scope**, set the packet-rate and bit-rate for **Network Anomaly Threshold** and **Per Host Anomaly Threshold**.
    - **Network Anomaly Threshold:** Set the packet-rate value between 1-10995116277760 and bit-rate between 800-87960930222080.
    - **Per Host Anomaly Threshold:** Set the packet-rate value between 1-2147483647 and bit-rate between 800-34359738360

15. Under the **Subnetwork Configuration** section, enter a **Subnet IP** and **Subnet Breakdown** value between 25-31 and then set the packet-rate and bit-rate thresholds for Subnet Anomaly Threshold, Anomaly Threshold, and Breakdown Subnet Threshold.
  - **Subnet Anomaly Threshold:** Set the packet-rate value between 1-2147483647 and bit-rate value between 800-34359738360.
  - **Anomaly Threshold:** Set the packet-rate value between 1-2147483647 and bit-rate value between 800-34359738360.
  - **Breakdown Subnet Threshold:** Set the packet-rate value between 1-2147483647 and bit-rate value between 800-34359738360.
16. Select **Trigger Anomaly on Static Thresholds Only** to trigger on the static thresholds.
17. To save and deploy the network object to the detectors, click **Save & Push**.

The TPS detector starts learning the thresholds for the subnets in the Network Object.

The detector detects an attack on any IP within subnets of the network object and notifies SecDevice of the victim IP. SecDevice starts the mitigation process for that victim IP based on the configuration specified in the mitigation section of the Network Object.

To know the complete end-to-end workflow of Network Object-based Detection, see [End-to-End Workflow](#).

For more information about Network Objects, see DDoS Mitigation Guide.

# Protected Zone Configuration

---

Zones can be created in the following ways:

- Create zones as protected objects under **Configurations >> Protected Objects >> Zones**. See [Create a Zone](#).
- Create zones that refer to a zone config profile that contains the majority of zone configuration, including the services. See [Zone Profiles](#).
- Create zones as protected objects and define services using service protection profiles. See [Zone Service Protection Profile](#).

## Manage a Zone

Perform the following steps to access the Zones page:

1. Go to **Configurations >> Protected Objects >> Zones**.
2. (Optional) Click to perform any of the following actions:

Action	Purpose
Reset	Resets the search filter on the zones.
Refresh	Refreshes the information displayed for the Zone page.
+Add New	Configures a new Zone.
Bulk Actions	Allows you to perform actions on multiple zones at once, see <a href="#">Performing Bulk Actions on Zones</a> .

Table 14 : Describes the zone page configuration.

Column heading	Description
<b>Name</b>	Displays the name of the zone.
<b>IP/Subnet</b>	Displays the IP address and subnet information of the zone.
<b>Services</b>	Displays the IP protocols and ports involved with service. Hover over the column for more information.
<b>Detector Group</b>	Displays the device or device set that acts as a detector or a detector group for the zone.
<b>Mitigation Group</b>	Displays the device or device set that acts as a mitigator or a mitigator group when an incident occurs.
<b>Mitigation Status</b>	Displays the current status of the mitigation. The status can be Mitigation, Normal, RTBH or Error.  NOTE: An auto start and stop mitigation notification is displayed on the page.
<b>Oper. Mode</b>	Displays the operational mode the zone is under currently (Idle, Learn, Protect). To edit the Oper. Mode, click the edit icon and

Column heading	Description
	<p>select the appropriate option. For more information on Oper. Mode, see <a href="#">Zone Operational Mode</a>.</p> <ul style="list-style-type: none"> <li><b>Idle</b>—In this mode, where CPU resources are not utilized for a zone.</li> <li><b>Learn</b>—In this mode, where traffic baseline values will be established for a zone that can be used to create thresholds.</li> <li><b>Protect</b>—This mode monitors and detects IP anomalies.</li> </ul> <p>A confirmation message is displayed, click OK to change the Oper. Mode. The Oper. Mode is updated accordingly.</p>
<b>Oper. Status</b>	<p>Displays the operational status of the zone. The status can be as follows:</p> <ul style="list-style-type: none"> <li><b>OK</b>—Indicates the status is normal.</li> <li><b>Unknown</b>—Indicates the status cannot be determined at the current time.</li> <li><b>Out of Sync</b>—Indicates the changes on SecDevice are not yet synchronized with the device(s).</li> <li><b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the zone(s).</li> <li><b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the zone(s).</li> </ul>
<b>Incidents</b>	<p>Displays the current status of incidents under a zone, listing the number of New Incidents, Ongoing Incidents, and Stopped Incidents.</p>
<b>Actions</b>	<p>Click the link in the Actions column to perform any of the following :</p> <ul style="list-style-type: none"> <li><b>Edit</b>—Allows you to modify one of the previously-configured detection zone.</li> <li><b>Duplicate</b>—Allows you to create an object with basic parameters that are identical to the original object.</li> </ul>

Column heading	Description
	<ul style="list-style-type: none"> <li>• <b>Charts</b>—Allows you to go to Zone Charts page where graphs for the zone are displayed.</li> <li>• <b>Statistics</b>—Allows you to go to the Zone Statistics page where statistics for the zone are displayed.</li> <li>• <b>Report</b>—Allows you to generate a report or report schedule.</li> <li>• <b>Sync to Device</b>—Allows you to push the current zone configuration (along with profile configuration, oper policy configuration, and associated BGP objects) to the device group. Once the zone is pushed successfully to the device group, the status is updated. Go to <b>Administration &gt;&gt; Scheduler or Job Execution Results</b> to view the job execution status and results.</li> <li>• <b>Delete</b>—Allows you to delete the current zone.</li> </ul>

Zones can be searched based on the Zone name, IP address or subnet, device group, and detectors configured in the zone.

- **Zone Name**—Enter a partial or a complete zone name (for example, example-zone or example-zone-a10) in the Zone Name/IP box. All the zones configured with the specified zone name will be displayed in the table.
- **IP address**—Enter a complete IP address (for example, 162.120.4.69) in the Zone Name/IP box. The list of zones associated with the IP address is displayed in the table.
- **All Device Groups**—Select a device group from the All Device Groups list. The list of zones configured with the specified device group is displayed.
- **All Detectors**—Select a detector from the All Detectors list. The list of zones configured with the specified detector is displayed.

## Create a Zone

Perform the following steps to create a new zone:

1. Click **+ Add New**.
2. In the Zone Name field, enter the name of the zone.

---

**NOTE:** Once a zone name is set, it cannot be modified. A zone name must contain only the alphanumeric characters (a-z, A-Z, 0-9) and the special characters such as period (.), hyphen (-), and underscore (\_).

---

3. In the IP Address(es) field, select one of the following options:
  - **Statically Configured**—In the IPv4 / IPv6 / Subnet field, enter the IPv4 or IPv6 address and subnet for the zone using one of the following actions:
    - After entering an IP address and subnet, click **Plus sign (+)** to add.

---

**NOTE:** Now you can add two new type of IP addresses, expand subnet static and expand subnet dynamic.

---

- Click **Edit** and enter or copy and paste the multiple IP addresses or subnet configurations and click **OK**.
  - **Dynamically Learnt from BGP Peer**—A zone auto-learns the IPs from a BGP Peer.
4. Expand the **Zone Parameters** section and enter the following information:
    - **Description**— Enter a description to help identify the zone.
    - **Operational Policy** —Choose an operational policy to use with the zone.
  5. Expand the **Mitigation** section and enter the following:

Table 15 : field and its purpose for mitigation section.

Fields	Purpose
Mitigator Group	Choose a group of mitigation devices that acts as a mitigator.
Packet Capture Policy	Choose a packet capture policy to use with the zone.
Rate Limit	Choose a configured GLID for the rate Limit configuration. <b>Limit per address</b> —Select the check box to apply the rate limit

Table 15 : field and its purpose for mitigation section.

Fields	Purpose
	configured in a GLID to each individual IP address in a zone subnet.
DSCP Marking	Select the check box to mark clean traffic at the zone level. Enter the values between 1-63 in the following fields: <ul style="list-style-type: none"> <li>• <b>Inbound Forward</b></li> <li>• <b>Outbound Forward</b></li> </ul>
Hardware Blacklist Drop	Select the check box to enable Hardware-assisted Traffic Blocking on the TPS devices. Select one of these options: <ul style="list-style-type: none"> <li>• <b>Destination Blocking</b>—Traffic that does not match the specific destination IP rules that are defined for DDoS protection are dropped in hardware.</li> <li>• <b>Source Blocking</b>—Traffic that does not match the specific source IP rules are dropped in hardware.</li> </ul>

**NOTE:** Hardware-assisted Traffic Blocking leverages the hardware chipset for traffic that goes beyond a threshold limit. When the packet drop rate exceeds the default threshold, for example—during a volumetric attack, packets get dropped in hardware rather than the CPU, this feature allows TPS to drop packets at a higher rate. It enables the CPU to focus exclusively on packets requiring further processing. This feature has some limitations. For detailed information about this feature and its limitations, see [ACOS 3.2.5-P1 TPS New Features and Enhancements](#).

## 6. Expand the **Detection** section and enter the following:

Table 16 : Field and its purpose for detection section

Fields	Purpose
Detector Group	Choose a group of detection devices. To create a detection group, see <a href="#">Device Groups</a> .
Top-K Source IPs	Enter a number of Top-K source IP addresses for each source subnet. By default, the top-k IPs displayed is 20. The top

Table 16 : Field and its purpose for detection section

Fields	Purpose
	source IPs above 20 and up to 100 is supported only from the TPS 5.0.1 version and above.
Top-K Destination IPs	Enter a number of Top-K destination IP addresses for each destination subnet that you want to get from the TPS device. By default, the top destination IPs displayed is 10. The maximum value can be 100. The top destination IPs is supported only on the TPS 5.0.1 devices and above.
Continuous Learning	Select the check box to determine the continuous learning of traffic baseline for a zone. It analyzes the observed traffic and turns the learned values into thresholds.
Service Discovery	Select the check box to enable the Service Discovery function if TPS other/UDP other are required.  <b>Packet Rate Threshold</b> —Enter the values between 1-255 in this field.
Packet Anomaly Detection	Select the check box to enable the detection of TCP and UDP port 0 DDoS attack. When a threshold is exceeded for a TCP or a UDP port 0, SecDevice receives an alert on the traffic surge.  Click <b>Plus sign (+)</b> and select the Indicator Type as Port Zero Packet Rate and enter the Threshold. The threshold value can be <1-255> packets per second.
Victim IP Anomaly Detection	Select the check box to enable the individual victim IP based detection when a zone is under attack. <ul style="list-style-type: none"> <li>• <b>Dynamic Traffic Threshold</b> — Select the check box to enable the detection based on traffic thresholds dynamically determined by the detector.</li> <li>• <b>Static Traffic Threshold</b> — Select the check box to enable the detection based on the statically configured traffic threshold such as the following: <ul style="list-style-type: none"> <li>◦ <b>Forward PPS</b> — Enter the value for forward traffic packet rate threshold.</li> </ul> </li> </ul>

Table 16 : Field and its purpose for detection section

Fields	Purpose
	<ul style="list-style-type: none"> <li>◦ <b>Forward BPS</b>— Enter the value for forward traffic byte rate threshold.</li> <li>• <b>Histogram</b> — Select the check box to enable the detection to be based on adaptive auto-learned traffic histogram thresholds.</li> </ul> <p><b>NOTE:</b> The Histogram and Static Traffic Threshold check boxes should be enabled together to monitor the anomaly even after it has aged out.</p> <p><b>NOTE:</b> If the “Victim IP Anomaly Detection” is selected in a zone template, the zone pushes only the “IP-Proto Other” service to the detector, irrespective whether you have selected the “IP-Proto Other” service among the discovered services under the zone template. While all other services are applied to the mitigator.</p>

7. Expand the **Source Ports** section, click the downward arrow and then click **Plus sign (+)** to see further options:

Table 17 : Field and its purpose for source ports section

Fields	Purpose
Protocol	Choose TCP or UDP as a protocol.
Port/Range	Enter a port or port range. When a port range is entered, specify the lower port number followed by a Hyphen (-) and then the highest port number.
GLID	Choose a <a href="#">Configure GLID</a> for rate limiting.
Template	Choose a template from the list.
Deny	Select Deny to drop and black-list matching inbound traffic. The black-list setting is permanent; that is static, and changes only if this configuration changes.

8. Select **Use Zone Profile for Configuration** check box and then choose the zone profile from the **Zone Config Profile**.

---

**NOTE:** You can either perform step 8 or step 11. They are mutually exclusive.

---

9. Click **Zone Charts** to view the graph. For more information, see [Zone Charts](#).
10. Click **Indicator Threshold** to enter the information for zones under protection. For more information, see [Operational Mode - Protect](#).
11. Click **Discovered Services** to view the Services, Packet Rate, Actions on the pop-up window.
12. In the **Services** section, configure the protocol services and the designated ports for such services in the appropriate fields. Click the **Plus sign (+)** to configure the additional services. Some standard protocols are pre-configured with the appropriate port number. The following is the list of Services supported:
  - TCP - <Port> or <Port Range> or other
  - UDP - <Port> or <Port Range> or other
  - HTTP - <Port> or <Protocol Number>
  - QUIC - <Port> or <Protocol Number>
  - DNS-TCP - <Port> or <Protocol Number>
  - DNS-UDP - <Port> or <Protocol Number>
  - SSL-L4 - <Port> or <Protocol Number>
  - SIP-TCP - <Port> or <Protocol Number>
  - SIP-UDP - <Port> or <Protocol Number>
  - Any TCP
  - Any UDP
  - ICMPv4
  - ICMPv6
  - GRE
  - IPv4 ENCAP

- IPv6 ENCAP
- Other
- Protocol Num - <Protocol Number>

**NOTE:** SIP over TCP is only supported in asymmetric mode.

13. Depending upon the type of Zone Service, click **Edit** for a configured service to edit a Zone Service. The Edit Zone Service for the selected protocol appears. For more information, see [Zone Service Protection Profile](#)

If Protocol Num 50 is configured as the zone service, ESP Inspect is available to allow configuration of ESP payload parameters with one of the following Auth Algorithms.

- AUTH\_NULL – No Integrity Check Value
- HMAC-SHA-1-96 – 96 bit Authentication Algorithm
- HMAC-SHA-256-96 – 96 bit Authentication Algorithm
- HMAC-SHA-256-128 – 128 bit Authentication Algorithm
- HMAC-SHA-384-192 – 192 bit Authentication Algorithm
- HMAC-SHA-512-256 – 256 bit Authentication Algorithm
- HMAC-MD5-96 – 96 bit Authentication Algorithm
- MAC-RIPEMD-160-96 – 96 bit Authentication Algorithm

Under Pattern Recognition (ZAPR):

Table 18 : Field and its purpose for ZAPR

Fields	Purpose
Start Pattern Recognition	<ul style="list-style-type: none"> <li>• Choose a zone service level at which you want to run the signature extraction. The signature extraction is pushed to TPS only when the mitigation is started.</li> <li>• TPS extracts the unknown attack signatures from the attack traffic and stops extraction when TPS sends deescalation notification to SecDevice.</li> <li>• The extracted attack signatures are analyzed using Machine Learning techniques and converted to signature</li> </ul>

Table 18 : Field and its purpose for ZAPR

Fields	Purpose
	rules using Berkeley Packet Filter (BPF) expressions.
Apply Extracted Filters	<p>Choose a zone service level at which the extracted signature extraction filters are applied on the incoming traffic and the packets that match the filters are dropped.</p> <p>To monitor the dropped packets and packet rates, go to <a href="#">Mitigation &gt; Zone Mitigation Console</a>.</p>
Triggered By	<p>Choose from the following options:</p> <ul style="list-style-type: none"> <li>• <b>Packet Rate Exceeds</b></li> <li>• <b>Zone Escalation</b></li> </ul> <p>You can trigger the pattern recognition when a packet rate threshold exceeds a global limit ID (GLID) or when there is zone escalation. If the option is not specified, by default the trigger is when a rate threshold exceeds a GLID.</p>
Capture Traffic	<p>Choose from the following options:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Dropped</b></li> </ul> <p>You can capture all traffic or capture only the dropped traffic for the purpose of extracting a ZAPR filter. If the option is not specified, the default behavior will capture only the dropped traffic.</p>

---

**NOTE:** The Triggered By and Capture Traffic options are applicable only when the TPS v5.0.2 device is used.

---

- Depending on the protocol selected, policy levels are configurable. A zone service configuration can have up to 5 levels, that start at zero and escalate to 4. Click on the downward arrow on the Level 0 row if it exists.
- Click on **Plus sign (+)** to add further indicator configuration for the zone

service. To enter the appropriate information in the indicator configuration, see [Configure Zone Service Protection Profile](#)

14. Perform one of the following actions:

- **Save**—Allows you to save the changes to SecDevice.
- **Save & Push**—Allows you to save the changes to SecDevice and send the configurations to the device simultaneously . Using this option saves time for users to send small configuration changes to the devices.

After a zone is created, the edit zone configuration page displays the **Zone Charts** button, which navigates you to the [Zone Charts](#) page in a new browser tab.

Depending on your topology, operational mode may be used to build a baseline for traffic thresholds for your zone services. To access the operational mode functions, go to the **Configuration >> Protected Objects >> Zones** and then choose **Learn** from Operational Mode drop-down to get a traffic baseline for your zone. For more information see [Operational Mode - Learning](#).

## Performing Bulk Actions on Zones

SecDevice allows you to perform actions on multiple zones at once. You can select more than one zone and remove a detector or replace another detector on the selected zones. Similarly, you can remove a mitigator group or replace another mitigator group in the selected zones. You can also change the associated operational policy on the bulk zones.

In addition, you can add or update the source port number or range on the selected zones.

To perform the bulk actions on zones:

1. On the **Configuration >> Protected Objects >> Zones**, select the zones for which you want to apply the configuration changes.
2. Under Bulk Actions, click **Edit**. The Bulk Edit Zones screen is displayed.
3. From the Detector drop-down list, select one of the following options:

- Do not update—Select this option if you do not want to update the current selection.
  - Remove detector—Select this option to remove the detector from the selected zones.
  - <Detector name>—Select the name of the detector device to be configured as the detector on the selected zones.
4. From the Mitigator Group drop-down list, select one of the following options:
- Do not update—Select this option if you do not want to update the current selection.
  - Remove mitigator group—Select this option to remove the mitigator group from the selected zones.
  - <Mitigator Group>—Select the name of the device to be configured as the mitigator group on the selected zones.
5. From the Oper Policy drop-down list, select one of the following options:
- Do not update—Select this option if you do not want to update the current selection.
  - <Oper Policy names>—Select the Oper policy to associate to the selected zones.
6. To add a new source port or update the existing source port number or port range on the selected service, expand the options by clicking the + button.
- From the Protocol drop-down list, select the protocol for which you want to enter the port number or range.
  - In the Port/Range box, enter the port number or the port range. The source ports are either configured or replaced on the selected zones.
  - From the GLID drop-down list, select a configured GLID for rate limiting. The GLID is replaced on the selected zones.
  - From the Template drop-down list, select a template.
  - Select Deny to drop and black-list matching inbound traffic.
7. Click **Save**. A job is automatically scheduled to push the selected zones to the devices. The status is displayed on the Job Execution Results page. To view the job execution results, see [Job Execution Results](#).

To update the zone operational mode:

1. On the **Configuration >> Protected Objects >> Zones**, select the zones for which you want to apply the configuration changes.
2. Under Bulk Actions, click **Oper Mode**. The Bulk Update Zone Operational Mode screen is displayed.
3. From the Operational Mode drop-down list, select idle, learning, or monitor mode. The operational mode is updated on the selected zones.
4. Click **Save**. A job is automatically scheduled to push the selected zones to the devices. The status is displayed on the Job Execution Results page. To view the job execution results, see [Job Execution Results](#).

To push multiple zone configurations to the device group:

1. On the **Configuration >> Protected Objects >> Zones**, select the zones for which you want to apply the configuration changes.
2. Under Bulk Actions, select **Sync to Device** to push the current zone configurations to the device group. Once the zone is pushed successfully to the device group, the status is updated. Go to **Administration >> Scheduler** or Job Execution Results to view the job execution status and results.

To create report for multiple zones, under Bulk Actions, select Report. For more information, see [Create a Report Schedule for more information](#).

To delete multiple zones at a time, under Bulk Actions, click Delete. The selected zones are deleted.

## Zone Operational Mode

Operational Mode has three states which are applied to a zone; Idle, Learn, and Protect (same as the Monitoring mode). See Zone Operational Modes in the *DDoS Mitigation Guide* for further information. To change the Operational Mode, go to **Configurations >> Protected Objects >> Zones**, and then choose the suitable mode from Operational Mode drop-down. The information here describes the important information related to Operational Mode for SecDevice zone configuration.

## Operational Mode - Idle

---

When Operational Mode is in Idle state, no CPU resources are being utilized for a zone.

## Operational Mode - Learning

---

The Operational Mode Learn can be used to determine a traffic baseline for a zone.

The zone services can include User-defined indicators, threshold values, and action parameters for learning mode. To accommodate four different escalation levels, lists of indicators per protocol can be configured with varying, incremental thresholds.

When a zone is set to the Learning mode, these indicators are learned by the detector or a mitigator group. Upon learning, the zone service page displays the final user-defined indicator values or learned indicator values.

When SecDevice learn values for the indicators, consider the following scenarios:

- If Learning occurs on a standalone detector, the user selected detection threshold value is divided by the total number of mitigators and is then sent to each mitigator. However, if thresholds are manually configured, the threshold values will still be divided by the number of mitigators.

For example, if a **zone-threshold 10** was learned and configured on a detector, and there were two mitigators, the value sent to each mitigator would be **zone-threshold 5**.

- If Learning occurs on multiple mitigators, the baseline value for detection threshold is the sum of all mitigators while there is no standalone detector.

For example, if a **zone-threshold 10** was learned through a deployment that had zero detectors and two mitigators, both mitigators would have a **zone-threshold 10** configured.

Perform the following steps to learn your traffic baseline:

1. Go to **Configuration >> Protected Objects >> Zones**, under the **Operational Mode** column, click the edit icon and choose **Learn**.
2. On Configure Zone Learning window, enter the appropriate information.

Field	Purpose
Detection Group	Choose a detection group associated with the zone.
Mitigation Group	Choose a mitigation group associated with the zone.
Learning Duration	<p>Choose a Learning Duration from the drop-down list to measure the baseline traffic.</p> <p><b>NOTE:</b> If the Learning Duration is set to Until Stopped (default), the Detection Sensitivity cannot be accessed.</p>
Detection Sensitivity	<p>Allows you to take your baseline traffic rates and create threshold values based on how much traffic variance you are willing to accept before being alerted for mitigation. The threshold values for configured services is multiplied by the detection sensitivity level.</p> <p>For example, if the HTTP packet rate baseline is 1,000, a setting of low would set the threshold value at 5,000 pack</p>

- Click **Start Learning** to begin the learning. If the zone has already learned the values (is in Protected Mode), the button appears as **Restart Learning**.

When Oper. mode of a zone is changed to Learning, the following information is displayed on **Configuration >> Protected Objects >> Zones >> Configure** page:

Fields	Description
Learning Device Group	Displays the name of the mitigator or detector group. If A10 Detector is used by the zone, then the detector group is displayed.
Learned Indicators	<p>Displays the latest learned values for each configured zone service in the form of bar charts on the Learning pop-up page. Modify the fields to view the appropriate information and click <b>Configure Protection</b>.</p> <p>An <b>Indicator Threshold</b> page opens, you can choose to either use Learned threshold values or Selected threshold values based on the</p>

Fields	Description
	detection sensitivity and click <b>Start Protection</b> to configure the threshold values on the devices and change the Oper. Mode of the zone to a Protected state.  For more information, see <a href="#">Operational Mode - Protect</a> .
Learning Duration	Displays the learning start and end date with time, based on the learning duration chosen on Configure Zone Learning window.  Once the learning time ends, the zone is automatically configured to the Protected state.  If the Learning Duration chosen is <b>Until Stopped</b> , the learning continues unless the Oper. Mode is manually changed to the Protected state.

## Operational Mode - Protect

When a traffic baseline is learned, detection sensitivity can be quickly configured to address escalating traffic thresholds by running operational mode protect.

Perform the following steps to change the Operational Mode of a zone to Protect:

1. Go to **Configuration >> Protected Objects >> Zones >> Configure** page, choose **Protect** as the Operational Mode and click **Indicator Thresholds**.
2. In the **Threshold Source (All Services)** and **Threshold Source (Per Service)** fields, choose the threshold for the total traffic.
3. In the **Zone Esc. Score** field, the score to filter the values is displayed.

Column heading	Description
Service	Displays the IP protocols and ports associated with service.
Indicator	Displays the indicator type for the selected service.
Learned Threshold	Displays the threshold values that are currently obtained from TPS detector or mitigator. Click the mitigator group link to view the learned indicator values for each mitigator.

Column heading	Description
	<p><b>NOTE:</b> If a zone is in learning state, the Refresh icon fetches the latest learned indicator values from the device.</p>
Configured Threshold (Total Traffic)	<p>Displays the existing threshold configurations that are defined in the zone service.</p>
Indicator Score	<p>Displays the score for each indicator and zone escalation.</p>
Selected Threshold (Total Traffic)	<p>Enter the indicator threshold values that correspond to the total traffic of the zone service. If a detector group is associated with this zone, these values are pushed to the TPS detector when you click <b>Start Protection</b>.</p> <p>From the sensitivity drop-down list, you can choose:</p> <ul style="list-style-type: none"> <li>• <b>Low Sensitivity (5.0)</b>—If traffic must greatly exceed the baseline traffic rate. Traffic must exceed five times the baseline traffic rate to trigger mitigation.</li> <li>• <b>Medium Sensitivity (default) (3.0)</b>—To create a balanced threshold. Traffic must exceed three times the baseline traffic rate to trigger mitigation.</li> <li>• <b>High Sensitivity (1.5)</b>—To create a low threshold for traffic mitigation. Traffic must exceed one point five times the baseline traffic rate to trigger mitigation.</li> <li>• <b>Currently Configured Thresholds (Total Traffic)</b>—To use the currently configured threshold defined for the zone service.</li> </ul> <p><b>NOTE:</b> Indicators with selected threshold as 0 are not pushed to the device.</p>
Selected Threshold (Per Device)	<p>Displays the indicator threshold values per mitigator.</p>

4. Click **Start Protection** to start the protection.

## Zone Templates

The Template for Zones page provides pre-configuration of mitigation options that can be saved and applied to incidents and zones. Depending on which countermeasures are configured, configuration of supporting objects such as GLID, Class Lists and DDoS templates may be required.

Pre-defined templates for TCP, UDP, HTTP, SSL, DNS-UDP, DNS-TCP and GLIDs are available. These are read-only templates. Click Duplicate to use these pre-defined templates to quickly generate a zone based template without the need to fill in common parameters.

To access the TPS Zone Based Template page, navigate as follows:

1. Hover over **Configurations >> Templates >> Zone Templates**.
2. (Optional) Enter a string in the **Search** field to filter the list of templates.
3. (Optional) The following buttons appear across the upper-right side of the TPS Mitigation Templates table:
  - Refresh – Refreshes the information displayed for the TPS Templates.
  - Delete – Select the check box at left for one or more TPS Templates, then click Delete.
  - Zone Templates - Click on the appropriate tab to configure a Zone related template. These templates are added to Zone Services. Go to a configured zone and click Edit to access Zone Services.
    - [TCP](#)
    - [UDP](#)
    - [DNS](#)
    - [HTTP](#)
    - [SSL-L4](#)
    - [ICMP-v4/v6](#)

- [IP Proto](#)
- [Encapsulation](#)
- [Logging Template](#)
- [Violation Actions](#)
- [SIP](#)
- [Source Port TCP Template](#)
- [Source Port UDP Template](#)
- [GLID](#)
- [Source Based Policy](#)

For more information about zone templates, refer to [Zone Templates](#).

## Zone Profiles

Zone configuration profiles can be configured to capture common DDoS protection configurations at the zones and zone service levels. This ability to define countermeasure profile once and reference it from various zones makes zone creation much faster and simpler, as zone creation now only requires the configuration of a zone name and an IP list, together with the association of a zone configuration profile to the zone.

The following topics are covered:

<a href="#">Zone Config Profile</a> .....	93
<a href="#">Zone Service Protection Profile</a> .....	99
<a href="#">Zone Operational Policy</a> .....	107

## Zone Config Profile

---

Zone Config Profile is a configuration profile that contains the common DDoS protection configurations at the zone and zone service levels.

This section covers the following:

- [Manage a Zone Config Profile](#)
- [Configure Zone Config Profile](#)

## Manage a Zone Config Profile

Perform the following steps to access the Zone Config Profile page:

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Config Profile**.
2. (Optional) Perform any of the following actions:

Table 21 : listed actions for for Zone Policies/Profiles

Actions	Purpose
Reset	Resets the search filter on the profiles.
Refresh	Refreshes the information displayed for the profile page.
Delete	Deletes the configured profile.
+ New Zone Profile	Configures a new profile.

The main Zone Profile page displays a table of configured Zone Profiles along with information about them.

Table 22 : Information About Previously Configured Zone Config Profile

Column Heading	Description
Name	Displays the name of the profile.
Services	Displays the services associated with the Zone Config Profile.
Actions	<ul style="list-style-type: none"> <li>• <b>Edit</b>—Allows you to edit previously configured profile.</li> </ul> <p><b>NOTE:</b> Changes made to a zone will propagate to any zones that are using the profile. If the profile is in use, click <b>Submit</b>, a confirmation dialog is displayed with a list of affected zones.</p> <ul style="list-style-type: none"> <li>• <b>Duplicate</b>—Allows you to duplicate the profile.</li> </ul> <p>For information on configurable parameters, see <a href="#">Configure Zone Config Profile</a>.</p>

## Configure Zone Config Profile

Perform the following steps to create a zone config profile:

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Config Profile**.
2. Click the green + **New Zone Profile** button.
3. Enter the name of the zone configuration profile.
4. Enter a Description of the zone configuration profile.
5. Configure the type of service to be associated to the zone configuration profile:

Table 23 : Describes the type of services

Column Heading	Description
Protocol	<p>Choose one of the following protocols from the drop-down list:</p> <ul style="list-style-type: none"><li>• <b>TCP</b>—&lt;Port&gt; or &lt;Port Range&gt; or other</li><li>• <b>UDP</b>—&lt;Port&gt; or &lt;Port Range&gt; or other</li><li>• <b>HTTP</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>DNS-TCP</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>DNS-UDP</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>SSL-L4</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>SIP-TCP</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>SIP-UDP</b>—&lt;Port&gt; or &lt;Port Range&gt;</li><li>• <b>Any TCP</b></li><li>• <b>Any UDP</b></li><li>• <b>ICMPv4</b></li><li>• <b>ICMPv6</b></li><li>• <b>GRE</b></li><li>• <b>IPv4 ENCAP</b></li><li>• <b>IPv6 ENCAP</b></li><li>• <b>Other</b></li></ul>

Table 23 : Describes the type of services

Column Heading	Description
	<ul style="list-style-type: none"> <li>• <b>Protocol Num</b>—&lt;Protocol Number&gt;</li> </ul>
Port/Protocol Num	Enter a port range or protocol number. For more information about the selected protocol, see <a href="#">Protocol</a> for the selected protocol.
Protection Profile	Select the Zone Service Protection Profile to be associated.

---

**NOTE:** Victim IP Identification feature supports port-Other TCP and port-Other UDP options only.

---

## 6. Configure the Source Ports to be associated to the zone configuration profile:

Table 24 : Describes the Source Ports

Column Heading	Description
Protocol	Choose one of the following options: <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> </ul>
Port/Range	Enter the associated port/port range/other with respect to the selected protocol.
GLID	Choose a configured GLID for rate-limits.
Template	Choose a Template to bind to this zone profile.
Deny	Select the checkbox to deny all traffic to the selected Source Port.

## 7. Expand the mitigation section to enter the appropriate information.

Table 25 : Field and its purpose for Mitigation section

Field	Purpose
Rate Limit	Choose a configured GLID for the Rate Limit configuration.
DSCP Marking	Select DSCP to mark for clean traffic at the zone level. Configure the DSCP value for packets by configuring the traffic direction.

Table 25 : Field and its purpose for Mitigation section

Field	Purpose
	<p>Select the following supported options:</p> <ul style="list-style-type: none"> <li>• <b>Inbound Forward</b></li> <li>• <b>Outbound Forward</b></li> </ul>
Hardware Blacklist Drop	<p>Select Hardware Blacklist Drop to enable Hardware-assisted Traffic Blocking on the TPS devices. Hardware-assisted Traffic Blocking leverages the hardware chipset for traffic that goes beyond a threshold limit. When the packet drop rate exceeds the default threshold, for example—during a volumetric attack, packets get dropped in hardware rather than the CPU. This feature allows TPS to drop packets at a higher rate and enables the CPU to focus exclusively on packets requiring further processing.</p> <p>You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Destination Blocking</b>—Traffic that does not match the specific destination IP rules that are defined for DDoS protection are dropped in hardware.</li> <li>• <b>Source Blocking</b>—Traffic that does not match the specific source IP rules are dropped in hardware.</li> </ul> <hr/> <p><b>NOTE:</b> Hardware Blacklist feature has some limitations. For detailed information about this feature and its limitations, see ACOS 3.2.5-P1 TPS New Features and Enhancements.</p>

8. Expand the detection section to enter the appropriate information.

Table 26 : Field and its purpose for detection section

Field	Purpose
Top-K Source IPs	Enter the number of top-k source IP addresses for each source subnet. By default, the top-K IPs displayed is 20. The top source IPs above 20 and up to 100 is supported only from the

Table 26 : Field and its purpose for detection section

Field	Purpose
	TPS 5.0.1 version and above.
Top-K Destination IPs	Enter the number of top-k destination IP addresses per service for each destination subnet that you want to get from the TPS device. By default, the top destination IPs displayed is 10. The maximum value can be 100. The top destination IPs per zone is supported from the TPS 5.0.1 devices and above. The top destination IPs per service is supported from the TPS 5.0.2 and later releases.
Continuous Learning	Select the check box to determine the continuous learning of traffic baseline for a zone. It analyzes the observed traffic and turns the learned values into thresholds.
Service Discovery	Select the check box to discover and notify SecDevice of IP addresses and services of the configured protocol such as TCP other or UDP other. In the Packet Rate Threshold field, enter a value between 1 to 255. When the packet rate exceeds the specified threshold, SecDevice learns about the discovered entity from the detector.  <b>NOTE:</b> The TCP other or UDP other services must be configured before enabling Service Discovery.
Packet Anomaly Detection	Select the check box to enable the detection of TCP and UDP port 0 DDoS attack. When a threshold is exceeded for a TCP or a UDP port 0, SecDevice receives an alert on the traffic surge.  Click the <b>Plus sign (+)</b> to choose the <b>Indicator type as Port Zero Packet Rate</b> and enter the <b>Threshold</b> value that can be between 1 to 255 packets per second.

- From the Detector Group drop-down list, select the group of detection devices. To create a detection group, see [Device Groups](#).

9. Click **Submit**.

## Zone Service Protection Profile

Zone Service Protection Profile is a configuration profile that contains the common DDoS protection configurations at the zone service levels.

This section covers the following:

- [Manage a Zone Service Protection Profile](#)
- [Configure Zone Service Protection Profile](#)

### Manage a Zone Service Protection Profile

Perform the following steps to access the Zone Config Profile page:

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Service Protection Profile**.
2. (Optional) Perform any of the following actions:

Actions	Purpose
Reset	Resets the search filter on the profiles.
Refresh	Refreshes the information displayed for the profile page.
Delete	Deletes the configured profile.
+ New <Protocol> Zone Service Profile	Configures a new <protocol> zone service profile.

The Zone Service Protection Profile page displays a table of configured Zone Service Protection Profiles along with information about them.

Column Heading	Description
Name	The name of the Zone Service Protection Profile.
Actions	<ul style="list-style-type: none"><li>• <b>Edit</b>—Allows you to edit previously configured profile.</li></ul>

Column Heading	Description
	<p><b>NOTE:</b> Changes made to the zone service profile propagates to any zone that is associated with it. If the profile is in use, click one of the following options:</p> <ul style="list-style-type: none"> <li>○ <b>Save</b>—Applies the configuration changes to all the associated zones without sending them to the TPS device(s).</li> <li>○ <b>Save &amp; Push</b>—Applies the configuration changes to all the associated zones and sends them to the TPS device.</li> </ul> <p><b>NOTE:</b> Select the appropriate check boxes from the dialogue box to overwrite the Indicator Setting of the zone services.</p> <hr/> <ul style="list-style-type: none"> <li>● <b>Duplicate</b>—Allows you to duplicate the profile.</li> </ul> <p>For information on configurable parameters, see <a href="#">Configure Zone Service Protection Profile</a>.</p>

## Configure Zone Service Protection Profile

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Service Protection Profile**.
2. Click the green **New <protocol> Zone Service Profile** button.

---

**NOTE:** The fields here are not applicable for all the protocols.

---

Table 29 : Displays Create Protocol Zone Service Protection Profile window

Field	Purpose
Name	Enter a name for the Zone Service Protection Profile.
Rate Limit	Choose a configured GLID.
Rate Limit Action	Choose one of the following actions: <ul style="list-style-type: none"> <li>● <b>Drop</b>—Drops the packet. It is the default option.</li> </ul>

Table 29 : Displays Create Protocol Zone Service Protection Profile window

Field	Purpose
	<ul style="list-style-type: none"> <li><b>Ignore</b>—Ignores the traffic.</li> <li><b>Blacklist-src (unsupported)</b>—Blacklists the source.</li> </ul>
Max Dynamic Entry Count	Enter the maximum number of allowable dynamic entries.
Enable Class List Overflow	Select the check box to allow an overflow policy to take effect if the maximum dynamic entry count is exceeded. If not selected, all traffic exceeding the maximum count is dropped.
Deny Packets	Select the check box to drop and blacklist the matching traffic.
Stateful	Select the check box to enable stateful session tracking. <b>NOTE:</b> Applicable only for UDP and DNS-UDP protocols.
Drop Fragmented Packets	Select the check box to drop the fragmented packets.
Tunnel Decap	Select the check box to decapsulate and process the inner packets. <b>NOTE:</b> Applicable only for IP-Proto, GRE, IPv4-ENCAP and IPv6-ENCAP protocols.
Tunnel Decap Key	Enter a key for tunnel decapsulation. <b>NOTE:</b> Applicable only for IP-Proto and GRE protocol.
Tunnel Rate Limit	Select the check box to enable DDoS protection on tunnel traffic. <b>NOTE:</b> Applicable only for IP-Proto, GRE, IPv4 and IPv6 protocols.

Table 29 : Displays Create Protocol Zone Service Protection Profile window

Field	Purpose
Source Based Policy	<p>Choose an existing Source Based Policy template.</p> <p>After the source based policy has been selected, choose the following:</p> <ul style="list-style-type: none"> <li>• <b>Class List</b></li> <li>• <b>Action</b></li> <li>• <b>GLID Action</b></li> <li>• <b>&lt;Protocol&gt; Template</b></li> <li>• <b>Encap Template</b></li> </ul> <hr/> <p><b>NOTE:</b> The Encap Template field is disabled by default for the following services:</p> <ul style="list-style-type: none"> <li>- ICMPv4</li> <li>- ICMPv6</li> <li>- Other</li> <li>- Protocol Number</li> </ul> <hr/> <ul style="list-style-type: none"> <li>• <b>Log Template</b></li> </ul> <p>Refer to the following:</p> <ul style="list-style-type: none"> <li>• For DNS-TCP/DNS-UDP, a DNS Template and TCP/UDP Template are required.</li> <li>• For HTTP, a HTTP Template and a TCP Template are required.</li> <li>• For SSL-L4, a SSL-L4 Template and a TCP Template are required.</li> <li>• For SIP-TCP/SIP-UDP, a SIP Template and a TCP/UDP Template are required.</li> <li>• For Protocol Num, an IP Proto Template and Encap Template are required.</li> </ul>
IP Filtering Policy	Select an IP Filtering Policy to be associated with the zone service.

### 3. Under Pattern Recognition (ZAPR).

Table 30 : Field and Purpose for ZAPR

Field	Purpose
Start Pattern Recognition	Choose a zone service level at which you want to run the signature extraction. The signature extraction is pushed to TPS only when the mitigation is started. TPS extracts the unknown attack signatures from the attack traffic and stops extraction when TPS sends deescalation notification to SecDevice. The extracted attack signatures are analyzed using Machine Learning techniques and converted to signature rules using Berkeley Packet Filter (BPF) expressions.
Apply Extracted Filters	Choose a zone service level at which the extracted signature extraction filters are applied on the incoming traffic and the packets that match the filters are dropped.
Triggered By	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Packet Rate Exceeds</b></li> <li>• <b>Zone Escalation.</b></li> </ul> <p>You can trigger the pattern recognition when a packet rate threshold exceeds a global limit ID (GLID) or when there is zone escalation. If the option is not specified, by default the trigger is when a rate threshold exceeds a GLID.</p> <p>If you choose the <b>Packet Rate Exceeds</b> option to trigger pattern recognition, you must specify the rate limit.</p>
Capture Traffic	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Dropped</b></li> </ul> <p>You can capture all traffic or capture only the dropped traffic for the purpose of extracting a ZAPR filter. If the option is not specified, the default behavior will capture only the dropped traffic.</p>

To monitor the dropped packets and packet rates, go to **Mitigation >> Zone Mitigation Console**.

---

**NOTE:** The Triggered By and Capture Traffic options are applicable only when the TPS v5.0.2 device is used.

---

4. Depending on the protocol selected, policy levels are configurable. A zone service level configuration can have up to 5 levels, that start at zero and escalates to 4. Click on the downward arrow on the Level 0 row if it exists.

Table 31 : Displays Policy Levels.

Fields	Purpose
Source Default GLID	Choose a configured GLID for rate-limits.
GLID Action	Choose one of the following options: <ul style="list-style-type: none"> <li>• <b>Drop</b></li> <li>• <b>Ignore</b></li> <li>• <b>Blacklist-src</b></li> </ul>
Protocol Template	A protocol template or two protocol templates may appear depending on the protocol selected earlier for the zone. Choose a configured zone protocol template.
Encap Template	Choose a template to encapsulate the packets.
Source Escalation Score	Enter the source escalation score for the level, which specifies the number of score units required to move source traffic to this security level. Only source threshold violations are counted against this score. <hr/> <p><b>NOTE:</b> Under <b>Level 0</b>, the default value is 10.</p> <hr/> <p>If the source traffic exceeds the set score, DDoS Source Escalation notification is generated. For more information, see <a href="#">SecDevice Logs</a> .</p>
Source	Choose a configured violation action.

Fields	Purpose
Violation Actions	
Zone Escalation Score	<p>Enter the zone escalation score for the level. The number specifies the score required to escalate to the next level.</p> <p><b>NOTE:</b> Under <b>Level 0</b>, the default value is 10.</p>
Zone Violation Actions	<p>Choose a configured zone violation action.</p>
Close Sessions for Unauth Sources	<p>Select the check box to close the sessions for the source-zone-services learned without any authentication in case of level escalation.</p> <p>The feature supports the following:</p> <ul style="list-style-type: none"> <li>• Service type: <ul style="list-style-type: none"> <li>◦ [port   port-range] [tcp   ssl   http   dns-tcp   sip-tcp   udp (stateful)   dns-udp   quic   sip-udp]</li> <li>◦ port other [tcp   udp]</li> </ul> </li> <li>• Service level: <ul style="list-style-type: none"> <li>◦ Level 1 to Level 4</li> </ul> </li> </ul> <p>For this feature to work, the zone-service must use a zone-template with any of following authentication mechanism configured:</p> <ul style="list-style-type: none"> <li>• syn-auth</li> <li>• ack-auth</li> <li>• UDP retry timeout</li> </ul> <p><b>NOTE:</b> Supports TPS version 5.0.2-P3 and above</p>

5. Click the **Plus sign (+)** to add further indicator configuration for the zone service.

Field	Purpose
Indicator	<p>Choose an indicator from the drop-down list.</p> <p><b>NOTE:</b> Under <b>Level 0</b>, by default the <b>pkt-rate</b> indicator is chosen.</p> <hr/> <p>To know more about the indicators, see <a href="#">Determining Attack Types</a>.</p>
Parameter	<p>Enter information for the specific indicator that requires the information.</p>
Score	<p>Enter the score for this escalation level.</p> <p><b>NOTE:</b> Under <b>Level 0</b>, for the <b>pkt-rate</b> indicator, the default value is 20.</p> <hr/>
Threshold Per Zone	<ul style="list-style-type: none"> <li>• <b>Threshold (Total Traffic)</b>—Enter the indicator threshold values that correspond to the total traffic of the zone service. If a detector group is associated with this zone, these values are pushed to the TPS detector when you click <b>Save</b> on the Edit Zone Service page and then click <b>Save &amp; Push</b> on the <b>Configuration &gt;&gt; Protected Objects &gt;&gt; Zones &gt;&gt; Configure</b> page.</li> <li>• <b>Threshold (Per Device)</b>—Enter the indicator threshold values per mitigator. If a mitigator group is associated with this zone, these values are pushed to the TPS mitigator when you click <b>Save</b> on the Edit Zone Service page and then click <b>Save &amp; Push</b> on the <b>Configuration &gt;&gt; Protected Objects &gt;&gt; Zones &gt;&gt; Configure</b> page.</li> <li>• <b>Violation Action</b>—Choose a configured violation action from the drop-down list.</li> </ul>
Threshold Per Source	<ul style="list-style-type: none"> <li>• <b>Threshold</b>—Enter the threshold for the indicator.</li> <li>• <b>Violation Action</b>—Choose a violation action from the drop-down list.</li> </ul>

6. Repeat the steps for any additional indicators.

7. Click **Save**.

## Zone Operational Policy

Zone Operational Policy allows you to specify operational behavior settings in a policy that can be associated to multiple zones. When the policy is updated, the updated settings will propagate to the associated zones.

This section covers the following:

- [Manage a Zone Operational Policy](#)
- [Configure a Zone Operational Policy](#)

### Manage a Zone Operational Policy

Perform the following steps to access the Zone Operational Policy page:

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Operational Policy**.
2. (Optional) Perform any of the following actions:

Table 32 : listed action for Zone Operational Policy

<b>Actions</b>	<b>Purpose</b>
Reset	Resets the search filter on the policies.
Refresh	Refreshes the information displayed for the policy page.
Delete	Deletes the configured policy.
+ New Zone Profile	Configures a new policy.

The main Zone Oper page displays a table of configured Zone Oper policies along with information about them.

Table 33 : Information About Configured Zone Operational Policy

<b>Field</b>	<b>Description</b>
Name	Displays the name of the policy.
Settings	Displays the settings for a policy.
Actions	<b>Edit</b> —Allows you to edit previously configured profile.

Table 33 : Information About Configured Zone Operational Policy

Field	Description
	<p><b>NOTE:</b> Changes made to a zone will propagate to any zones that are using the profile. If the profile is in use, click <b>Submit</b>, a confirmation dialog is displayed with a list of affected zones.</p> <ul style="list-style-type: none"> <li>• <b>Duplicate</b>—Allows you to duplicate the profile.</li> </ul> <p>For information on configurable parameters, see <a href="#">Configure Zone Operational Policy</a>.</p>

## Configure a Zone Operational Policy

You can either create a new logging template or select the predefined template named **A10\_Logging\_Basic** to create the Zone Operational Policy.

Perform the following steps to configure Zone Operational Policy:

1. Go to **Configurations >> Zone Policies / Profiles >> Zone Operational Policy**.
2. Click **+ New Policy**.

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
Name	Enter a name for the policy. The supported value is a string of 1-63 characters.
Logging	Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Log Enable</b>—Enables the log functionality.</li> <li>• <b>Log Periodic</b>—Enables periodic timed logs.</li> </ul>
Logging Template	Choose a zone logging template to be used by the policy and its associated zones.  If there is no logging template chosen, the A10_Logging_Basic template is selected by default. The A10_Logging_Basic template is a predefined template that cannot be deleted. However, it can be edited as required.

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
Report Mitigator Stats	<p>Select one of the two options to specify when the TPS mitigator should export statistics information for all zones to SecDevice:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—Exports mitigation statistics to SecDevice during both peacetime and wartime, allowing the user to always view zone charts. This is the default option selected for <b>Report Mitigation Stats</b>.</li> <li>• <b>Enable on Start Mitigation</b>—Exports mitigation statistics to SecDevice only when the mitigation is started for the zone.</li> </ul> <hr/> <p><b>NOTE:</b> TPS devices can export zone and zone service statistics to SecDevice for only a limited number of zones at a given time. When the maximum zone count is reached for statistics export, the TPS mitigator throws a "Max T2 counters reached" exception.</p>
Start Mitigation	<p>Select one of the options to start mitigation on a zone when receiving a DDoS escalation notification:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b></li> <li>• <b>Manual</b></li> </ul> <p>If <b>Start Mitigation</b> is set to <b>Manual</b>, Arbor PeakFlow messages and alert notifications are ignored and SecDevice will not create any incidents. However, alert messages are logged.</p> <hr/> <p><b>NOTE:</b> The Start Mitigation option <b>Automatic</b> and the BGP Flowspec option <b>Manual</b> are mutually exclusive. When Automatic is enabled, the BGP Flowspec is disabled and vice versa.</p>
BGP	Select one of the following options:

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
	<ul style="list-style-type: none"> <li><b>Enable</b>—Configures the BGP network for the protected IPs or subnets of the zone.</li> <li><b>Disable</b>—Configures the BGP Flowspec on incident creation.</li> </ul> <p><b>NOTE:</b> BGP and BGP Flowspec are mutually exclusive. When BGP is enabled, you see BGP Routes and BGP Route Map options and BGP Flowspec is automatically disabled and vice versa.</p>
BGP Routes	<p>Select one of the following as the source for the routes:</p> <ul style="list-style-type: none"> <li><b>All Zone IPs/Subnets</b>—Configures BGP routes for all the IPs/subnets in the zone.</li> <li><b>Top Destination IPs</b>—Configures BGP routes for the top-K attacked IPs that are reported by a detector, on start mitigation. <ul style="list-style-type: none"> <li><b>Top-K IP count</b>, enter the number of top-K IP addresses to use from the reported top-K destination IPs while configuring BGP routes.</li> </ul> </li> <li><b>Victim IP</b>—Configures BGP routes for Victim IPs that are detected by A10 Detector or 3rd party detector.</li> </ul>
BGP Route Map	<p>Choose a route map you want to apply on all the attacked IPs in the zone.</p> <p>Route map is used when BGP route(s) are automatically created for the zone under attack.</p> <p>The drop-down lists the route maps that do not have RTBH enabled.</p> <p><b>NOTE:</b> If a Route Map is not selected, a default Route map called A10-SET-NEXT-HOP will be used.</p>

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
	<p><b>NOTE:</b> If a BGP Route Map is associated with a Zone Operational Policy, it cannot be deleted.</p>
RTBH Route Map	<p>Choose a route map you want to associate with the zone that is used for RTBH mitigation.</p> <p>The drop-down lists only those route maps that have RTBH enabled.</p> <p><b>NOTE:</b> If an RTBH Route Map is associated with a Zone Operational Policy, it cannot be deleted.</p> <p>For more information, see <a href="#">Remotely Triggered Black Hole</a>.</p>
BGP Flowspec	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Manual Enable</b>—Configures BGP Flowspec rules in disabled state for the protected IPs/subnets or top-K destination IPs and attacked services on incident creation. It is recommended that you explicitly enable the Flowspec rules, in order to do so, go to <b>BGP &gt;&gt; Flowspec</b> and click <b>Enable</b> under <b>Actions</b>.</li> <li>• <b>Auto Enable</b>—Configures BGP Flowspec rules in enabled state for the protected IPs/subnets or top-K destination IPs and attacked services on incident creation.</li> <li>• <b>Disable</b>—Configures the BGP Flowspec rules automatically on incident creation.</li> </ul>
BGP Flowspec IPs	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Zone/IP Subnets</b>—Configures BGP flowspec for all the IPs/subnets in the zone.</li> <li>• <b>Top Destination IPs</b>—Configures BGP flowspec for the top-K attacked IPs that are reported by a detector, on start mitigation.</li> </ul>

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
	<ul style="list-style-type: none"> <li>○ <b>Top-K IP count</b>—Enter the number of top-K IP addresses to use from the reported top-K destination IPs while configuring BGP flowspec.</li> </ul>
Traffic Filtering Action	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Redirect to TPS (Extended Community/NLRI)</b>—The router sends the traffic to the TPS device. Use the TPS outside interface IP address when redirecting traffic to TPS. To configure the outside interface IP, go to <b>Devices &gt;&gt; Device List</b>. Open the Configure Mitigation window for each mitigator in the Mitigator Group to set the interface IP. For more information, see <a href="#">Device List</a>.</li> </ul> <hr/> <p><b>NOTE:</b> If Flowspec is enabled with default filtering action as <b>Redirect to TPS (NLRI)</b>, then depending upon the format of zone subnet/destIP and source IP, mitigator outside interface IP either should use IPv4 or IPv6.</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Redirect to VRF</b>—Redirect the traffic to the specified VRF. <ul style="list-style-type: none"> <li>○ <b>VRF Target String</b>—Enter the VRF route target.</li> <li>○ <b>IP Host RT</b>—Enter Route target IP.</li> <li>○ <b>Index</b>—Enter Route target IP index.</li> </ul> </li> <li>• <b>Redirect to TPS (Extended Community/NLRI)</b>—The router sends the traffic to the TPS device. Use the TPS outside interface IP address when redirecting traffic to TPS. To configure the outside interface IP, go to <b>Devices &gt;&gt; Device List</b>. Open the Configure Mitigation window for each mitigator in the Mitigator Group to set the interface IP. For more information, see <a href="#">Device List</a>.</li> </ul>

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
	<ul style="list-style-type: none"> <li>• <b>Redirect to VRF</b>—Redirect the traffic to the specified VRF.             <ul style="list-style-type: none"> <li>◦ <b>VRF Target String</b>—Enter the VRF route target.</li> <li>◦ <b>IP Host RT</b>—Enter Route target IP.</li> <li>◦ <b>Index</b>—Enter Route target IP index.</li> </ul> </li> </ul> <p><b>NOTE:</b> VRF target string and IP Host RT/Index are mutually exclusive.</p>
Class-List Push Policy	<p>Select one of the following options to set the policy to control whether to push or not to push the class-list to the associated zones or mitigator groups on saving the zone.</p> <ul style="list-style-type: none"> <li>• <b>Always</b>—Always pushes the class-list to the zone and its supporting objects. This is the default.</li> <li>• <b>If Not Present</b>—If a class-list does not exist on at least one device in the group, SecDevice pushes the class-list to all devices in the device group.</li> <li>• <b>Never</b>—Never pushes any class-list to the device group. This behavior might cause the zone configuration push to device group fail if any of the devices do not have a class-list used by the zone.</li> </ul> <p><b>NOTE:</b> The class-list is applicable to all actions performed on the Zone Mitigation Console even when the manual mode configuration is enabled. For example, if a zone has Zone Operational Policy for class-list set to 'NEVER', and for an incident on one of the zone services, if you push Src Based Policy with class-list, the class-list push is skipped but the Src Based Policy is attempted to push.</p>

Table 34 : Fields and its purpose for Create a Zone Operational Policy windows

Field	Purpose
Exclude Pushing Class-Lists	Enter the names of the class-lists that should be excluded when pushing the zone or the zone services to the devices. When entering multiple class-lists, use comma to separate each class-list.
Stop Mitigation	Select one of the following options to automatically stop mitigation on a zone when all zone incidents have de-escalated to level zero. <ul style="list-style-type: none"> <li>• <b>Automatic</b></li> <li>• <b>Manual</b></li> </ul>
Zone Mode After Mitigation	Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Protected</b>—Configures the zone in the protected mode. By default, Protected is selected.</li> <li>• <b>Idle</b>—Configures the zone in the idle mode.</li> </ul>

3. Click **Submit**.

# Attack Detection

---

Unified detection is the static baseline detection with continuous learning of traffic baseline to determine protocol-specific indicator thresholds. It provides advanced traffic indicators, zone baseline detection, and automatic escalation and de-escalation for zone level protection, based on threshold values.

Based on the deployment topology illustrated in [SecDevice Zone Proactive Mitigation](#), attacks can be detected in three different ways:

- If TPS standalone detector is used, then it receives sFlow from router and signals SecDevice when it detects an attack. SecDevice starts mitigation by configuring zone on mitigator to draw traffic towards itself.
- If TPS mitigator is deployed in proactive mode, then it is continuously monitoring traffic and notifies SecDevice when it detects attack. This allows SecDevice to start incident. In addition, TPS also automatically starts mitigation.
- If a 3rd party detector is used, it can:
  - Signal SecDevice via REST API to create an incident and start mitigation for the zone.
  - Signal SecDevice via REST API to configure BGP route for the attacked IP.
  - Redirect traffic to TPS mitigator by sending BGP message to the router. TPS mitigator in turn signals SecDevice to start the incident.
  - Integrate Arbor Peakflow with SecDevice and TPS for mitigation. SecDevice can receive Arbor syslog anomaly start and stop notifications containing the victim IP.

The following topics are covered:

<a href="#">Determining Attack Types</a> .....	116
<a href="#">Zone Incident</a> .....	119
<a href="#">Dst Entry Incident</a> .....	126
<a href="#">Configuring Automatic Start and Stop Mitigation for Zones</a> .....	130

## Determining Attack Types

From the indicator behavior under specific protocols, SecDevice can assess what are the likely attack types. This provides information on how attack types are determined. Attack type is provided only for zone services and is not available for protected destinations.

Attack type information is available on the [Dashboard Overview](#), [Zone Incident](#) and [Zone Mitigation Console](#) page.

Table 35 : Attack Type Analysis

Protocol/ Service	Indicators	Attack Types
DNS-TCP TCP SSL-L4	pkt-rate  bit-rate pkt-drop-rate syn-rate syn-fin-ratio concurrent-conns conn-miss-rate small-payload-rate empty-ack-rate  small-window-ack-rate fin-rate rst-rate bytes-to-bytes-from-ratio pkt-drop-ratio learnt-sources	SYN Flood, ACK Flood  SYN Flood SYN Flood  Zero Window, Random Payload (STOMP), ACK Flood Zero Window, Random Payload (STOMP)  Random Payload (STOMP)
HTTP	pkt-rate	Request Flooding, Post Flood

Table 35 : Attack Type Analysis

Protocol/ Service	Indicators	Attack Types
	bit-rate pkt-drop-rate syn-rate syn-fin-ratio concurrent-conns  conn-miss-rate  small-payload-rate empty-ack-rate small-window-ack-rate fin-rate rst-rate bytes-to-bytes-from-ratio  pkt-drop-ratio learnt-sources	Request Flooding, Post Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack  Request Flooding, Post Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack
UDP DNS-UDP OTHER	pkt-rate bit-rate pkt-drop-rate bytes-to-bytes-from-ratio concurrent-conns pkt-drop-ratio learnt-sources	UDP Flood  UDP Flood UDP Flood
IPPROTO ICMPv4 IPPROTO ICMPv6	pkt-rate bit-rate pkt-drop-rate bytes-to-bytes-	Ping Flood, Smurf Attack  Ping Flood, Smurf Attack Ping Flood, Smurf Attack

Table 35 : Attack Type Analysis

Protocol/ Service	Indicators	Attack Types
	from-ratio frag-rate pkt-drop-ratio learnt-sources	Ping of Death
IPPROTO Other IPPROTO GRE IPPROTO IPv4- ENCAP IPPROTO IPv6- ENCAP	pkt-rate bit-rate pkt-drop-rate bytes-to-bytes- from-ratio frag-rate pkt-drop-ratio learnt-sources	Ping of Death
SIP UDP	bytes-to-bytes- from-ratio  concurrent-conns  conn-miss-rate  pkt-rate bit-rate learnt-sources	Request Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack Request Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack Request Flood
SIP TCP	bytes-to-bytes- from-ratio  concurrent-conns  conn-miss-rate  pkt-rate	Request Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack Request Flood, SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack SlowLoris, SlowPost, SlowRead, Malformed Protocol Attack Request Flood

Table 35 : Attack Type Analysis

Protocol/ Service	Indicators	Attack Types
	bit-rate learnt-sources	

## Zone Incident

An incident is created when a particular zone service is under a DDoS attack. An incident helps to track and manage the mitigation of an attack on a zone service. If a protected zone has more than one service that is simultaneously under attack, SecDevice creates multiple incidents, one for each service in the zone under attack.

A zone incident captures information such as start and end time of the attack, attack type, total attack bandwidth, peak attack rate and east-west traffic rate. The east-west traffic is zone-to-zone traffic, which traverses through the Thunder TPS within the same datacenter. The TPS mitigator ensures to inspect all the east-west traffic and blocks the lateral threats. Under Zone Charts, the east-west traffic information is displayed for all the devices. Also, a comprehensive report is created with all the significant information. However, if the east-west traffic is insignificant, no charts for east-west traffic are displayed under the Protected Zone Incident Detail Report.

A zone service incident can be created manually through GUI or aGAPI, or automatically through GUI when it receives an attack detected notification from the A10 detector (in the case of reactive deployment) or the TPS mitigator (if it's deployed in a proactive mode).

In case of proactive deployment, since the inbound traffic flows through the mitigator at all times, TPS automatically starts mitigation when it detects an attack. In case of reactive deployment, SecDevice configures TPS mitigator to advertise BGP routes and redirect the traffic to the attacked service through TPS.

For a reactive mode deployment, after the incident creation, a user can enable or disable automatic start and stop mitigation for a zone. Using SecDevice, this option can be set globally under **Administration >> Settings >> TPS** or at a per zone level through the Zone Operational Policy associated with that zone.

If the automatic start and stop mitigation is enabled, then SecDevice starts mitigation for a zone after the incident is created for any service. If there are attacks on multiple services, then SecDevice stops mitigation after the attack stops on the last of the attacked services.

---

**NOTE:** Incidents are for SecDevice TPS local incidents and are not associated to incidents on ACOS TPS devices.

---

Perform the following steps to access the TPS Incidents page:

1. Go to **Mitigation >> Zone Incidents** from the main menu

Table 36 : Information on Zone Incidents page

Field	Purpose
Search By	<p>Choose an option to filter the Incident List based on the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>Incident Name</b></li> <li>• <b>Zone Name</b></li> <li>• <b>Service</b></li> <li>• <b>Attack Type</b></li> <li>• <b>Peak Rate pps</b></li> <li>• <b>Peak Rate bps</b></li> <li>• <b>Total Bandwidth Packets</b></li> <li>• <b>Total Bandwidth Bytes</b></li> </ul>
Search Incident or Zone	Enter a string (from the list of TPS Incidents).
Start and End Time	<p>Enter a start and an end time, all incidents that match the Status selected for this period will be listed.</p> <ul style="list-style-type: none"> <li>• If only a start time is provided, and a search is done, then the end time is assumed to be the current time. For example, if the status Stopped was selected, and only a start time was provided, SecDevice would search for all incidents that were stopped beginning at the specified start time, up until the current time.</li> <li>• If only an end time is provided, and a search is done, then the start time is considered the beginning of time. So for example, if the status Stopped was selected and only an end time was provided, SecDevice would search for all stopped incidents that occurred until the end time.</li> </ul>
Filter By Status	Choose one of the following status:

Table 36 : Information on Zone Incidents page

Field	Purpose
	<ul style="list-style-type: none"> <li><b>New</b>—Indicates that an attack is detected but the mitigation has not started. Hence, it requires immediate attention.</li> <li><b>Ongoing</b>—Indicates that an attack is detected and the mitigation is started. Therefore, TPS is currently mitigating the attack.</li> <li><b>Stopped</b>—Indicates that the attack is stopped. SecDevice receives an escalation level 0 notification from all mitigators that were part of the mitigator group associated with that zone.</li> </ul>

2. (Optional) The following buttons appear across the upper-right side of the TPS Incidents table:

Table 37 : Displays Action function

Options	Purpose
+Add New	Click the button to add a new Incident , see <a href="#">Create a New Incident (Zone)</a> for further information.
Reset	Select the option to clear out the previous input.
Refresh	Select the option to refresh the information displayed for the TPS Incidents.
Delete	Select the check box at left for one or more incidents, then go to <b>Bulk Action &gt;&gt; Delete</b> .
Report	Select the option to create a report, see <a href="#">Create a Report Schedule</a> for more information.

Table 38 : Incidents Description of the Column Headings in the Incidents

Column heading	Description
Status	Displays the current status of the incident being mitigated. If the incident is still open, this column will read <b>New</b> or <b>Ongoing</b> if the incident is still open.
Incident Name	Displays the name of the incident. Click on

Table 38 : Incidents Description of the Column Headings in the Incidents

Column heading	Description
	Incident Name to move to Mitigation Console page with selected Incident.
Zone Name	Displays the name of the zone.
Service	Displays the service provided for the incident.
Attack Type	Displays the type of attack assessed by TPS.
Peak	Displays the peak attack rate in packets per second (pps) and bytes per second (bps).
Total	Displays the total number of packets and bytes passed and dropped.
Chart (pps)	Displays the graphical representation of traffic related to the incident, plotted over time. Passed packets are shown in green and dropped packets are shown in red.
Time (Created/Started/Stopped)	Displays the time stamp as follows: <ul style="list-style-type: none"> <li><b>Created</b>—Displays the time when the incident was created in red.</li> <li><b>Started</b>—Displays the time when the mitigation started for the incident in orange.</li> <li><b>Stopped</b>—Displays the time when the mitigation stopped for the incident in green.</li> </ul>
Actions	Click to view the following options: <ul style="list-style-type: none"> <li><b>Info</b>—Displays a summary of the zone incident information in a pop-up.</li> <li><b>Edit</b>—Allows you to make the changes to zone incident. For information on configurable parameters, see <a href="#">Create a New Incident (Zone)</a>.</li> <li><b>Report</b>—Based on the status of the incident, the following is displayed:</li> <li><b>Ongoing</b>—If the incident status is Ongoing, a</li> </ul>

Table 38 : Incidents Description of the Column Headings in the Incidents

Column heading	Description
	<p>Schedule Report popup is displayed. For scheduling a report, see <a href="#">Create a Report Schedule</a>.</p> <ul style="list-style-type: none"> <li>• <b>Stopped</b>—If the incident status is Stopped, a Protected Zone Incident Detail Report is generated. This report provides a detailed information about the summary, zone service charts, countermeasures deployed, countermeasures statistics, and logs.</li> <li>• <b>Mitigation Console</b>—This is displayed only when the incident status is Ongoing. Mitigation Console redirects the page to <b>Mitigation &gt;&gt; Zone Mitigation Console</b> page. Zone Mitigation Console allows you to view complete information about the selected zone incident. For more information about Zone Mitigation Console, see <a href="#">Zone Service</a>.</li> </ul>

## Create a New Incident (Zone)

Perform the following steps to create a new incident;

1. Go to **Mitigation >>Zone Incidents**.
2. Click the **+ Add New** button, a Create Incident window pops-up.

Fields	Purpose
Name	Enter the name of the new incident.
Zone	Select a configured Zone.
Service	Choose a service among the services configured for the selected zone.
Notes	Enter an optional note in the field to describe any known details about the attack.

3. Perform one of the following actions:

- **Create**—Allows you to save your changes.
- **Create & Start Mitigation**—Allows you to save and start mitigation.

[Figure 13](#) shows the Create Incident window.

Figure 13 : Create Incident

#### Create Incident

The form consists of four input fields and a set of action buttons at the bottom. The first three fields are mandatory, indicated by a red asterisk (\*). The 'Name' field contains 'Example\_Incident'. The 'Zone' field contains 'Example\_Zone'. The 'Service' field contains 'HTTP 80'. The 'Note' field contains 'Zone with HTTP Zone Service' and is highlighted with an orange border. Below the fields are three buttons: 'Cancel' (gray), 'Create' (blue), and 'Create & Start Mitigation' (green).

* Name:	Example_Incident
* Zone:	Example_Zone
* Service:	HTTP 80
Note:	Zone with HTTP Zone Service

Buttons: Cancel, Create, Create & Start Mitigation

## Stop a Zone Incident

---

While an Zone Incident is New or Ongoing, the ability to stop the incident is available. To do so, click **Edit**, and from the Edit Incident Window, click **Stop**.

Figure 14 : Stop Incident

#### Edit Incident

The form is identical to the Create Incident window, with fields for Name, Zone, Service, and Note. The Note field contains '1 - 255 characters'. At the bottom are four buttons: 'Cancel' (gray), 'Start Mitigation' (green), 'Save' (green), and 'Stop' (red).

* Name:	Example_Incident
* Zone:	Example_Zone
* Service:	HTTP 80
Note:	1 - 255 characters

Buttons: Cancel, Start Mitigation, Save, Stop

## Dst Entry Incident

An incident is created when a particular zone service is under a DDoS attack. An incident helps to track and manage the mitigation of an attack on a zone service. If a protected destination has more than one service that is simultaneously under attack, SecDevice creates an incident that is associated with the entire destination.

A zone incident captures information such as start and end time of the attack, attack type, total attack bandwidth, and peak attack rate.

A zone service incident can be created manually through GUI or aGAPI, or automatically through GUI when it receives an attack detected notification from the A10 detector (in the case of reactive deployment) or the TPS mitigator (if it's deployed in a proactive mode).

In case of proactive deployment, since the inbound traffic flows through the mitigator at all times, TPS automatically starts mitigation when it detects an attack. In case of reactive deployment, SecDevice configures TPS mitigator to advertise BGP routes and redirect the traffic to the attacked service through TPS.

For a reactive mode deployment, after the incident creation, a user can enable or disable automatic start and stop mitigation for a zone. Using SecDevice, this option can be set globally under Administration > Settings > TPS or at a per zone level through the Zone Operational Policy associated with that zone.

If the automatic start and stop mitigation is enabled, then SecDevice starts mitigation for a zone after the incident is created for any service. If there are attacks on multiple services, then SecDevice stops mitigation after the attack stops on the last of the attacked services.

---

**NOTE:** Incidents are for SecDevice TPS local incidents and are not associated to incidents on ACOS TPS devices.

---

To access the TPS Incidents page, navigate as follows:

1. Hover over **Mitigation** and click Dst Entry Incidents.
2. The list of TPS Incidents may be extensive. To help filter the information that is displayed:

- a. Enter a string in the **Search** field and select Name or IP/Subnet from the drop-down menu (the default setting is Name). This will reduce the list by displaying only incidents that match the search term.
- b. Filter the TPS Incident list by selecting from the drop-down menu.  
Select Ongoing to display only ongoing mitigation incidents.
  - Select Stopped to display only stopped mitigation incidents.
  - Select Archived to display saved mitigation incidents.
  - Select Error to display mitigation incidents where an error occurred.
  - Select All to display all incidents.
  - Enter the Created Time to list incidents created after this start time by inputting the following information in this order, two digit month, “/”, two digit day, “/”, four digit year followed by a space, two digit hour followed by a colon, two digit minute, followed by a space, and input AM or PM. For example, the Created Time for July 5, 2015, 1:10 PM, would have an input of “07/05/2015 01:10 PM”.
  - Enter the End Time to list incidents created before this time by inputting the following information in this order, two digit month, “/”, two digit day, “/”, four digit year followed by a space, two digit hour followed by a colon, two digit minute, followed by a space, and input AM or PM. For example, the End Time for July 9, 2015, 3:09 AM, would have an input of “07/09/2015 03:09 AM”. Entering both the Created Time and End Time returns a list of incidents created between the Created Time and End Time.
  - Click Search to filter the Incident list based on the parameters provided.
  - Click Reset to clear out previous input.

3. (Optional) The following buttons appear across the upper-right side of the TPS Incidents table:

- Report - Create a report. See [Create a Report Schedule](#) for more information.
- Refresh – Refreshes the information displayed for the incidents.
- Delete – Select the check box at left for one or more incidents, then click Delete.

- New – Click this button to add a new Incident (described below in [Creating a new incident](#) ).

Fields	Purpose
Name	Name of the incident. Click on Incident Name to move to Mitigation Console page with selected Incident.
Chart	Graphical representation of traffic related to this incident, plotted over time.
Dst IP/Subnet	The destination IP address/subnet associated with the incident and the protected object name (if one exists).
Devices	The managed devices that the incident was added on. Hover over devices for more details.
Device Group	The device group that is associated with this incident.
Status	The current status of the incident being mitigated. If the incident is still open, this column will read “Ongoing”.
Packets	Displays the total amount sent, and the cumulative number passed and dropped. Total amount is in blue, passed packets are in green, and dropped packets are shown in red. A percentage of passed packets and dropped packets is also displayed.
Info	<p>Highlighting or clicking on Info will provide the following information:</p> <ul style="list-style-type: none"> <li>• Attack Type: Displays the type of attack.</li> <li>• Status: Provides the current status of the incident.</li> <li>• Mitigation Started: The time when the mitigation was started.</li> <li>• Created On: The date and time the mitigation was created.</li> <li>• Created By: The user who created the mitigation.</li> </ul> <hr/> <p><b>NOTE:</b> Any notes provided will appear here.</p>

## Creating a new incident

To create a new incident;

1. Hover over **Mitigation** and click on Dst Entry Incidents.
2. Click the **New** button at upper right. A page similar to that shown below appears:

Figure 15 : Add a New Incident

Add Incident

\* Name: My-Incident

Protected Object:

Enter a new entry...  
0.0.0.0/32 (test-13)  
1.1.1.1/32 (testentry)  
1.4.5.6/32 (abc)  
10.1.11.12/32 (DST12)  
10.1.11.44/32 (dst44)

Filter By: IPv4 Address

\* Protected Object Name: Protected\_Object\_Test

\* Destination IP/Subnet: A.B.C.D/nn or A:B:C:D:E:F:G:H/nnn

Select devices from:  Device List  Device Group

Devices:

10.6.9.44  
10.6.7.8  
10.6.0.82

Mitigation Template: Default [default]

Attack Type:

Note:

Cancel Save Save & Start

3. In the **Name** field, enter the name of the new incident.
4. In the **Protected Object** field, perform one of the following:
  - Select **Enter a new entry** and then enter a Protected Object Name and Destination IP/Subnet, or select one of the existing Protected Objects that already appears in the field.
    - a. In the Protected Object Name field, enter the name of the Protected Object.
    - b. In the **Destination IP/Subnet** field, enter the IP/subnet.

- c. Choose the radio button for where you would like to create the new protected object.
- d. Select the Device List radio button to list the available devices or select the Device Group radio button to list the available group of devices.
- Select one of the existing Protected Objects. The device or device group and peacetime template will be auto-selected if it is pre-configured to the DST entry. Depending upon your selection, a drop-down menu for Devices or Device Groups appears. The **Devices** field displays a list of managed devices.
  - a. Select the IP that corresponds with the managed device where you would like to create the new incident. The **Device Groups** field displays a list of device groups for the managed devices.
  - b. Select the group that corresponds with the managed device where you would like to create the new incident.
5. Click the **Mitigation Template** drop-down menu and select a pre-configured template from the list.
6. In the **Attack Type** field, enter the type of attack (for example, SYN Flood, DNS Attack, or Unknown).
7. Enter an optional note in the **Notes** field to help later identify this incident.
8. Click **Save** to save your changes or Click Save & Start to save and start mitigation.

## Configuring Automatic Start and Stop Mitigation for Zones

SecDevice can be configured to automatically start and stop mitigation on zones based on the DDoS escalation threshold and the escalation level.

To start and stop mitigation per zone, go to Configurations >> Zone Policies / Profiles >> Zone Operational Policy and set the options in the Create or Edit Zone Operational Policy.

To configure automatically start and stop mitigation on zones:

1. Select **Administration >> Settings** from the main menu and click on TPS.
2. Click on the checkbox to enable or disable the following features:

- Auto-Start Zone Mitigation

Select to have mitigation automatically start for a zone when the first DDoS escalation threshold is exceeded. If this check box is unchecked, a new status incident will be created when the first DDoS escalation threshold is exceeded.

- Auto-Stop Zone Mitigation

Select to have mitigation automatically stop for a zone when all incidents reach escalation level zero.

# Attack Mitigation

---

Mitigation can be defined as actions or steps to reduce potential or existing crises. In relation to network traffic, the threat of Distributed Denial of Service (DDoS) attacks is what Threat Protection Service (TPS) devices attempt to mitigate.

The following topics are covered:

<a href="#"><u>Overview</u></a>	133
<a href="#"><u>Zone Mitigation</u></a>	133
<a href="#"><u>Zone Mitigation Console</u></a>	135
<a href="#"><u>Dst Entry Mitigation</u></a>	153
<a href="#"><u>BGP FlowSpec</u></a>	160
<a href="#"><u>BGP Route</u></a>	168
<a href="#"><u>BGP Route Map</u></a>	174
<a href="#"><u>End of Mitigation</u></a>	177
<a href="#"><u>Remotely Triggered Black Hole</u></a>	177
<a href="#"><u>Cloud Mitigation</u></a>	179

## Overview

The basics of mitigation require configuration of templates, binding them with the object(s) that need protection. Organization offers this in the form of configuring Zones and Destination Entries. (For more information, see [Overview of Protected Objects.](#))

When a violation action occurs, an incident is created, at which point mitigation can be started manually, or automatically, depending on the configuration (See [Configuring Automatic Start and Stop Mitigation for Zones](#) settings).

To facilitate mitigation, the SecDevice interface offers a centralized “operational center” to better view and take actions on an incident currently undergoing mitigation through the Mitigation Console page. Zones and Destination Entries each have their own specific page, [Zone Mitigation](#) and [Dst Entry Mitigation](#) respectively.

## Zone Mitigation

### Zero-day Attack Protection

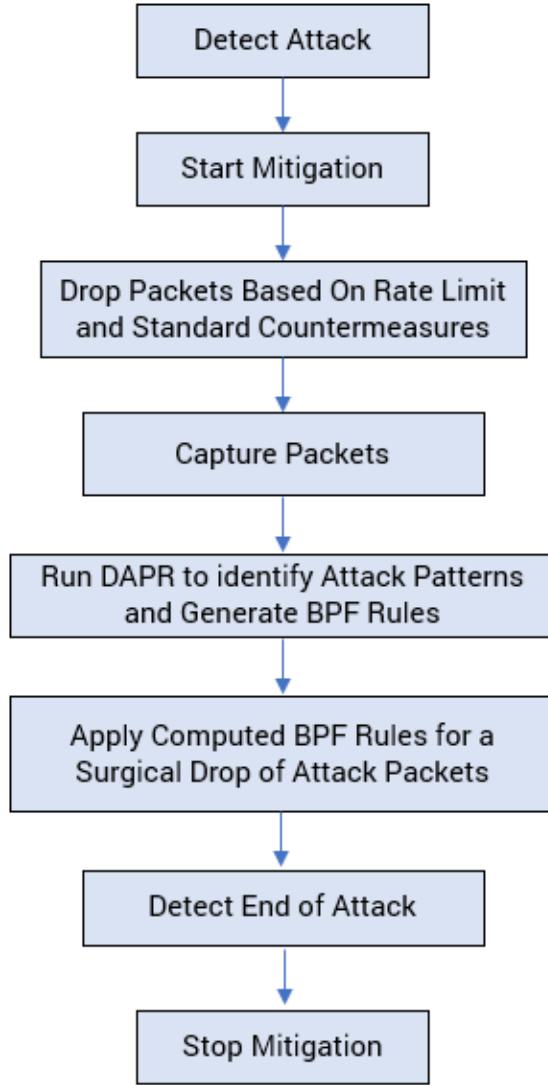
---

The emergence of unknown DDOS attacks requires a mitigation strategy that identifies new attack vectors rapidly; using automation for analysis and extraction of signatures. SecDevice supports Zero-day Attack Protection which enables the A10 Thunder TPS 3.2.3-P1 or later devices to identify and extract unknown attack signatures using machine learning techniques.

Zero-day Attack Protection is supported for TCP, UDP, DNS-TCP, DNS-UDP, SSL-L4, SIP-TCP, and SIP-UDP zone services with the port number.

[Zero-day Attack Protection](#) shows the Zero-day Attack Protection logical workflow.

Figure 16 : Zero-day Attack Protection



When an attack is detected, SecDevice starts the mitigation either manually or automatically based on the zone configuration. At the time of mitigation, the packets are dropped based on the rate limit and standard countermeasures configured. SecDevice configures TPS to capture the dropped packets and applies the Zero-day Attack Protection to identify the attack pattern. Once the attack patterns are

identified, they are used to generate BPF rules. The BPF rules can be applied on the incoming packets for a more surgical drop of attack packets.

The TPS mitigator continues to drop packets based on standard countermeasure and BPF computed via attack pattern recognition. A detector detects when the attack stops and sends de-escalation notifications to SecDevice. When the mitigator sends de-escalation to level 0, SecDevice stops mitigation.

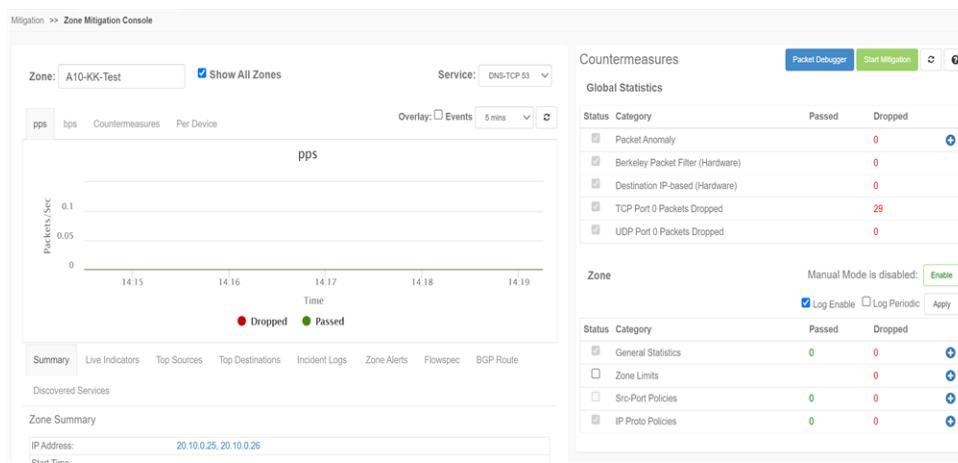
For information about configuring Zero-day Attack Protection at the zone service level, see step 8 under [Create a Zone](#). After configuring Zero-day Attack Protection, to monitor the dropped packets and packet rates, go to Mitigation >> [Zone Mitigation Console](#).

## Zone Mitigation Console

The Zone Mitigation Console page displays the information about SecDevice TPS incidents and is divided into three sections (see [Figure 17](#)):

- [Graph](#)
- [Summary](#)
- [Countermeasures](#)

[Figure 17 : Zone Mitigation Console](#)



## Graph

Go to **Mitigation >> Zone Mitigation Console**. This page displays passed and dropped charts for a zone service having an active incident. Below the chart, individual dropped/passed pps/bps chart can be viewed by clicking an appropriate tab. For example, in pps, select or deselect **Dropped** to filter this parameter from the pps graph.

Link	Description
Zone	Choose an incident from the drop-down menu to display information and a chart. You can also select the check box with <b>Show all Zones</b> .
Type	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• DST—Receives the incoming traffic from the destination.</li> <li>• SRC—Receives the incoming traffic from the source.</li> </ul> <hr/> <p><b>NOTE:</b> If source port is chosen, Live Indicators, Top Sources, Top Destinations, and Incident Logs tab are not displayed.</p>
Service	Choose a zone service to see the appropriate graph.
pps	Select pps to view a snapshot as packets per second.
bps	Select bps to view a snapshot as bits per second.
Countermeasures	Select Countermeasures to view a snapshot of the traffic data per countermeasure. The section displays information such as packets dropped based on auth, service, GLID, blacklist and source GLID. Select or deselect an indicator to filter specific countermeasure indicators.
Per Device	Select Per Device to view a snapshot of the traffic data for each TPS device. A window appears that shows per device charts for packets per second and bits per second depending on the tab selected. The peak rate tab displays stacked bar chart for passed and dropped pps/bps per device.
Overlay: Events	Select the Overlay: Events check box to display the event

Link	Description
	markers for actions that took place during the course of the pps or bps time line. Hover your mouse cursor over the event marker for more information.
Time	Choose a time duration to view the summary incident chart for 5 mins, 15 mins, 30 mins, 1 hour, 6 hours, 24 hours or All. The default time is 5 mins.
Refresh button	Click the button to manually refresh.

## Summary

The following topics are covered:

<a href="#">Summary</a>	137
<a href="#">Live Indicators</a>	138
<a href="#">Top Sources</a>	139
<a href="#">Top Destination</a>	140
<a href="#">Incident Logs</a>	141
<a href="#">Zone Alerts</a>	142
<a href="#">Flowspec</a>	142
<a href="#">BGP Route</a>	143
<a href="#">Discovered Services</a>	144

## Summary

The Summary tab provides information on the zone selected, including all zone services.

Table 42 : Zone Summary

Fields	Purpose
IP Address	Displays the IP Address of the zone.
Start Time	Displays the time when a zone started mitigation. Start time is calculated based on the current incident under mitigation
Status	Displays the current status of the zone.

Table 43 : Services section in Zone Mitigation Console

Column Heading	Purpose
Service	Displays a list of zone services configured for a zone.
Incident	Displays the status of the ongoing incidents.
Level	Displays the escalation level of the incidents.
Attack Type	Displays the type of attack a zone is under.
Packets (Passed/Dropped)	Displays the amount of packets passed and dropped.
Info	Displays the additional information. For more details, hover over the info icon.

## Live Indicators

The Live Indicators section on Zone Mitigation Console displays information for the traffic on SecDevice-managed TPS devices by charting information for various traffic packet rates. To display Live Indicators when Logs or Alerts is displayed, click on Live Indicators. The parameters for Live Indicators are dependent on the protocol. For example, the TCP protocol offers 13 indicators, while the UDP protocol offers 5.

The following are the list of indicators displayed based on the protocol selected:

Table 44 : Top Sources column headings

Indicator Type	Description
Packets per second (pps)	The UDP/TCP/ICMP/Other packets per second.
Bits per second (bps)	The UDP/TCP/ICMP/Other bits per second.
Packet Rate	Displays the graph of UDP/TCP/ICMP/Other packet forward rate.
Bit Rate	Displays the graph of UDP/TCP/ICMP/Other inbound forward bit rate in bits per second (bps).
Packet Drop Rate	Displays the graph of UDP/TCP/ICMP/Other packet drop rate.
Packet Drop Ratio	Displays the graph of UDP packet drop rate divided by UDP packet receive rate.

Table 44 : Top Sources column headings

Indicator Type	Description
Bytes to Bytes From Ratio	Displays the graph of UDP/TCP/ICMP/Other packet byte rate to the server that is divided by the packet byte rate from the server. The IP packet total length does not include the Ethernet header.
Concurrent Conns	Displays the graph of current number of UDP/TCP sessions. This value is not a rate.
Syn Rate	Displays the graph of TCP SYN packet rate.
Fin Rate	Displays the graph of TCP FIN packet rate.
Rst Rate	Displays the graph of TCP RST packet rate.
Small Window Ack Rate	Displays the graph of rate of TCP ACK packets that have a TCP window length of 0. The TCP ACK does not have SYN, FIN, or RST set.
Empty Ack Rate	Displays the graph of rate of TCP ACK packets with no data.
Small Payload Rate	Displays the graph of TCP packets with a payload that is below 536 bytes.
Syn Fin Ratio	Displays the graph of SYN rate divided by the FIN rate.
Connection Miss Rate	Displays the graph of number of new TCP connections including new SYN packets. If SYN-cookie is enabled, the ACK packets that pass SYN-cookie do not count towards this rate.

## Top Sources

The Top Source section provides a list of the most frequent source IP addresses that are attempting an attack. Click **Refresh** to update the information being displayed.

---

**NOTE:** This table is not refreshed automatically.

---

The Indicators drop-down list displays the traffic type indicators such as Packet Rate, SYN Rate, FIN Rate, RST Rate, and so on.

Table 45 : Information on Top Sources

Column Heading	Description
Source IP	Displays the source IP address of the attacker.
Country	Displays the country from where the IP address originated.
City	Displays the city from where the IP address originated.
ASN	Displays the Autonomous System Number of the IP address.
Rate	Displays the rate of the attack from the source IP address.
Action	Displays the BGP Flowspec that is associated to the zone.

## Top Destination

The Top Destination section provides a list of the most frequent destination IP addresses per service that are being attacked. The top destination IPs per service is supported from the TPS 5.0.2 and later releases. Click **Refresh** to update the information being displayed.

---

**NOTE:** This table is not refreshed automatically.

---

Table 46 : Traffic Type Indicators Supported

Detection and Mitigation	Standalone Detection only
Packet Rate	Packet Rate
Bit Rate	SYN Rate
Packet Drop Rate	FIN Rate
RST Rate	RST Rate
SYN Rate	Bit Rate
FIN Rate	
Small Payload Rate	
Empty ACK Rate	
Small Window ACK Rate	
Connection Miss Rate	

Table 46 : Traffic Type Indicators Supported

Detection and Mitigation	Standalone Detection only
Fragmented Packet Rate	

Table 47 : Information on Top Destination

Column Heading	Description
Destination IP	Displays the destination IP addresses for a service being attacked.
Rate	Displays the rate of the attack to the destination IP address.
Action	<p>Displays the following options:</p> <ul style="list-style-type: none"> <li>• Create Flowspec—Flowspec rules can be created for the corresponding zone and the IP address. For more information about creating a Flowspec, see <a href="#">Create a BGP FlowSpec</a>.</li> <li>• Deploy BGP Route—BGP route can be deployed for the corresponding top destination IP address. On deploying the BGP route, you must manually start the mitigation.</li> </ul>

## Incident Logs

The Logs section provides a list of actions that have taken place for mitigation.

Click the refresh button to update the log.

Click the **Comment** button to enter a Log Message. Enter the log message and click **Submit**. The message is sent to the Logs script.

Table 48 : Incident Logs

Column Heading	Description
Time	Displays the date and time of when the incident log is created.
Host	Displays the involved Host device.
Severity	Displays the severity level of the issue.
User	Displays the user that are involved while a logged action takes place.

Table 48 : Incident Logs

Column Heading	Description
Message	Displays more information about the mitigation action that takes place.

## Zone Alerts

The Alerts section provides a list of issues the system log has identified during mitigation.

Table 49 : Zone Alerts

Column Heading	Description
Created Time	Displays the date and time of when the notice is created.
Source	Displays the involved source IP address.
Component	Displays any pertinent component information.
Type	Displays the type of issue that is being provided.
Severity	Displays the severity level of the issue.
Description	Displays the description of the event.

## Flowspec

The Flowspec section displays the following information about the BGP Flowspec configuration:

Table 50 : Information on BGP Flowspec

Column Heading	Description
Name	Displays the name of the Flowspec.
Filter Config	Displays the configuration details of the BGP Flowspec.
Filter Action	Displays the traffic filter action applied when there is traffic matching the filtering options.
Mode	Displays the operational mode of the BGP Flowspec. It can Enabled or Disabled.
Oper	Displays the operational status of the BGP Flowspec deployment. It

Table 50 : Information on BGP Flowspec

Column Heading	Description
Status	can be Device Error, Device Partial Error, Out of Sync, or OK.
Deploy State	Displays the deployment status of the BGP Flowspec. It can be deployed, deployed pending or undeployed pending.
Actions	Allows you to perform the following: <ul style="list-style-type: none"> <li>• <b>Edit</b></li> <li>• <b>Deploy or Undeploy</b></li> <li>• <b>Delete</b></li> </ul>

## BGP Route

The BGP Route section displays the following information about the BGP route configuration:

Table 51 : BGP Route Information

Column Heading	Description
BGP Prefix	Displays the IP address/subnet for which the BGP route is configured.  <b>NOTE:</b> RTBH icon in red is displayed if the zone is under RTBH mitigation.
Route Map	Displays the route map associated with the route.
Device Group	Displays the device group of the zone.
Created By	Indicates if the BGP Route is user created.
Oper Status	Displays the operational status of the BGP route deployment as follows: <ul style="list-style-type: none"> <li>• <b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the BGP Route .</li> <li>• <b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the BGP route .</li> </ul>

Table 51 : BGP Route Information

Column Heading	Description
	<ul style="list-style-type: none"> <li><b>Out of Sync</b>—Indicates the BGP route changes that are not yet synchronized with the device(s).</li> <li><b>OK</b>—Indicates the successful deployment of the BGP route to all the devices in the device group.</li> </ul>
Auto Remove	Indicates that the BGP route will be auto removed from SecDevice and TPS device when the mitigation stops.
Actions	Allows you to perform the following: <ul style="list-style-type: none"> <li><b>Edit</b></li> <li><b>Deploy or Undeploy</b></li> <li><b>Delete</b></li> </ul>

Click + Create to [Create a BGP Route](#).

## Discovered Services

The Discovered Services section displays the services discovered, the packet rate for each service, and the Create Flowspec option for the discovered service:

Table 52 : Discovered Service Information

Column Heading	Description
Services	Displays the services that are discovered in the incoming traffic.
Packet Rate	Displays the packet rate which is the max value from all detectors in the detector group.
Actions	Allows you to create a Flowspec for the selected discovered service. For more information about creating a Flowspec, see <a href="#">Create a BGP FlowSpec</a> .

Click **Add Services to Zone** to add Discovered service(s) in the Zone configuration page.

## Countermeasures

---

The Countermeasures section of the Mitigation Console page is comprised of the following:

- [Global Statistics](#)
- [Zone and Zone Services Manual Mode](#)
- [Zone Service](#)

To access the TPS Zone Mitigation Console page, navigate as follows:

1. From **Mitigation**, click on **Zone Mitigation Console** from the main menu.
2. (Optional) Click the Packet Debugger button across the upper-right side of the Mitigation Console. A Packet Debugger page appears.

The Packet Debugger shows packets that are forwarded and dropped by mitigation based on the parameters selected. Forwarded packets are in green, whereas dropped packets are shown in red.

Figure 18 : Packet Debugger

The screenshot shows the configuration interface for a network capture session. At the top, there are fields for 'Capture Name' (set to 12811ee6-0ecf-46b2-94be-8c6), 'Timeout' (set to 60 seconds), 'Max Packets Per Device' (set to 500), 'Max Packet Length' (set to 128 bytes), and protocol selection checkboxes for IP, IPv6, TCP, UDP, and ICMP. Below these are 'Berkeley Packet Filter' and 'Device' dropdowns, and 'Start' and 'Clear' buttons. A search bar is also present.

The main area displays a table of captured packets. The columns include Index, Time, CC, Source, Port, CC, Destination, Port, Protocol, Length, Device, Drop Reason, and Match. The table lists 10 captured packets, all of which were dropped due to 'kibit rate limit'. The last row shows a detailed view of a single packet:

```

ETHERNET          23:45:24,2841724984 UTC 234 bytes
+--> Src: 00:0c:29:00:00:00 (Unknown) --> Dest: 02:1f:a8:04:00:00 (Unknown)
| Ether Type : 0x800 (IPv4)
+--> IP
| Version : 4 Header Length : 20 bytes
| Type of Service : 0x00 Total Length : 220
| Identification : 43121 Flags : 0x00
| Fragment Offset : 0 TTL : 63
| Proto : 0x0800 To : 172.17.3.68
From : 172.16.3.62

```

Field	Purpose
Capture Name	Auto populated by the uuid
Max Packets Per Device	Enter the maximum number of packets to capture from a device before it stops.
Protocols	Select the check boxes for the protocols to be captured. Leave all the boxes unchecked, if you want to capture all protocols. For example, select the IP and TCP to capture ipv4 tcp packets.
Berkley Packet Filter	Enter in Berkeley Packet Filter syntax, the expressions to filter packets, for example, ip proto 47.
Device	Choose either <b>All</b> to capture packets from all the devices in an incident, or select a single device for capture.
Time out	Enter the maximum capture duration. If the maximum packet counter per device is reached first, the capture will automatically stop. This is a required field.
Max Packet Length	Enter the maximum allowable size packet value.
Egress Only	Select the check box to enable capture of all packets

Field	Purpose
	forwarded to the destination entry.
File Size	Enter the maximum file size value.
Regex Finder	Field to search for a pattern in the payload of a packet, for example Host:*
Start	Click the button to begin packet debugging. When the process has already begun, the Start button is replaced by a Stop button. Select Stop to manually halt the process, or wait until time is up for the full captured packet session. A table displays the last 9 captured packets in real-time. When the capture is stopped, a table index is displayed with all captured packets.
Search	The Search bar is used to search packets.

---

**NOTE:** The ongoing capture will not show index and timestamp of capture. Click on a Packet to select. Use the up and down arrows on the keyboard to select the previous or next packet.

---

Table 53 : Packet Debugger Column Information

Zone Service	Description
Index	Displays the Index sequence.
Time	Displays the Timestamp of the packet.
CC	Displays the Geo-location of source ip address.
Source	Displays the Source IP address.
Port	Displays the Source Port information.
CC	Displays the Geo-location of destination ip address.
Destination	Displays the Destination IP address.
Port	Displays the Destination Port information.
Protocol	Displays the Protocol involved (TCP, UDP, ICMP, ARP, Other).
Length	Displays the length of packet.
Device	Displays the device involved with packet capture.

Table 53 : Packet Debugger Column Information

Zone Service	Description
Drop Reason	Displays the reason for dropped packet.
Match	Displays the string in payload that matches regex filter.

## Global Statistics

Shows the overall security check statistics for each TPS device. Select the check box to enable the countermeasures in the Status column. The number of packets that have been passed and dropped is listed by the protocol anomaly. Click the **Plus Sign (+)** to expand the Global Statistics Packet Anomaly section.

Table 54 : Global Statistics

Column Heading	Description
Status	Select or deselect the check box.
Category	Lists the various types of packet anomalies.
Passed	Display the aggregated total of packets passed.
Dropped	<p>Displays the aggregated total of packets dropped</p> <p><b>NOTE:</b> The countermeasure statistics drop counter increments when a packet matches the countermeasure criteria. It is not affected by the configured action to take, such as using the ignore action or blacklist instead of drop. See <a href="#">Zone and Zone Services Manual Mode</a> for flow.</p>

## Zone and Zone Services Manual Mode

The zone section allows you to include logging functionality, view general statistics, view and configure source port policies, IP protocol policies, and configure zone limits. Click the **Plus sign (+)** to expand the various available zone options. Click **More** to configure further options.

Table 55 : Displays the Zone section

Options	Purpose
Manual Mode is Disabled	<p>Allows you to implement Zone and Zone Service manual mode configurations. Click <b>Enable</b> button to add all the removed manual mode configurations back.</p> <p><b>NOTE:</b> Deselect the same button to remove the existing changes. All the changes made for Zone or Zone service under manual mode is removed.</p>
Log Enable	Select the check box to enable log functionality. This is required to be enabled in order to receive alerts for BGP failures and when networks are unreachable.
Log Periodic	<p>Select the check box to enable routine time logs.</p> <p><b>NOTE:</b> If Log Enable is not selected, this option is not selectable.</p>

Table 56 : Column Headings in Countermeasure section

Column Heading	Description
General Statistics	Views traffic packet information.
Zone Limits	Configure various rates and actions to take for a zone, similar to configuring a GLID object.
Src-Port Policies	Configure source port policies. Currently, only UDP is supported under this option.
IP Proto Policies	Configure ip protocol policies.

## Zone Service

The Zone Service section allows you to view and configure zone services. Click the **Plus sign (+)** to expand the various available zone service options. Additional configuration can be done by clicking “More...”

Existing zone service templates can be duplicated, by selecting existing mitigation level configured templates from the “Copy config from service and auto-mitigation level” drop-down list.

Table 57 : Information on Zone Service

<b>Zone Service</b>	<b>Description</b>
Service Limits	Configure GLID policy for destination IP.
Per-Source Limits	Configure GLID policy for source IP.
HTTP Authentication HTTP Service	Configure HTTP template attributes.
UDP Authentication UDP Service	Configure UDP template attributes.
TCP Authentication TCP Service	Configure TCP template attributes.
DNS-TCP Service	Configure DNS and TCP template attributes.
DNS-UDP Authentication DNS-UDP Service	Configure DNS and UDP template attributes.
SSL-L4 Authentication SSL-L4 Service	Configure SSL-L4 template attributes.
Src IP Policies	Configure source based policy using a class list.
SIP-TCP	Configure SIP and TCP template attributes
SIP-UDP	Configure SIP and UDP template attributes
Attack Pattern Filters	The number of packets dropped because the packets matched the applied signature extraction filters.  Click More... The Dynamic Attack Pattern Filters pop-up displays the following information:

Table 57 : Information on Zone Service

Zone Service	Description
	<ul style="list-style-type: none"> <li>• Device—The name of the device on which the Zero-day Attack Protection is enabled.</li> <li>• Enabled—The signature extraction filters that are learnt will be applied to filter the bad traffic and drop the matching incoming packets.</li> <li>• Filter Expression—The filter expressions applied on the traffic to pass or drop the incoming traffic. Each device can have a maximum of 5 filters applied at any point of time.</li> </ul>

To access the TPS Zone Mitigation Console page, navigate as follows:

1. From **Mitigation**, click on **Zone Mitigation Console** from the main menu.
2. (Optional) Click the Packet Debugger button across the upper-right side of the Mitigation Console. A Packet Debugger page appears.

The Packet Debugger shows packets that are forwarded and dropped by mitigation based on the parameters selected. Forwarded packets are in green, whereas dropped packets are shown in red.

Figure 19 : Packet Debugger

The screenshot shows the Packet Debugger interface with the following configuration parameters:

- Capture Name: 12811ee6-0ecf-46b2-94be-8c8
- Timeout: 60 Seconds
- Max Packets Per Device: 500
- Max Packet Length: 128 Bytes
- Protocols: IP, TCP, UDP, ICMP (checked)
- Egress Only: Unchecked
- Berkeley Packet Filter: 1-1275 characters
- File Size: 1-300 MB
- Device: All
- Regex Filter: (empty)

The table below lists the captured packets:

Index	Time	CC	Source	Port	CC	Destination	Port	Protocol	Length	Device	Drop Reason	Match
1	0	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
2	0.000000000	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
3	0.000000000	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
4	0.000000000	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
5	0.000000000	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
6	0.000000000	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
7	0.003999949	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
8	0.003999949	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
9	0.003999949	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	
10	0.003999949	Unknown	172.16.3.62		Unknown	172.17.3.68	109	234		AX1030-01	Kibit rate limit	

Below the table, a detailed packet analysis is shown for the first packet:

```

ETHERNET : 23:45:24.2041724984 UTC - 234 bytes on wire (186 bits), 234 bytes captured (186 bits, 100%)
MAC Source : 00:1f:a0:10:0c:52 -> Dest : 02:1f:a0:04:00:0f
Ether Type : 0x0800 (IPv4)
IP Version : 4 Header Length : 20 bytes
Type of Service : 0x0000 Identification : 43121 Flags : 0x00
Fragment Offset : 0 TTL : 63
Protocol : 0x6d = ? To : 172.17.3.68
Port : 172.16.3.62

```

The Capture Name field will be auto populated by the uuid.

3. In the Max Packets Per Device field, enter the maximum number of packets to capture from a device before it stops.
4. In the Protocols field, select the check boxes for the protocols to capture or leave all unchecked to capture all protocols. For example, select the IP and TCP to capture ipv4 tcp packets.
5. In the Berkeley Packet Filter field, enter, in Berkeley Packet Filter syntax, the expressions to filter packets, for example, “ip proto 47”.
6. From the Device drop-down menu, select either “All” to capture packets from all the devices in an incident, or select a single device for capture.
7. In the Timeout field, enter the maximum capture duration. If the maximum packet counter per device is reached first, the capture will automatically stop. This is a required field.
8. In the Max Packet Length field, enter the maximum allowable size packet value.
9. Select the Egress check box to enable capture of all packets forwarded to the destination entry.
10. In the File Size field, enter the maximum file size value.
11. Use the Regex Filter field to search for a pattern in the payload of a packet, for example “Host:\*”.
12. Select Start to begin packet debugging.
13. When the process has begun, the Start button will be replaced by a Stop button. Select Stop to manually halt the process, or wait until time is up for the full captured packet session. A table will display the last 9 captured packets in real-time. When the capture is stopped, a table index is displayed with all captured packets.

---

**NOTE:** The ongoing capture will not show index and timestamp of capture.  
Click on a Packet to select. Use the up and down arrows on the keyboard to select the previous or next packet.

---

Table 58 : Packet Debugger Column Information

Zone Service	Description
Index	Index sequence

Table 58 : Packet Debugger Column Information

Zone Service	Description
Time	Timestamp of the packet
CC	Geo-location of source ip address
Source	Source IP address
Port	Source Port information
CC	Geo-location of destination ip address
Destination	Destination IP address
Port	Destination Port information
Protocol	Protocol involved (TCP, UDP, ICMP, ARP, Other)
Length	Length of packet
Device	Device involved with packet capture
Drop Reason	Reason for dropped packet
Match	String in payload that matches regex filter

The Search bar can be used to search packets.

## Dst Entry Mitigation

The Mitigation Console page displays information about SecDevice TPS incidents. The Dst Entry Mitigation Console page is divided into three sections:

- Summary – The Summary section of the page provides a snapshot of the aggregate traffic of the managed devices associated with the incident, including information on its Status, Start Time, Duration, Parent Template, and Notes. You can filter based on incidents on the Dashboard / Incidents page. A report can be created by clicking on the Report button. For report generation information, see [Create a Report Schedule](#). An incident can be archived by clicking on the Archive button.

By clicking the Archive button, a message confirming the action will appear. Archiving will stop mitigation, generate an immediate report and change the incident to an archived incident. If an archived incident is opened,

countermeasures are put in a “read only” state, so functionality such as submitting or saving is not possible.

Table 59 : Summary section of the Mitigation Console

Link	Description
Name	Select an incident from the Name drop-down menu to display information and a chart.
IP Address	The IP Address of the incident.
Total Recvd/Dropped	The total number of received and dropped packets is displayed.
Status	Current status of the Incident. The list of possible statuses are as follows: Ongoing, Ongoing with Error, Stopped, Stopped with Error, and Archived. If mitigation for the Incident is still being conducted, this will read Ongoing.
Created Time	Indicates the time at which the Incident was configured.
Last Started Time	The last time the mitigation was started.
Total Duration	The duration of the mitigation.
Parent Template	The parent template initially used to create the incident is shown.
Note	Additional Information on the incident, if available.
pps	Select pps to view a snapshot as packets per second.
bps	Select bps to view a snapshot as bits per second.
Per TPS	Select Per TPS to view a snapshot of the traffic data for each TPS device. Select bps to view as bits per second or pps to display as packets per second (default).
Per CM	Select Per CM to view a snapshot of the traffic data per countermeasure. A window appears that displays charts for Dst-Rates, Port Wildcards, Application CM, Src-Based Policy, and Port CM.
“Time” (default 5 mins)	A drop-down menu allows viewing the summary incident chart for 5 mins, 15 mins, 30 mins, 1 hour, 6 hours, 24 hours or All.

Table 59 : Summary section of the Mitigation Console

Link	Description
“Refresh” button	Click to manually refresh.
PDF Report	An incident report can be generated by clicking on PDF Report. See <a href="#">Create a Report Schedule</a> for configuration options.

- Live Indicators – (Default) The Live Indicators section of the page displays information for the traffic on SecDevice-managed TPS devices by charting information for various traffic rates. The information is broken down by traffic type, specifically, the TCP packet rate, UDP packet rate, ICMP packet rate, Other packet rate, SYN request rate, and Fin packet rate. Each chart can be toggled to appear or hidden by clicking on the appropriate check boxes Syn Rate and Fin Rate are hidden by default. A drop-down menu is accessible nearby, allowing charts to show a time frame of 5 mins, 15 mins, or 30 mins. Click Refresh to manually update. The space for Live Indicators is shared with the Logs and Alerts section. To display Live Indicators when Logs or Alerts is displayed, click on Live Indicators.

Table 60 : Top Destination column headings

Top Dst column heading	Description
DST IP addr	The destination ip address (target) of the attacker.
Rate	The rate of the attack on the destination ip address.
Action	An incident can be created.

- Top Src - The Top Source section provides list of the most frequent source IP addresses that are being attacked. This can be shown by the Port (Protocol), and filtered further through the Indicators drop-down menu. Click Refresh to update the information being displayed.

---

**NOTE:** Note: This table does not automatically refresh.

---

Table 61 : Top Source column headings

Top Src column heading	Description
SRC IP addr	The source IP address of the attacker.
Rate	The rate of the attack from the source IP address.
Action	An incident can be created.

- Logs - The Logs section provides a list of actions that have taken place for mitigation. To display this information, click on Logs. Click on the refresh button to update the log. Click on the Comment button to enter a Log Message. A window appears with the Log Message: field available for any comments. Click on Submit to add the message to the Logs script.

Alerts - The Alerts section provides a list of the issues the system log has identified during mitigation.

Table 62 : Description of the Column Headings in the Alerts table

Column heading	Description
Created Time	Date and time when the notice was created.
Source	The source IP address involved is indicated.
Component	Any pertinent component information is displayed.
Type	The type of issue is provided.
Severity	The severity level of the issue is displayed.
Description	Description of the event.

- Counter Measures

The Counter Measures section of the Mitigation Console page allows mitigation for protected destinations based on security checks. The check boxes in the Status column indicate which countermeasures are enabled. Clearing the check box will disable the countermeasure on the TPS devices. The number of packets that have been passed and dropped is listed by protocol. Click the “plus” icon in the Actions column to expand the configurable countermeasure options.

Mitigation templates that have been created are available in the Countermeasures Templates drop-down list.

Table 63 : Description of the Column Headings in Countermeasures

<b>Column heading</b>	<b>Description</b>
Status	Click to select or deselect
Protocol	Lists the various protocols that are selectable from the Status check box.
Passed	Display the aggregated total of packets passed.
Dropped	Displays the aggregated total of packets dropped
Actions	Click on the “plus” icon to expand the configurable countermeasure options.

- DST Options - The Countermeasures section of the Mitigation Console page provides additional control over destination entry options.

Table 64 : Description of DST Options in Countermeasures

<b>DST Options Choices</b>	<b>Description</b>
Auto Bypass	Enable to set Operational Mode to Bypass when a mitigation is stopped.
BGP	Enable to apply Border Gateway Protocol router configuration when starting mitigation for a DST entry.
Drop Disable	Enable to allow ACOS to continue processing over-limit traffic instead of dropping it, for certain types of over-limit violations. Violations are still logged, if DDoS event logging is enabled.
Log Enable	Select this check box to enable log functionality. This is enabled by default.
Log Periodic	Routinely timed logs will occur if this check box is selected. Note, if Log Enable is not selected, this option is not selectable. This is enabled by default.
Log with sFlow	A log which includes sFlow information will occur if this check box is selected. Note, if Log Enable is not selected, this option is not selectable.

Table 64 : Description of DST Options in Countermeasures

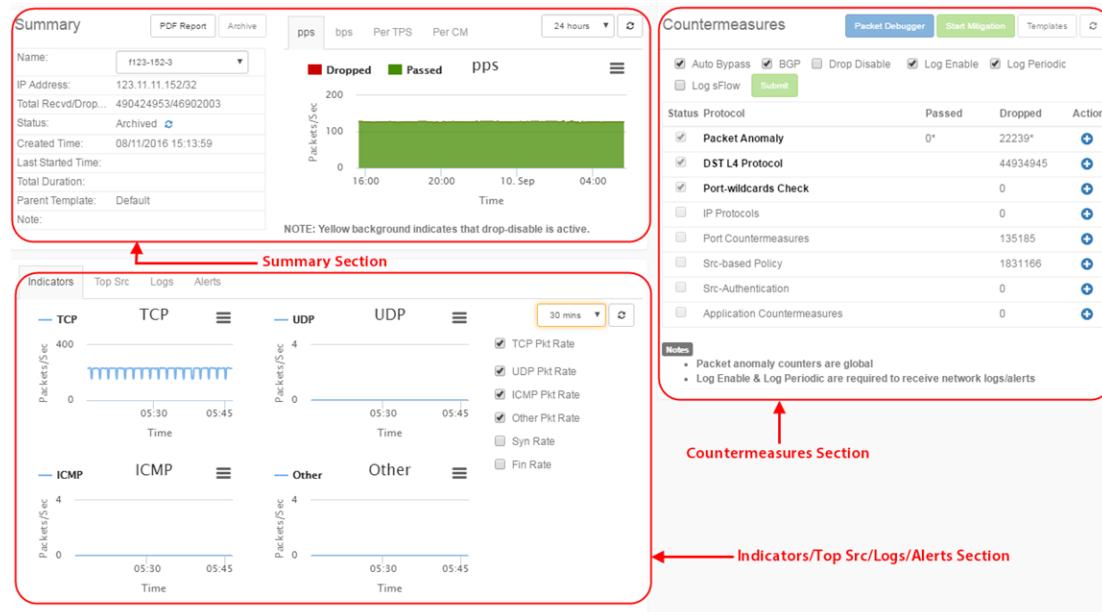
DST Options Choices	Description
Compute Top Dst	Enable computing of the top-k destination IP addresses for each destination subnet. This is currently only applicable for 3.1.4 TPS devices. This is enabled by default.
Submit	Click when done with destination entry choices.

To access the TPS Mitigation Console page, navigate as follows:

- From **Mitigation**, click on **Dst Entry Mitigation Console** from the main menu.

A window similar to that shown below appears:

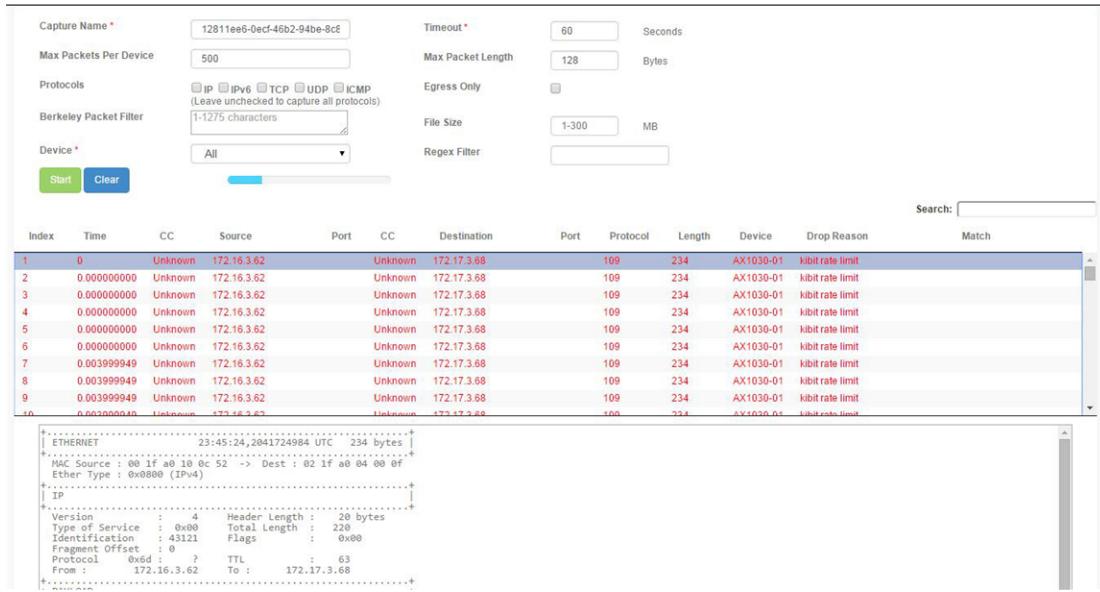
Figure 20 : Dst Entry Mitigation Console



- (Optional) Click the Packet Debugger button on the upper-right side of the Mitigation Console. A Packet Debugger page appears.

The Packet Debugger shows packets that are forwarded and dropped by mitigation based on the parameters selected. Forwarded packets are in green, whereas dropped packets are shown in red.

Figure 21 : Packet Debugger



The Capture Name field will be auto populated by the uuid.

- In the Max Packets Per Device field, enter the maximum number of packets to capture from a device before it stops.
- In the Protocols field, select the check boxes for the protocols to capture or leave all unchecked to capture all protocols. For example, select the IP and TCP to capture ipv4 tcp packets.
- In the Berkeley Packet Filter field, enter, in Berkeley Packet Filter syntax, the expressions to filter packets, for example, "ip proto 47".
- From the Device drop-down menu, select either "All" to capture packets from all the devices in an incident, or select a single device for capture.
- In the Timeout field, enter the maximum capture duration. If the maximum packet counter per device is reached first, the capture will automatically stop. This is a required field.
- In the Max Packet Length field, enter the maximum allowable size packet value.
- Select the Egress check box to enable capture of all packets forwarded to the destination entry.
- In the File Size field, enter the maximum file size value.

11. Use the Regex Filter field to search for a pattern in the payload of a packet, for example “Host: \*”.
12. Select Start to begin packet debugging. When the process has begun, the Start button will be replaced by a Stop button.
13. Select Stop to manually halt the process, or wait until time is up for the full captured packet session. A table will display the last 9 captured packets in real-time. When the capture is stopped, a table index is displayed with all captured packets.

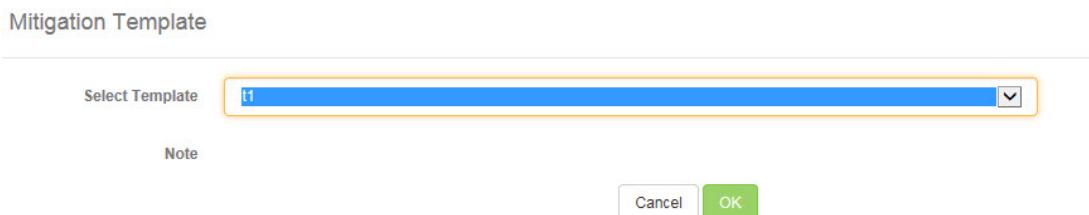
---

**NOTE:** Note: The ongoing capture will not show index and timestamp of capture. Click on a Packet to select. Use the up and down arrows on the keyboard to select the previous or next packet.

---

- Start Mitigation/Stop Mitigation button – Start or stop mitigation for the selected incident.
- Templates button – Click this button to apply an Existing Template. A page similar to that shown below appears:

Figure 22 : Mitigation Template



14. From the Existing Templates drop-down menu, select an existing template. This will automatically populate the Name field and the Note field.
15. Select OK to apply the Mitigation Template.

## BGP FlowSpec

The Border Gateway Protocol (BGP) FlowSpec provides a DDoS mitigation solution to rate limit or block the attack traffic at the edge router, or redirect the traffic to the TPS device or VRF. When SecDevice configures the FlowSpec on the TPS mitigator, it

uses BGP protocol for advertising traffic identifiers and filtering actions to the edge router.

After FlowSpec is configured, you can enable the operational mode to send the FlowSpec information to the routers. You can also disable the operational mode to pull back the FlowSpec information from the routers.

Perform the following steps to access the BGP FlowSpec page:

1. Go to **Configurations >> BGP >> Flowspec**.
2. (Optional) Enter a complete or a partial name of the BGP FlowSpec in the search field for searching the BGP FlowSpec.
3. (Optional) Click the Reset, Refresh, or Delete button to perform the corresponding action.

To create a new BGP Flowspec, click **+ Create**. For more information, see [Create a BGP Flowspec](#).

To edit a BGP Flowspec, select the Flowspec you want to edit and click Edit under Actions. Edit the Flowspec as described under Create a BGP FlowSpec.

To duplicate a BGP Flowspec, select the Flowspec you want to duplicate and click Duplicate under Actions. Edit the Flowspec as described under Create a BGP FlowSpec.

All the BGP Flowspecs created are displayed on the Flowspec page in a tabular format.

Column Heading	Description
Name	Displays the name of the BGP Flowspec.
Filter Action	Displays the type of filtering action applied to the Flowspec.
Zones	Displays the name of the zone to which the Flowspec is associated.
Mitigator Group	Displays the name of the mitigator group to which the Flowspec is associated.
Oper Status	Displays the operational status of the BGP Flowspec deployment as follows:

Column Heading	Description
	<ul style="list-style-type: none"> <li><b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the BGP Flowspec .</li> <li><b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the BGP Flowspec .</li> <li><b>Out of Sync</b>—Indicates the Flowspec changes that are not yet synchronized with the device(s).</li> <li><b>OK</b>—Indicates that the Flowspec is successfully deployed to all the devices in the device group. Here, the BGP Flowspec is created. However, it is yet to be sent to the mitigator group.</li> </ul>
Deploy State	<p>Displays the deployment status of the BGP Flowspec as follows:</p> <ul style="list-style-type: none"> <li><b>Deployed</b>—Indicates that the Flowspec is successfully deployed on all devices in the mitigator group.</li> <li><b>Deploy Pending</b>—Indicates that the Flowspec is not yet deployed on devices.</li> <li><b>Undeploy Pending</b>—Indicates that, when the BGP Flowspec is undeployed, the Flowspec will momentarily be in Undeploy Pending (transient state) and then change to Deploy Pending state.</li> </ul>
Mode	Indicates whether the BGP Flowspec rules are configured in Enabled or Disabled state.
Info	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li><b>User-created</b>—Indicates that the Flowspec is user-created.</li> <li><b>System-created</b>—Indicates that the Flowspec is system-created.</li> <li><b>Auto-remove</b>—Indicates that the Flowspec will be deleted from SecDevice and TPS device once the mitigation stops.</li> </ul>
Actions	<p>Allows you to perform any of the following:</p> <ul style="list-style-type: none"> <li><b>Edit</b></li> <li><b>Deploy or Undeploy</b></li> <li><b>Duplicate</b></li> </ul>

## Create a BGP Flowspec

Perform the following steps to create a new BGP Flowspec:

1. Go to **Configurations >> BGP >> Flowspec**.
2. Click **+ Create**.

Table 66 : Field and its purpose for Create BGP Flowspec window

Field	Purpose
Name	Enter a name for the BGP Flowspec.
Description	Enter a short description.
Operational Mode	Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Disabled</b>—Select the option to send the Flowspec configuration to the edge router</li> <li>• <b>Enabled</b>—Select the option to pull back the Flowspec configuration from the edge router.</li> </ul>
Auto Remove on Stop Mitigation	Select the check box to automatically remove the Flowspec rule from SecDevice and TPS device after the mitigation stops. The system-created BGP Flowspecs are always removed after the mitigation stops.
Zone	Choose a zone to deploy BGP FlowSpec for all the IPs or subnets in the zone.
Mitigator Group	Choose a mitigator group on which you want to configure the BGP Flowspec.
Traffic Filtering Action	Choose one of the following options that must be applied if the traffic matches the Flowspec configuration: <ul style="list-style-type: none"> <li>• <b>Deny</b>—The router denies or blocks the traffic.</li> <li>• <b>Traffic Action</b>—The attack traffic can be sampled to gather information about the attack.</li> <li>• <b>Rate</b>—The router can apply the rate limiter, in bytes per second, to apply to the traffic.</li> <li>• <b>Marking - DSCP</b>—The router can change the Differentiated</li> </ul>

Table 66 : Field and its purpose for Create BGP Flowspec window

Field	Purpose
	<p>Services (DiffServ) Code Point (DSCP) value in the IP header to the specified value.</p> <ul style="list-style-type: none"> <li>• <b>Marking - IPv6 Traffic Class</b>—The router can change the IPv6 Traffic Class value in the IP header to the specified value.</li> <li>• <b>Redirect to TPS (Extended Community / NLRI)</b>—The router sends the traffic to the TPS device. Use the TPS outside interface IP address when redirecting traffic to TPS. To configure the outside interface IP, go to <b>Devices &gt;&gt; Device List</b>. Open the Configure Mitigation window for each mitigator in the Mitigator Group to set the interface IP. For more information, see <a href="#">Device List</a>.</li> </ul> <hr/> <p><b>NOTE:</b> Depending upon the source and destination address type, <b>next-hop-nlri</b> should use either IPv4 or IPv6 address for the mitigator outside interface IP in the Redirect to TPS (NLRI).</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Redirect to VRF</b>—The router sends the traffic to the VRF device. <ul style="list-style-type: none"> <li>◦ <b>VRF Target String</b>—Enter the VRF route target.</li> <li>◦ <b>IP Host RT</b>—Enter Route target IP.</li> <li>◦ <b>Index</b>—Enter Route target IP index.</li> </ul> </li> </ul> <hr/> <p><b>NOTE:</b> VRF target string and IP Host RT/Index are mutually exclusive.</p>
Mitigators	Displays the following: <ul style="list-style-type: none"> <li>• <b>Mitigator</b></li> <li>• <b>DDoS Outside the Interface IP</b></li> </ul>
Copy Actions	Select this check box to request the router to mirror the traffic to TPS.

3. To filter the traffic based on source, select the **Filter by Source** check box. You can specify either the source IP address or the source subnet. Select the following options:

Table 67 : Field and its purpose for Filter by Source section

Field	Purpose
Source Address Type	Select one of the following options: <ul style="list-style-type: none"> <li>• <b>IPv4</b></li> <li>• <b>IPv6</b></li> </ul> <b>NOTE:</b> Always add the same address type for source and destination address type.
Source IP	Enter a source IP address of the incoming traffic that you want to filter. If you select this option, the Source Subnet field is disabled.
Source Subnet	Enter the subnet of the incoming traffic that you want to filter. If you select this option, the Source IP Host field is disabled.
Source Port	Click <b>Plus Sign (+)</b> to enter the appropriate information for the following: <ul style="list-style-type: none"> <li>• <b>Operator</b>—Choose an option from the drop-down list.</li> <li>• <b>Number</b>—Enter a value.</li> </ul>

4. To filter the traffic based on destination, select the **Filter by Destination** check box. You can specify either the destination IP address or the destination subnet. Enter the required details under Filter by Destination similar to Filter by Source.

Table 68 : Field and its purpose for Filter by Destination section

Field	Purpose
Destination Address Type	Select one of the following options: <ul style="list-style-type: none"> <li>• <b>IPv4</b></li> <li>• <b>IPv6</b></li> </ul>

Table 68 : Field and its purpose for Filter by Destination section

Field	Purpose
Destination IP	Enter a Destination IP address of the outgoing traffic that you want to filter. If you select this option, the Destination Subnet field is disabled.
Destination Subnet	Enter the subnet of the outgoing traffic that you want to filter. If you select this option, the Destination IP Host field is disabled.
Destination Port	Click <b>Plus Sign (+)</b> to enter the appropriate information for the following: <ul style="list-style-type: none"> <li>• <b>Operator</b>—Choose an option from the drop-down list.</li> <li>• <b>Number</b>—Enter a value.</li> </ul>

5. To filter the traffic based on other criteria, select the Filter by Additional Attributes check box. Enter the following details:

Table 69 : Field and its purpose for Filter by Additional Attributes section

Field	Purpose
Protocols	Click <b>Plus Sign (+)</b> to enter the appropriate information for the following:
Source or Destination Ports	<ul style="list-style-type: none"> <li>• <b>Operator</b>—Choose an option from the drop-down list.</li> <li>• <b>Number / Type / Code</b>—Enter a value.</li> </ul>
ICMP Types	
ICMP Codes	
TCP Flags	Choose one of the following options to determine the presence or absence of the TCP Flags defined under TCP Flags Bitmask: <ul style="list-style-type: none"> <li>• <b>Match Any</b></li> <li>• <b>Not Match</b></li> <li>• <b>No Match</b></li> <li>• <b>Match All</b></li> </ul>
TCP Flags Bitmask	Select one of the following check boxes:

Table 69 : Field and its purpose for Filter by Additional Attributes section

Field	Purpose
	<ul style="list-style-type: none"> <li>• CWR</li> <li>• ECE</li> <li>• URG</li> <li>• ACK</li> <li>• PSH</li> <li>• RST</li> <li>• SYN</li> <li>• FIN</li> </ul>
Fragmentation	Select one of the following check boxes: <ul style="list-style-type: none"> <li>• Is fragment</li> <li>• First fragment</li> <li>• Last fragment</li> <li>• Dont fragment</li> </ul>
Packet Lengths	Click <b>Plus Sign (+)</b> to enter the appropriate information for the following:
DSCPs	<ul style="list-style-type: none"> <li>• <b>Operator</b>—Choose <b>Equals</b>, <b>Greater than</b>, <b>Less than</b>, or <b>Between</b> option from the drop-down list.</li> <li>• <b>Length / DSCP</b>—Enter a value.</li> </ul>

6. Perform one of the following:

- **Save**—Allows you to save the BGP Flowspec configuration on SecDevice.
- **Save and Deploy**— Allows you to save and deploy the BGP Flowspec configuration on SecDevice and the associated mitigator group.

---

**NOTE:** SecDevice does not allow you to update the system created flowspec rule if **Deployed** and **Enabled**. When you **Edit** the rule, **Save** and **Save & Deploy** buttons are greyed out and a message is displayed "Please undeploy System created rule to modify."

---

## BGP Route

The Border Gateway Protocol (BGP) routes can be deployed for all the IPs or subnets in the zone to draw traffic towards the mitigator for effective attack mitigation.

When a particular IP address in a zone is under DDoS attack, the BGP route can be deployed for that specific IP address identified by the detector or on all the IPs in the zone.

On start mitigation, the BGP routes can either be deployed for all zone IPs/subnet or top-K attacked IPs based on the specified configuration. On stop mitigation, the BGP routes are removed from the devices in the device group.

Go to **Configurations >> Zone Policies / Profiles >> Zone Operational Policy**, and click **+ New Policy** or Edit Zone Operational Policy to select the zone IPs or top-K destination IPs. For more information, see [Configure Zone Operational Policy](#).

The BGP Route page provides you a list of all the BGP routes created, the associated zone, the operational status, and the actions that can be performed. You can create, edit, and delete a BGP route configuration.

Perform the following steps to access the BGP Route page:

1. Go to **Configurations >> BGP >> Route**.
2. (Optional) Enter a complete or a partial name of the BGP Route in the search field for searching the BGP Route.
3. (Optional) Click the Reset, Refresh, or Delete button to perform the corresponding action.

To create a BGP Route, see [Create a BGP Route](#).

Column Heading	Description
Route Prefix	Displays the IP address/subnet for which the BGP route is configured.  <b>NOTE:</b> RTBH button in red is displayed if the zone is under RTBH mitigation.
Zone	Displays the zone associated to the IP address or subnet.
Mitigator	Displays the device group of the zone.

Column Heading	Description
Group	
Route Map	Displays the route map associated with the route.
Oper Status	<p>Displays the operational status of the BGP route deployment as follows:</p> <ul style="list-style-type: none"> <li>• <b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the BGP Route .</li> <li>• <b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the BGP route .</li> <li>• <b>Out of Sync</b>—Indicates the BGP route changes are not yet synchronized with the device(s).</li> <li>• <b>OK</b>—Indicates that the BGP route has been successfully deployed to all the devices in the device group. It can also indicate that the BGP route has been created but not sent to the mitigator group yet.</li> </ul>
Deploy State	<p>Displays the deploy state of the route as follows:</p> <ul style="list-style-type: none"> <li>• <b>Deployed</b>—Indicates that the route is successfully deployed on all devices in the mitigator group.</li> <li>• <b>Deploy Pending</b>—Indicates that the route is not yet deployed on devices.</li> <li>• <b>Undeploy Pending</b>—Indicates that, when the BGP route is undeployed, the route will momentarily be in Undeploy Pending (transient state) and then change to Deploy Pending state.</li> </ul>
Info	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li>• <b>User-created</b>—Indicates that the route is created by a user.</li> <li>• <b>System-created</b>—Indicates that the route is created by the system.</li> <li>• <b>Auto-remove</b>—Indicates that the route will be deleted from SecDevice and TPS device once the mitigation stops.</li> </ul>
Actions	Allows you to perform the following:

Column Heading	Description
	<ul style="list-style-type: none"> <li>• <b>Edit</b>—Allows you to modify one of the previously-configured BGP Route.</li> </ul> <hr/> <p><b>NOTE:</b> Route Maps associated with Route's Mitigator Group can only be edited.</p> <ul style="list-style-type: none"> <li>• <b>Deploy or Undeploy</b>—Allows you to add or remove a previously-configured BGP Route on a device.</li> <li>• <b>Delete</b>—Allows you to delete the current BGP Route. On clicking Delete, a confirmation message is displayed. Click Submit. If SecDevice is unable to remove a BGP route on Stop Mitigation, use <b>Force Delete</b> to manually delete the route.</li> <li>• <b>Steer Traffic</b>—Allows you to add or remove a BGP Route on any of the TPS devices listed under mitigator group. This feature is introduced because in reactive deployment, when SecDevice receives zone escalation notification, it creates BGP route(s) and sends them to all devices in the zone's mitigator group. After the routes are sent to the TPS mitigator, the network traffic starts flowing through these devices. With steer traffic feature, you can selectively steer traffic through the selected devices in the mitigator group based on intensity and/or nature of the attack. To indicate that the steer traffic option is currently used, a steer tag is displayed under the Route Prefix column.</li> </ul>

## Create a BGP Route

Perform the following steps to create a BGP route:

1. Go to **Configurations >> BGP >> Route**.
2. Click **+ Create**.

Field	Purpose
BGP Route Prefix	<p>Enter the BGP Prefix IP, which can either be a specific IP or a subnet.</p> <p><b>NOTE:</b> RTBH icon in red is displayed if the zone is under RTBH mitigation.</p>
Zone (Optional)	<p>Choose a zone to associate with the BGP route. If the zone is selected, BGP Route Prefix IP must be present in the zone configuration.</p>
Mitigator Group	<p>Choose a mitigator group to apply to the BGP route.</p>
BGP Route Map	<p>Choose a route map from the drop-down list. If the zone selected already has BGP Route Map configured using the Zone Operational Policy, then the same Route Map is preselected by default in this step.</p> <p><b>NOTE:</b> If a Route Map is not selected, a default Route map called A10_Next_Hop Route map is used.</p> <p><b>NOTE:</b> If a BGP Route Map is associated with a Zone Operational Policy, it cannot be deleted.</p> <p>For information about creating a BGP route map, see <a href="#">BGP Route Map</a>.</p>
Auto remove on stop mitigation	<p>Select the check box to automatically remove the BGP route from SecDevice and TPS device after the mitigation stops. The system-created BGP Routes are always removed after the mitigation stops.</p>

3. Perform one of the following actions:

- **Save**—Allows you to save the BGP Route configuration only on SecDevice.
- **Save & Deploy**—Allows you to save and deploy the BGP Route configuration on SecDevice and the associated mitigator devices.

## Create a Cloud Mitigation Route

Perform the following steps to create a Cloud Mitigation route:

1. Go to **Configurations >> BGP >> Route**.
2. Click **+ Create Cloud Mitigation Route**. Enter the following details:

Table 72 : Cloud Mitigation Route Fields

Field	Purpose
High Traffic Destinations	<p><b>Zone:</b> Select a zone. To know how to create a new zone, see <a href="#">Create a Zone</a>.</p> <p>The associated zone status, mitigation group and configured IP/subnets are displayed. Cloud mitigated IP/subnets displays BGP Prefix(es) that are associated and configured for the zone.</p> <p>The Top Dest IPs section displays the traffic rate for top-k destination IP/subnets for the zone, based on selected indicator.</p>
Create Cloud Mitigated Route	<p>To create a Cloud Mitigation route, configure the following options:</p> <ul style="list-style-type: none"> <li>• <b>BGP Route Prefix:</b> Enter an IPv4 address, which should have minimum /24 subnet.</li> <li>• <b>Mitigator Group:</b> Select a mitigator group. See <a href="#">Device Groups</a>.</li> <li>• <b>BGP Route Map:</b> Select a BGP Route Map for Cloud Mitigation. The route maps that are enabled for cloud mitigation and are associated with a mitigator group will be available for routing. To know how to create a BGP route map, see <a href="#">Create a BGP Route Map</a>.</li> </ul> <p>In order to create a BGP Route for Cloud Mitigation, first a Route Map must be created with "Cloud Mitigation" checkbox selected, see <a href="#">Create a BGP Route Map</a>.</p>

Table 72 : Cloud Mitigation Route Fields

Field	Purpose
	<p><b>NOTE:</b> If a normal BGP route and a Cloud Mitigation route are created with the same BGP Route Prefix, the normal BGP route gets replaced by the latter.</p>
	<p><b>NOTE:</b> If you enter an IP/subnet that is not part of any zone, a caution appears.</p>

3. Perform the following action:

- **Save & Deploy**—Allows you to save and deploy the Cloud Mitigated Route configuration on SecDevice and the associated mitigator devices.

All the Route Prefixes display whether Cloud Mitigated Route is associated with them.

## Initiate Cloud Mitigation

Perform the following steps to initiate Cloud Mitigation:

1. Go to **Configurations >> BGP >> Route**.
2. Click **Edit** from the Actions column for the targeted BGP route. Make sure that Cloud Mitigation is associated with the BGP route.

Table 73 : Cloud Mitigation Fields

Field	Purpose
High Traffic Destinations	<p><b>Zone:</b> Select a zone that you want to analyze.</p> <p>All the IPs configured in the selected zone display the traffic pattern.</p>
BGP Route Map	<p>Allows you to change the BGP route map, if required. The BGP route maps are displayed as per your configuration. See <a href="#">Create a BGP Route Map</a>.</p> <p>If there is a spike in the traffic that the TPS mitigators</p>

Table 73 : Cloud Mitigation Fields

Field	Purpose
	<p>cannot handle, you can initiate <b>Cloud Mitigation</b> by changing the BGP Route Map to the wartime route. Traffic will be routed through cloud mitigation service.</p> <p>When the traffic returns to normal, you can change the BGP Route Map to the peacetime route to redirect the traffic to the TPS mitigators. To know how to create a Cloud Mitigation route, see <a href="#">Create a Cloud Mitigation Route</a>.</p>

- Click **Save & Deploy** to start Cloud Mitigation.

## BGP Route Map

A BGP route map is used by the BGP route and can be applied on the attacked IP addresses in the zone for redirecting the traffic.

A route map consists of the following:

- Tag—A name of the route map.
- Action—The action to permit or deny the traffic.
- Sequence—An ordered sequence of clauses to either permit or deny the routes.

To create a BGP Route Map, go to **Configurations >> BGP >> Route Map**. For creating a BGP Route Map, see [Create a BGP Route Map](#).

To create a Cloud Mitigation route, go to **Configurations >> BGP >> Route**. For further steps, see [Create a Cloud Mitigation Route](#).

To apply a BGP route map to a BGP route, go to **Configurations >> BGP >> Route**. For more information, see [Create BGP Route](#).

You can also select a BGP route map on the Zone Operational Policy. For more information, see [Configure Zone Operational Policy](#).

For detailed information about BGP Route Map, see DDoS Mitigation Guide.

The BGP Route Map page provides you a list of all the BGP routes maps created, the associated mitigator group, the operational status, and the actions that can be

performed. You can add a sequence, edit the mitigator group, and delete a BGP route map configuration.

Column Heading	Description
Route Map	<p>Displays the name of the BGP route map.</p> <p>This route map also displays whether any mitigation policies such as RTBH and Cloud Mitigation are applied.</p>
Mitigator Group	<p>Displays the mitigator group on which the BGP route map is applied.</p> <p>Route map can be applied on multiple mitigator groups.</p> <p>When a new mitigator is added to a mitigator group, the route map is automatically sent to the new mitigator.</p>
Oper Status	<p>Displays the operational status of the BGP route map deployment as follows:</p> <ul style="list-style-type: none"> <li>• <b>Device Error</b>—Indicates the error has occurred on all the devices while configuring the BGP route map.</li> <li>• <b>Device Partial Error</b>—Indicates the error has occurred on one or more devices while configuring the BGP route map.</li> <li>• <b>Out of Sync</b>—Indicates the BGP route map changes are not yet synchronized with the device(s).</li> <li>• <b>OK</b>—Indicates that the BGP route map has been successfully deployed to all the devices in the mitigator group. It can also indicate that the BGP route map has been created but not sent to the mitigator group yet.</li> </ul>
Actions	<p>Allows you to perform the following:</p> <ul style="list-style-type: none"> <li>• <b>Add Sequence</b></li> <li>• <b>Edit Mitigator Group</b></li> </ul>

## Create a BGP Route Map

Perform the following steps to create a BGP route map:

1. Go to **Configurations >> BGP >> Route Map**.
2. Click **+ Create**.

Table 75 : Fields and its purpose for Create BGP Route window

Field	Purpose
Tag	Enter the tag that is used to compare the injected route received on the BGP running on the TPS device with the tag available in the BGP route map.
Action	<p>Choose one of the following actions to be applied on the received packets:</p> <ul style="list-style-type: none"> <li>• <b>Permit</b></li> <li>• <b>Deny</b></li> </ul> <p>When you create a route map for Cloud Mitigation, you must create two dedicated route maps, one for peacetime and second for wartime. Select the action <b>Permit</b> for peacetime to route the traffic to the TPS mitigators and <b>Deny</b> to stop the traffic to the TPS mitigators.</p>
Sequence	Enter the sequence in which the clauses must be applied.
Mitigator Group	Select the appropriate mitigator you need to apply to the BGP route map.
RTBH	Select the check box to create an RTBH route map.
Cloud Mitigation	Select the check box to associate the BGP route map with Cloud Mitigation service.
CLI Config	Enter a set or match community string. For example, set community 100. For more information about configuring community strings, see DDoS Mitigation Guide.

3. Perform one of the following actions:

- **Save**—Allows you to save the BGP Route Map configuration only on SecDevice. Under the **Actions** column, click **Deploy** to push the route map to the mitigator devices.

- **Save & Deploy**—Allows you to save and deploy the BGP Route configuration on SecDevice and the associated mitigator devices.

## End of Mitigation

When DDoS attack subsides and the traffic goes below configured threshold, the mitigation level of the zone service in the TPS mitigator de-escalates and TPS sends de-escalation signal to SecDevice.

SecDevice automatically stops the incident when mitigation level for a given zone service reaches level 0 in all mitigators and detector, and then generates an incident report. The incident report can be automatically sent to one or more email recipients by scheduling a zone detail report with Email Report upon Incident Stop selected. To configure SecDevice to automatically send email reports, refer to [Viewing the Reports](#).

When attack stops on all services within a zone, SecDevice automatically stops mitigation if auto-stop mitigation for that zone is enabled. To configure auto-start and auto-stop mitigation, refer to [Configuring Automatic Start and Stop Mitigation for Zones](#).

## Remotely Triggered Black Hole

Remotely Triggered Black Hole (RTBH) is a filtering technique in which TPS mitigator makes peer router aware of an attack on the traffic coming towards a particular destination IP address. Instead of redirecting the traffic through TPS mitigator, edge router drops the attack traffic entering the network. A threshold is set for traffic flow and when the threshold exceeds, Border Gateway Protocol (BGP) routing updates are used to block the whole zone for a specific amount of time.

### Setup RTBH

- Go to **Configurations >> BGP >> BGP Route Map**, and enable **RTBH** check box to create a specific route map for RTBH mitigation.  
For more information, see [Create a BGP Route Map](#).

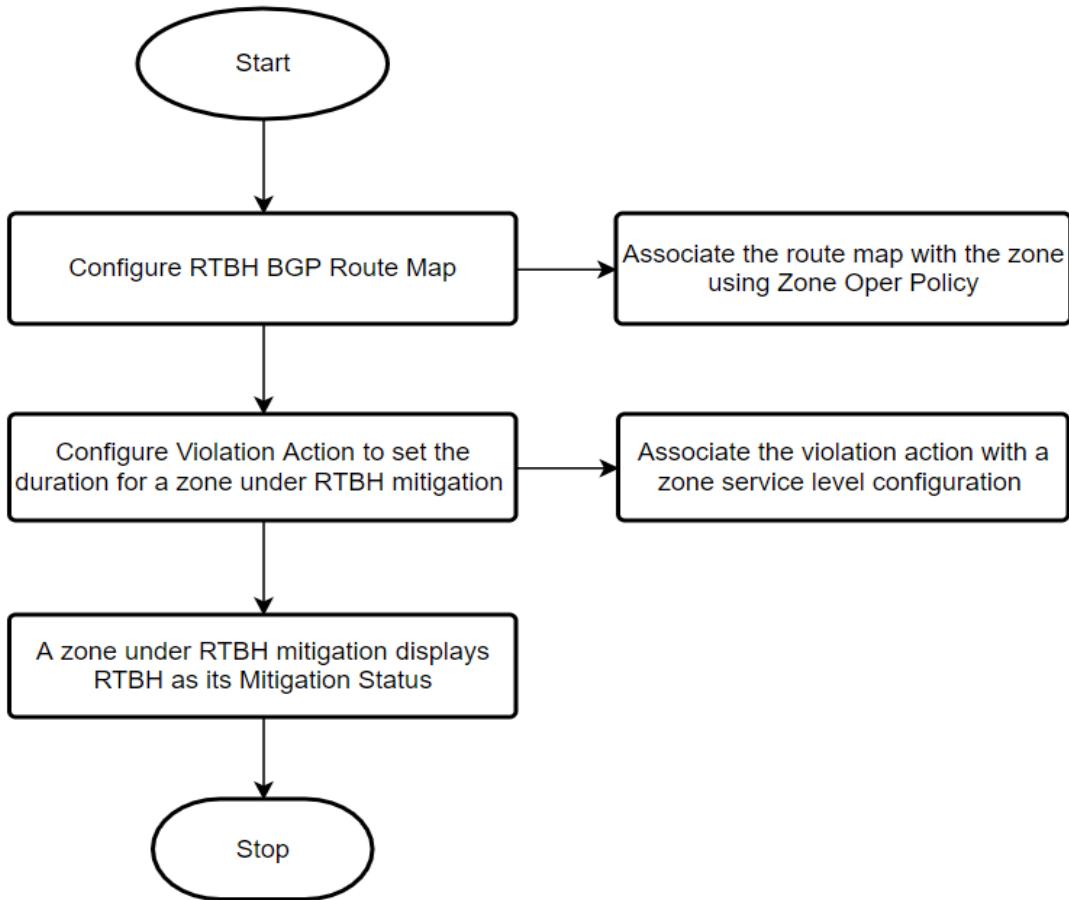
- Go to **Configurations >> Zone Policies >> Zone Operational Policy**, select the oper policy and then use the **RTBH Route map** drop-down to associate the route-map to be used for RTBH mitigation.  
For more information, see [Configure Zone Operational Policy](#).
- If BGP is enabled, use the drop-down to select the BGP Route map.  
For more information, see [Create a BGP Route](#).
- Go to **Configurations >> TPS Other Objects >> Violation Actions**, set the duration for a zone to be under RTBH mitigation.  
For more information, see [Violation Actions](#).
- Associate the violation action to the zone service level configuration (usually higher levels), so that whenever a specific indicator is violated, TPS mitigator takes the chosen action.

---

**NOTE:** By default, the attack traffic is redirected to TPS mitigators using A10\_Next\_Hop Route map.

---

The following image illustrates the workflow of RTBH:

**NOTE:**

The RTBH feature is supported only from TPS Mitigator v5.0.2-P1 and above.

---

## Cloud Mitigation

Cloud Mitigation provides the ability to mitigate increased DDoS attacks to the networks.

Normally, all traffic is mitigated by TPS mitigators deployed on the server. During wartime, if there is a spike in DDoS attacks that exceeds the capacity of locally

hosted TPS mitigators, the traffic can be routed through Cloud Mitigation service provider. When locally hosted TPS mitigator(s) is unable to handle high volume of DDoS attacks, Cloud Mitigation service can help mitigate the attacks allowing clean traffic to the server.

Cloud Mitigation can be initiated when there is a huge DDoS attack. Once the attack subsides and the traffic returns to normal, you can redirect the traffic back to the local TPS mitigators.

## Prerequisite

---

To use Cloud Mitigation, ensure that you meet the following requirements:

- Enable the DDoS Protection solution on TPS devices, SecDevice, and have the Cloud Scrubbing contract signed.
- Cloud Mitigation is supported from TPS 6.0.4 and later versions.

## Create a Cloud Mitigation Rule

---

Routing of traffic through Cloud Mitigation is achieved by learning BGP prefixes. To know how BGP Route works, see [BGP Route](#).

To use Cloud Mitigation, perform the following:

- **Create two BGP Route Maps:** One BGP route map policy should be created for peacetime, when the traffic is normal and is allowed on the locally hosted mitigators. The second BGP route map policy should be created for wartime, when the DDoS attack traffic is high and should be routed through cloud mitigation service provider. To know how to create BGP route maps, see [Create a BGP Route Map](#).
- **Configure Cloud Mitigation Route:** Enter a BGP route prefix and associate it with a mitigator group and a BGP route map. For more information, see [Create a Cloud Mitigation Route](#).
- **Initiate Cloud Mitigation:** Observe the traffic rate to the destination IP addresses. If there is spike in traffic, change the BGP Route Map to the wartime to initiate the traffic through Cloud Mitigation. For more information, see [Initiate Cloud Mitigation](#).



# Monitoring & Reporting

---

The following topics are covered:

<a href="#"><u>Reports</u></a> .....	183
<a href="#"><u>Charts</u></a> .....	194
<a href="#"><u>Zone Statistics</u></a> .....	198
<a href="#"><u>Destination Statistics</u></a> .....	199
<a href="#"><u>IP Visibility</u></a> .....	200
<a href="#"><u>Packet Capture</u></a> .....	202
<a href="#"><u>Logging</u></a> .....	208
<a href="#"><u>Events</u></a> .....	210

## Reports

SecDevice provides built-in reporting capabilities for creating summarized or detailed reports on device inventory, protected destinations, protected destination incidents, protected zones, and protected zone incidents. You can schedule these reports either to run immediately or at specified time, specify the time range to derive the events captured during the specific range of time, set the email recipients to send the reports, and finally customize the provider name and the logo for certain reports as needed.

The following topics are covered:

- [Understanding the Types of Reports](#)
- [Viewing the Reports](#)
- [Scheduling a Report](#)
- [Configuring the Report Settings](#)

## Understanding the Types of Reports

---

You can create the following types of reports:

- **Inventory Report**—Provides a summary of devices SecDevice is managing by listing the following information: Device Name, Serial Number, Model, Management IP address, ACOS version on device, date in service, and license renewal information.
- **Protected Destination Detail Report**—Provides destination entry information that includes the name of the dst entry, destination IP address or subnet, total packets received and dropped, total protected services, total number of incidents, and active incident information, including pps and bps charts.
- **Protected Destinations Summary Report**—Provides a list of all configured destination entries, their associated IP address or subnet, total packets received, passed, and dropped, and the number of protected services and incidents.
- **Protected Destination Incident Detail Report**—Displays the following information: Name of the incident, the destination IP address or subnet, total packets received, passed, and dropped, current status, creation time, last time started, duration,

parent template, bps and pps charts, indicator charts, per device charts, per countermeasure charts, countermeasures deployed information, and countermeasure statistics.

- **Protected Destination Incidents Summary Report**—In the Incident Status drop-down list, select from the available options (All, Ongoing, Stopped, Archived, Error) to configure what incidents should be included in the report.

The report includes the following incident information:

A summary providing: total number of incidents, total number of destination entries with incidents, cumulative packets received, passed and dropped, peak incident duration, and average incident duration.

An incident table providing a list of incident names, the destination IP address/subnet, the device(s)/device group, creation date, packets received, passed and dropped, attack-type, status and duration.

- **Protected Zone Detail Report**—Provides a summary of the name of the protected zone, the associated ip address(es), total packets received and dropped, total types received and dropped, and total incidents for the zone.

A Services Summary table provides a list of zone services.

A Recent Incidents table provides zone service information, the start time, and status of the incident, duration, total packets passed and dropped, and total bytes passed and dropped information.

Three types of Incident Trend Charts are provided in the report.

- Incident Trend by Incident Count helps to view the number of incoming incidents during the selected time period.
- Incident Trend by Attack Intensity helps to analyze the number of packets dropped due to attacks during the selected time period.
- Incident Trend by Peak Attack Rate helps to analyze the peak attack traffic rate during the selected time period.

---

**NOTE:** For the Incident Trend Charts, you can select the time range as Last 6 hours, Last 24 hours, Last 7 days, and Last 30 days while scheduling a report. The Custom time period is not supported.

---

A Services section provides a list of all services, IP protocols and number of protected services for the zone.

The report also provides Zone and general statistics, Zone charts showing pps and bps information, and Zone service statistics, along with pps and bps charts.

If applicable, active and closed incident information for the zone is provided, including pps, bps, and per countermeasure drop rate charts.

- **Protected Zones Summary Report**—Provides a table showing all zones, associated ip addresses, zone services, the device group for mitigation, and TPS detectors.

A chart showing the most frequently top 10 attacked zones.

A Protected Zone Service Statistics table provides a list of zones, the services offered under the zone, packets received and dropped, bytes received and dropped and incidents for the zone services.

- **Protected Zone Incident Detail Report**—Provides a summary listing the name of the incident, associated zone, the zone service, status of the incident, total packets passed and dropped, total bytes passed and dropped, peak attack rate in pps and bps, east-west traffic rate in pps and bps, the creation time, start time, and duration of the incident and attack type.

---

<b>NOTE:</b>	If the east-west traffic is insignificant (less than 20% of the total traffic) no chart for east-west traffic is prepared under Protected Zone Incident Detail Report. For more information on east-west traffic, see <i>DDos Mitigation Guide</i> .
--------------	---

---

Zone service pps, bps, protocol indicator, per device and per countermeasure drop rate charts are provided.

A Countermeasures Deployed table, countermeasures statistics, escalation log information, top sources information and general log information is also included.

- **Protected Zone Incidents Summary Report**—Provides a summary of recent protected zone incidents displaying total number of incidents, the number of protected objects that have incidents, cumulative packets passed and dropped information, peak incident duration, and average incident duration information.

Charts showing the top 10 attacked protected objects, attack intensity, attack type are provided.

A protected zone Incidents table showing the incident names, protected objects, zone service, start time of the incident, incident status, duration, attack type, and total packets passed and dropped is provided.

Three types of Incident Trend Charts are provided in the report.

- Incident Trend by Incident Count helps to view the number of incoming incidents during the selected time period.
- Incident Trend by Attack Intensity helps to analyze the number of packets dropped due to attacks during the selected time period.
- Incident Trend by Peak Attack Rate helps to analyze the peak attack traffic rate during the selected time period.

---

**NOTE:** For the Incident Trend Charts, you can select the time range as Last 6 hours, Last 24 hours, Last 7 days, and Last 30 days while scheduling a report. The Custom time period is not supported.

---

When scheduling report generation, it is recommended to have five to ten minutes of gap between each report generation. While SecDevice can handle simultaneous report generation, requesting a number of reports simultaneously may sometimes result in failure due to the sudden demand of resources required to handle simultaneous requests.

## Viewing the Reports

---

To view the reports, navigate to **Monitoring & Reporting >> Reports >> Reports**. The Reports tab allows you to view the existing inventory reports as well as TPS related reports.

You can perform the following actions on the Reports tab:

- **Email**—Select the checkbox of an existing report and click **Email**. You can also click the **Email** link under **Actions** for emailing an existing report. In order to email reports, the SMTP server must be already configured in [Notification Settings](#).
- **Download**—Click the **Download** link under **Actions**.

- **Delete**—Select the checkbox of an existing report and click **Delete**.
- **Refresh**—Refreshes the current listing.

Table 76 : Available Reports Column

Field	Description
Name	Displays the filename of the report.
Type	Displays the report type information.
Object	Lists the protected object involved with the report, if applicable.
Creation Time	Displays the date and time the report was created.
Description	Shows the description provided during report creation.
Actions	<p>Allows you to email or download an existing report.</p> <ul style="list-style-type: none"> <li>• <b>Email</b>—Email an existing report</li> <li>• <b>Download</b>—Download an existing report</li> </ul> <p>For information on creating reports, see <a href="#">Create a Report Schedule</a>.</p> <p>In order to email reports, the SMTP server must be already configured in <a href="#">Notification Settings</a>.</p>

## Scheduling a Report

To schedule a report, navigate to **Monitoring & Reporting >> Reports >> Report Scheduler**. The Report Scheduler page lists all existing Report Schedules and allows you to schedule a report creation.

You can perform the following:

- **Scheduling a Report**— On the Report Scheduler page, click **Schedule**. For more information, see [Create a Report Schedule](#).

When scheduling report generation, it is recommended to have about five to ten minutes of gap between each report generation. While SecDevice can handle simultaneous report generation, requesting a number of reports simultaneously

may, sometimes, result in failure. This can be due to the sudden demand of resources required to handle simultaneous requests.

- **Creating an Email Alert**—Configure an email alert per zone to send the incident reports to one or more recipients. The reports for different zones can be sent to different recipients. To create an email alert, see [Create a Report Schedule](#).
- **Deleting a Report Schedule**—Select the checkbox of a report schedule and click **Delete**.
- **Refreshing the Report Schedules List**—Click refresh to view the current listing.

## Create a Report Schedule

You can schedule a report either to run immediately or at a specific date and time. The reports can be scheduled to run one time or every 6 hours, 12 hours, daily, weekly, bi-weekly, or monthly. Once the reports are generated, they can be sent to one or many email recipients.

---

**NOTE:** If you are generating a report by clicking on **Report** from another page, skip to select the [Protected Destination](#)

---

### Report Details

1. Go to **Monitoring & Reporting >> Reports >> Report Scheduler**.
2. On the Report Scheduler page, click **+ Schedule** to schedule a report.
3. Expand the Report detail section to see the following fields:

Fields	Purpose
Type	Choose a report type from the following options: <ul style="list-style-type: none"><li>• Protected Zone Detail Report</li><li>• Protected Zones Summary Report</li><li>• Protected Zone Incident Detail Report</li><li>• Protected Zones Incident Summary Report</li><li>• Protected Destination Detail Report</li><li>• Protected Destinations Summary Report</li></ul>

Fields	Purpose
	<ul style="list-style-type: none"> <li>Protected Destination Incident Detail Report</li> <li>Protected Destination Incidents Summary Report</li> <li>Inventory Report</li> </ul>
Protected Zone	<p>Enter or select a Protected Zone.</p> <p><b>NOTE:</b> Protected Zone is displayed for Protected Zone Detail Report, Protected Zone Summary Report, Protected Zone Incident Detail Report, and Protected Zone Incident Summary Report.</p> <p><b>NOTE:</b> A check box to <b>Select All Zones</b> is displayed for Protected Zone Summary Report and Protected Zone Incident Summary Report.</p>
Protected Zone Incident	<p>Enter or select the Protected Zone Incident.</p> <p><b>NOTE:</b> Displayed only for Protected Zone Incident Detail Report.</p>
Protected Destination	<p>Enter or select the Protected Destination.</p> <p><b>NOTE:</b> Displayed only for Protected Destination Detail Report.</p>
Incident	<p>Enter or select the name of the incident.</p> <p><b>NOTE:</b> Displayed only for Protected Destination Incident Detail Report.</p>
Time Range	<p>Choose one of the following options to specify the time range to restrict the data of the report that contains the event:</p> <ul style="list-style-type: none"> <li>Last Hour</li> <li>Last 6 Hours</li> <li>Last 24 Hours</li> </ul>

Fields	Purpose
	<ul style="list-style-type: none"><li>• Last 7 days</li><li>• Last 30 days</li><li>• Last Calendar Month</li><li>• All</li><li>• Custom</li></ul> <p><b>NOTE:</b> Time Range is not displayed for Inventory Report, Protected Destination Incident Detail Report, and Protected Zone Incident Detail Report.</p> <p><b>NOTE:</b> Last Calendar Month option is available only for Protected Zone Detail Report, Protected Zones Summary Report, Protected Zone Incidents Summary Report.</p>
Incident Status	<p>Choose one of the following options:</p> <ul style="list-style-type: none"><li>• All</li><li>• Ongoing</li><li>• Stopped</li><li>• Archived</li><li>• Error</li></ul> <p><b>NOTE:</b> Incident Status is displayed only for Protected Destination Incidents Summary Report.</p>
Schedule Type	<p>Select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Immediate</b>—Generates a report immediately.</li><li>• <b>Schedule</b>—Schedules a report at a specified time. Perform the following:</li></ul>

Fields	Purpose
	<ul style="list-style-type: none"> <li>○ <b>Start Datetime</b>—Enter the start date and time in the following format: mm/dd/yyyy HH:MM AM/PM</li> <li>○ <b>Schedule Option</b>—Choose an option to determine how frequently the report must be generated.</li> </ul>
<b>Format</b>	Select the check box for the suitable file format of the report. You can either select one or both of the following options : <ul style="list-style-type: none"> <li>• PDF</li> <li>• CSV</li> </ul>
<b>Email Recipient</b>	Enter the email addresses of the recipients to whom you wish to send the reports. Use a comma to separate email addresses.

4. Expand the **Report Customization** section. to see the following fields:

Fields	Purpose
<b>Filename (Prefix)</b>	Enter the prefix that precedes the report name. For example, if you enter Report01, the report filename name can be <b>Report01-20180927-&lt;title&gt;.pdf</b> .
<b>Title</b>	Enter the name of the report. This appears as the <b>Report_Title</b> within the generated document. See <a href="#">Figure 23</a> for an example.
<b>Include Sections</b>	Select the check boxes to include the information you want in the report.  <b>NOTE:</b> If you have an existing zone incident summary report that is periodically scheduled from previous releases (SecDevice 5.0.6 and earlier), edit the schedule to include the new sections provided in SecDevice 5.0.7.

Figure 23 : Report Title in pdf

The Report Title will appear here within the pdf file.

Report Generation Time: 2017-12-13 15:20:47 PST  
 Time Period (Start - End): 2017-12-13 14:20:47 PST - 2017-12-13 15:20:47 PST

Protected Zones Summary				
Zone Name	IP Address	Services	TPS Mitigator Group	TPS Detector
agapi_tmp_1508358920	37.101.226.31, 45.31.161.0/24, e086:a12c:1 371:fe9b:44b9:abc3:c73d:b2 20, 2bb5:73b3:d0ae:18a0::/64	TCP 8080	group1	

5. Expand the **Report Description** section, in the **Description** field, enter a description about the scheduled report. This information will appear in the Description column in the Reports and Report Scheduler table.
6. Click **OK**.

The following table describes the information shown in each column.

Table 77 : Report Schedules Columns

Column Heading	Description
Report Type	Displays the report type information.
Object	Displays the protected object involved with the report scheduler if applicable.
Description	Displays the description provided during report creation.
Scheduled	Displays the time scheduled for report generation.
Start Time	Displays the time when the schedule was started.
Next Run Time	Displays the next period of time when a report will be generated.
Actions	Click on the hyperlink to be taken to the Reports page.

## Configuring the Report Settings

SecDevice provides the ability to customize certain reports by adding the provider name and the logo to the cover page of the reports. When the reports are generated, the first page reflects the provider name, the logo at the top, time period states the time and date rage, and report generation time.

The Report Settings is applicable for the following reports:

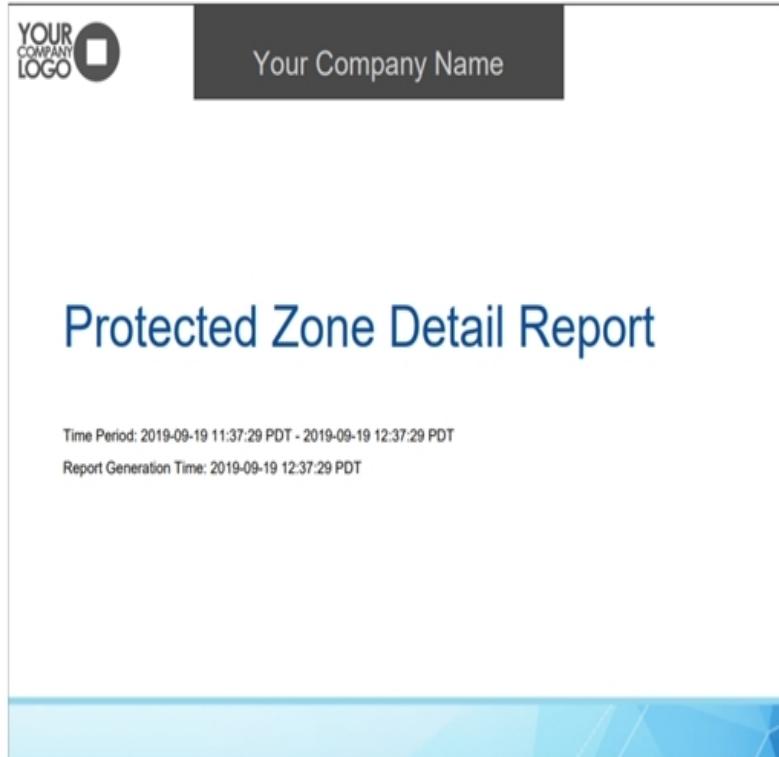
- Protected Zone Detail Report
- Protected Zones Summary Report
- Protected Zone Incident Detail Report
- Protected Zone Incidents Summary Report

To customize the reports, perform the following:

1. Navigate to **Monitoring & Reporting >> Reports >> Settings**.
2. On the Settings page, enter the provider name in the **Provider Name** box. The provider name can have up to 32 characters.
3. For logo, click **Choose File** and select the logo image. The log can have a maximum dimension of 500 x 250px. The logo file size should not exceed 200KB.
4. For Background Image in the cover page, you can select either the A10 default image or a custom image. To choose a custom image, click Choose File and navigate to the desired location to select the file. The background file size should not exceed 500KB.
5. (Optional) Select check box to auto generate zone incident detail report on incident stop.
6. (Optional) Select check box to auto generate zone detail report on mitigation stop.
7. Enter the email signature in the **Email Signature** box.
8. Select the **Use Default Email Settings** check box (default checked) to use the default Email Sender for emailing Reports.. The default email settings are under **Administration >> Settings >> Notification >> Notification settings** section.
9. If the above check box is unchecked, you can configure a Dedicated Email Sender address for emailing reports.
10. Perform one of the following:
  - Click **Reset** to remove the logo, delete the provider name, and remove the background image. It basically resets the page.
  - Click **Submit** to apply the report settings.

[Figure 24](#) shows a sample report customized with “Your Company Name” as the provider name and “Your Company Logo” as the logo.

Figure 24 : Report Settings Sample Output



## Charts

Charts provides information in a series of user-friendly graphical charts showing the traffic on the SecDevice device plotted over time. Information is plotted for specified managed devices.

You can view the following charts:

- [Zone Charts](#)
- [Destination Charts](#)
- [Device Charts](#)

## Zone Charts

The charts can display information for all zone traffic on devices.

The following Zone Charts are displayed when a standalone detector and a mitigator is selected:

- Packets per second (pps)
- East-West (e-w) pps
- Bits per second (bps)
- East-West (e-w) bps

For more information on east-west traffic, see [Zone Incident](#) page.

In addition to the above charts, the indicator charts are displayed depending on the type of zone service selected. For example, the following indicator charts are displayed when you select an HTTP service.

- Packet Rate
- Bit Rate
- Bytes to Bytes From Ratio
- Concurrent Conns
- Syn Rate
- Fin Rate
- Rst Rate
- Small Window Ack Rate
- Empty Ack Rate
- Small Payload Rate
- Syn Fin Ratio
- Conn Miss Rate

To access the TPS Charts page, navigate as follows:

1. Navigate to **Monitoring & Reporting >> Charts >> Zone Charts**.
2. Click the **Zone** drop-down menu and select a configured zone.
3. Click the **Zone Services** drop-down menu and select All Services, a Zone Service or Zone Source Service to view the statistics for the specified selection.

**NOTE:** If zone source service is chosen the Protocol Indicators Detection section is masked.

4. Click the **Device** drop-down menu and select a detector or a TPS mitigator to view the traffic flowing through the device or select **All Mitigators** to view the total traffic flowing through all mitigators for that zone. The drop-down lists the ADC and CGN devices, if any.
5. From the time drop-down, specify the time frame (X-axis) over which the traffic will be plotted. The time selections are 5 minutes (default), 15 minutes, 30 mins, 1 hour, 6 hours, 24 hours, or Custom Time.

If Custom Time is selected, the Start Time and End Time is enabled. Select the start time and end time in the respective fields and click **Apply**.

## Destination Charts

Charts provides information in a series of user-friendly graphical charts showing the traffic on the SecDevice device plotted over time. Information is plotted for specified managed devices.

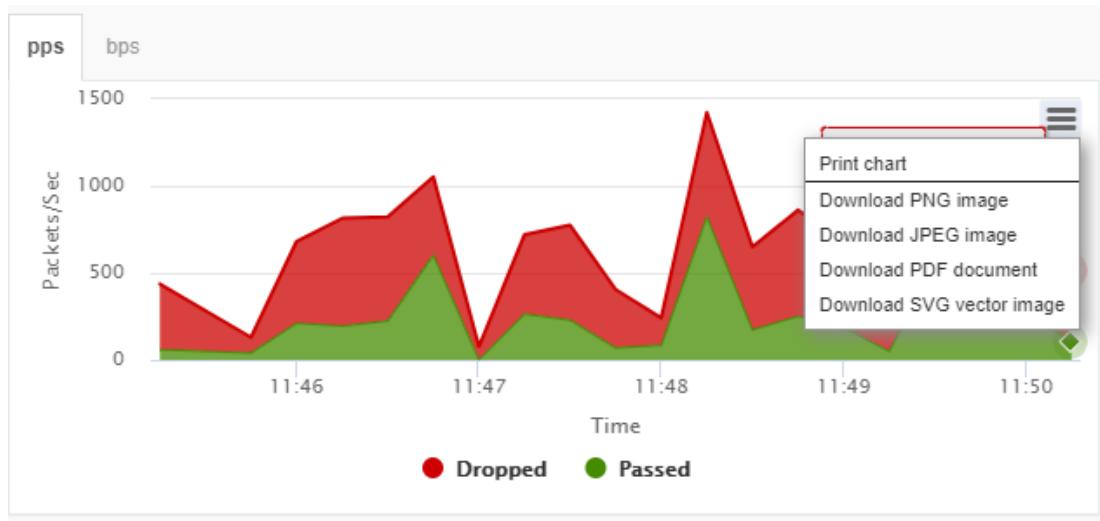
The Destination Charts page provides the following charts:

- pps (packets per second) / bps (bits per second)
- TCP (TCP packets per second)
- UDP (UDP packets per second)
- TCP Sessions (TCP sessions per second) / UDP Sessions (UDP sessions per second)
- ICMP (ICMP packets per second)
- Other (Other packets per second)

To access the TPS Charts page, navigate as follows:

1. Navigate **Monitoring & Reporting >> Charts >> Destination Charts**.
2. Select a protected destination to view its traffic charts. Use filters to select a subset of protected destinations. The filters can be the name and the destination IP address.
3. Select a TPS mitigator associated with that protected destination.
4. Choose a time duration using the drop-down menu list.
5. (Optional) Print charts (as well as download the image in a variety of formats) by clicking the menu icon at the upper-right of the chart (see [Figure 25](#)).

Figure 25 : Monitoring & Reporting >> Destination Charts



#### Details:

- The Reporting Charts page will automatically refresh itself every 30 seconds.
- Passed packets are charted in green, whereas Dropped packets are shown in red.
- By default, all charts display information in packets-per-second (as opposed to bits-per-second).
- Plotting data for several devices over many days could take a long time. Therefore, as a best practice, it is recommended that you limit the number of devices queried to no more than the following:
  - 1 device for 10 days of data
  - 2 devices for 5 days of data

- In addition, it is recommended that you do not refresh your Web browser while the Reporting Charts page is still loading a chart containing large amounts of data, as doing so may cause SecDevice to hang and could require a reboot.

## Device Charts

The Device Charts page provides the following charts:

- pps (packets per second)
- BPS (Bits per second)

To access the Device Charts page, navigate as follows:

1. Navigate to **Monitoring & Reporting >> Charts >> Device Charts**.
2. Select a TPS mitigator to view its traffic charts.
3. Choose a time duration using the time drop-down list. If you select Custom Time from the drop-down list, enter the start time and end time in the respective boxes. Click **Apply**.

## Zone Statistics

The Statistics page displays counters for configured zones. The statistics are received by requesting information from the devices through aXAPI commands, and this page serves the same function as running the “show statistics” for the zone and zone service.

To access the TPS Zone Statistics page, navigate as follows:

1. Navigate to **Monitoring & Reporting >> Statistics >> Zone Statistics**. Zone Statistics displays the list of TPS statistics. The list may be extensive.
2. Use the following options to filter the displayed information:
  - Click the Zone drop-down menu and select a configured zone.
  - Click the Zone Services drop-down menu and choose either a Zone Service or Zone Source Service to view the statistics for the specified selection.

- Click the drop-down menu and select **All Devices** or select a specific managed device.
3. (Optional) Choose the following from the top right side of the TPS statistics table:
- Exclude 0s—Displays the counters with non-zero statistics. The zone statistics with the value of zero are excluded from the table.
  - Rate—Displays a non-cumulative statistics value that is calculated as follows:
    - $(\text{Previous statistics} - \text{Current statistics}) / \text{time interval}$
  - Autorefresh – Refreshes the value of the zone statistics every 5 seconds.

## Destination Statistics

The Statistics page displays counters for a variety of protocols (TCP/UDP), applications (DNS/HTTP), as well as for sessions and anomaly drops. The statistics are received by requesting information from the devices through aXAPI commands, and this page serves the same function as running the “show” CLI command from a device. You can display this information globally or for a particular managed device.

To access the TPS Statistics page, navigate as follows:

1. Navigate **Monitoring & Reporting >> Destination Statistics**.
  2. The list of TPS statistics may be extensive. To help filter the information that is displayed, use the following options:
    - Click the drop-down menu and select **All Devices** or select a specific managed device.
    - The **Global** radio button is selected by default (displaying traffic for a managed device in both directions).  
However, you can select the **DST Entry** radio button to limit the statistics page to display counters for traffic going to a particular managed device.
3. (Optional) Choose the following from the top right side of the TPS statistics table:
- Exclude 0s—Displays the counters with non-zero statistics. The zone statistics with the value of zero are excluded from the table.
  - Rate—Displays a non-cumulative statistics value that is calculated as follows:

- (Previous statistics - Current statistics) / time interval
  - Autorefresh – Refreshes the value of the destination statistics every 5 seconds.
4. In the current release, a number of tabs are available from the Statistics Summary page. These options are:
- Summary (displayed by default)
  - TCP
  - UDP
  - ICMP
  - Other
  - DNS
  - HTTP
  - SSL-L4
  - Sessions
  - Switch
  - IP/IPv6
  - Anomaly Drops

For descriptions of the fields/counters that appear in any of the tabs above, please refer to the SecDevice online help.

## IP Visibility

TPS detector auto-discovers and breaks down the network hierarchy, determines the active subnets and hosts within the network object. The IP Visibility pages in SecDevice enhances visibility of your network by displaying all the discovered IP addresses/networks and anomaly IP addresses/network.

The following topics are covered:

- [Network Object](#)
- [Zone](#)

## Network Object

---

To monitor the network object and devices, navigate as follows:

1. Navigate to **Monitoring & Reporting >> IP Visibility >> Network Object**.
2. From the **Network Object** drop-down list, select a network object that you want to monitor.
3. From the **TPS Detector** drop-down list, select a device IP address.
4. Click **Show**.

The IP subnets with discovered thresholds are displayed. The anomalies are highlighted. Clicking on a discovered or configured subnet of /24 or smaller displays the top active IP addresses discovered and the current and max traffic (in pps & bps) observed, along with the threshold value.

The pps and bps can be helpful in deciding the per-host static detection thresholds based on the top-k IP-host receivers' peak rates and using the same thresholds for network objects.

## Zone

---

To monitor the victim IP enabled zone and devices, navigate as follows:

1. Navigate to **Monitoring & Reporting >> IP Visibility >> Zone**.
2. From the **Victim IP Enabled Zone** drop-down list, select a zone that you want to monitor.
3. From the **TPS Detector** drop-down list, select a device IP address.
4. From the **Indicator** drop-down list, select either the packet rate or bit rate as indicator.
5. Click **Show**.

The discovered IP addresses and associated packet rate or bit rate are displayed.

---

**NOTE:** The number of results depend on the detection threshold Top-K Destination IPs configured under the zone template. For more information, see [Create a Zone](#).

---

## Packet Capture

SecDevice provides on-demand or automatic packet capture at incident start or during the ongoing incident.

You can access Packet Capture by navigating to Monitoring & Reporting >> Packet Capture

Packet Capture allows you to view the following:

- **Jobs**-Packet capture jobs are displayed for both zones and destination entry protected objects.

To create a new job for packet capture, click + New Capture Job.

To view the existing packet capture job, click View under Actions.

To stop packet capturing, click Stop under Actions.

- **Templates**-Packet Capture template helps to fine tune packet capturing using the following configuration options:

- Length per packet (number of bytes) - Configures the allowable length per packet that can be captured.
- Packet Direction- Configures whether to capture all packets, only forward packets, or only drop packets.
- Berkeley Packet Filter - Uses the Berkeley Packet Filter to filter packet capture.
- File size - Configures the maximum size the packet capture file can grow to before stopping the packet capture.
- Maximum number of packets coming from a device - Configure the maximum allowable number of packets that can come from a device for the packet capture.

- **Policy**-Binds the packet capture template with the policy controls for enabling packet capture at incident start or during the ongoing incident. Sends the packet capture complete notification to the configured email recipients.

## Jobs

Packet capture jobs are displayed for both zones and destination entry protected objects. To view jobs, navigate to Monitoring & Reporting >> Packet Capture >> Jobs.

The following diagram shows the packet capture jobs created at incident start or during ongoing incidents:

Figure 26 : Packet Capture List View

Search		Q	Capture Name					Refresh	Delete	New Capture Job
	Capture Name	Description	Protected Object	Devices	Created Time	Status	Actions			
<input type="checkbox"/>	auto_cap_20201219_010728	auto capture: incident detect...	detection1_zone73	1 Device(s)	2020/12/18 09:07:28	CAPTURING	<a href="#">View</a>   <a href="#">Download</a>   <a href="#">Stop</a>			
<input type="checkbox"/>	auto_cap_20201219_00572C	auto capture: incident detect...	detection1_zone73	1 Device(s)	2020/12/18 08:57:20	FINISHED	<a href="#">View</a>   <a href="#">Download</a>   <a href="#">Stop</a>			
<input type="checkbox"/>	auto_cap_20201219_005603	auto capture: incident detect...	detection1_zone73 (...)	1 Device(s)	2020/12/18 08:56:03	FINISHED	<a href="#">View</a>   <a href="#">Download</a>   <a href="#">Stop</a>			

The following statuses are displayed in the Packet Capture Live View:

- Capturing—Indicates that the packet capturing is in progress
- Transferring—Indicates that the captured packets are being transferred
- Parsing—Indicates that the captured packets are being parsed
- Finished—Indicates that the packet capture is complete
- Idle—Indicates that the packet capture job is currently not active. The inactivity may be because the job is in between an ongoing incident capture interval or a mitigator has reached its maximum capture-config allowed.

The real-time packet capturing can be viewed when the packet capture status is Capturing. To view a packet capture, select View under Actions. The following page is displayed:

Figure 27 : Packet Capture Detailed Live View

Capture Info: test-live-view											
Description											
Capture Config		38463f78-b6bc-4e33-be2e-561da21cf9fe									
Capture Status		CAPTUREING									
Zone Name		yliu-zone									
Scope		Entire Zone									
Device		2 Device(s)									
Length per Packet		128									
Packet Direction		all									
Berkeley Packet Filter		10 MB									
File Size		0 Packets									
<a href="#">Statistics</a>		3 seconds				Pause					
Index	Time	Src CC	Source	Src Port	Dst CC	Destination	Dst Port	Protocol	Length	Device	Comment
2018-02-12 06:47:31.275000		DE	80.226.244.39	19233	US	20.30.0.15	53	UDP	60	vThunder	ddos action:drop, entryzone, reason...
2018-02-12 06:47:30.999000		US	54.52.126.93	19232	US	20.30.0.15	1111	TCP	60	vThunder	ddos action:drop, entryzone, reason...
2018-02-12 06:47:30.999000		US	20.10.0.11		US	20.30.0.15		ICMP	60	vThunder	ddos action:forward, entryzone
2018-02-12 06:47:30.999000		AU	1.1.1.1	19232	US	20.30.0.15	0	TCP	154	vThunder	ddos action:drop, entryzone, reason...
2018-02-12 06:47:30.999000		AU	1.1.1.1		US	20.30.0.15	47	134	vThunder	ddos action:forward, entryzone	
2018-02-12 06:47:30.999000		US	20.10.0.11	19233	US	20.30.0.15	8080	TCP	60	vThunder	ddos action:drop, entryzone, reason...
2018-02-12 06:47:30.999000		FR	148.60.129.152	19233	US	20.30.0.15	4500	TCP	60	vThunder	ddos action:drop, entryzone, reason...

**NOTE:** The real-time packet capturing view cannot be seen when the packet capturing status is any of the following—Transferring, Parsing, Finished, or Error.

For every 3 seconds (by default), the latest captured packet will be refreshed on the packet list. The following functions are available:

- Change refresh interval.
  - Pause the refresh.
  - View packet dissect.

**NOTE:** Red-colored text is used to identify packets that have been forwarded or dropped. By selecting a packet, the packet information will be displayed in the window below the Packet Capture table.

**NOTE:** When the packet capture job is finished, the pcap view automatically appears.

Field	Description
Index	Index number for the packets captured.
Time	The date and time when each packet was captured.
Src CC	The country where the packet originated.
Source	The source IP address of the packet.
Src Port	The source port that the packet came from.
Dst CC	The country where the packet is destined to go.
Destination	The destination IP address of the packet.
Dst Port	The destination port that the packet is being routed to.
Protocol	The protocol that is involved with the packet capture.
Length	The length of the packet.
Device	The device that handled the packet.
Comment	Additional information related to the packet, such as the reason a packet was dropped. Hover over the item to read the available comments.

[Figure 28](#) shows an example of the Comment that appears when hovering over an item in the Comment column.

Figure 28 : Packet Capture Comment

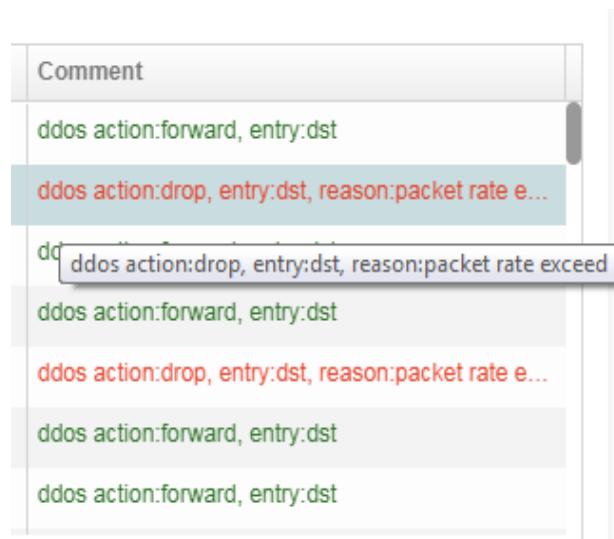


Figure 29 : Finished Packet Capture Job Log

The following illustrates the log of a finished packet capture job.

Capture Info: trina-test-3											
Total: 60 Packets											
Index	Time	Src CC	Source	Src Port	Dst CC	Destination	Dst Port	Protocol	Length	Device	Comment
6	Wed, 07 Feb 2018 10:45:11 GMT	AU	1.1.1.1		US	20.30.0.15		47	134	mitigator2	ddos action:forward, entryzone
7	Wed, 07 Feb 2018 10:45:16 GMT	US	20.10.0.11		US	20.30.0.15		ICMP	60	mitigator2	ddos action:forward, entryzone
8	Wed, 07 Feb 2018 10:45:14 GMT	AU	1.1.1.1	60998	US	20.30.0.15	0	TCP	154	mitigator2	ddos action:drop, entryzone, reason...
9	Wed, 07 Feb 2018 10:45:14 GMT	US	20.10.0.11	61001	US	20.30.0.15	8080	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
10	Wed, 07 Feb 2018 10:45:11 GMT	US	23.109.26.113	60999	US	20.30.0.15	1111	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
11	Wed, 07 Feb 2018 10:45:04 GMT	US	20.10.0.11	60999	US	20.30.0.15	8080	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
12	Wed, 07 Feb 2018 10:45:16 GMT	AU	1.1.1.1	61000	US	20.30.0.15	0	TCP	154	mitigator2	ddos action:drop, entryzone, reason...

```

*-----*
* Ethernet: 02:45:86:12:49:97 <-> 02:45:86:12:49:97 (UTC) 154 bytes *
*-----*
* MAC Source : 00:0c:29:07:81:26 --> Dest : 00:0c:29:8c:fa:95 Ether Type : 0x8000 (IPv4)
*-----*
* IP Ver: 4 Fwd: 1.1.1.1 To : 20.30.0.15 Total Len: 148 Hdr Len: 20 bytes
*-----*
* Type of Service : 0x00 Identification : 24537 Flags : 0x00
* Fragment Offset : 0 Protocol : 0x06 TCP TTL : 63
*-----*
* TCP
*-----*
* Source Port : 60998 Destination Port : 0
* Sequence number : 274354200 Acknowledgment : 0
* Control bits : 0x0000 FIN (No more data from sender)
* .0..... SYN (Synchronize sequence number)
* ..0... RST (Reset the connection)
* ...0.. PSH (Push function)
* ....0.. ACK (Acknowledge field sign.)
* .....0.. URG (Urgent pointer field sign.)
*-----*
* PAYLOAD
*-----*
0000 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0010 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0020 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0030 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0040 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X

```

Figure 30 : On-going Packet Capture Job Log (Live View)

The following illustrates the log of an on-going packet capture job live view.

Capture Info: trina-test-3											
Total: 60 Packets											
Index	Time	Src CC	Source	Src Port	Dst CC	Destination	Dst Port	Protocol	Length	Device	Comment
6	Wed, 07 Feb 2018 10:45:11 GMT	AU	1.1.1.1		US	20.30.0.15		47	134	mitigator2	ddos action:forward, entryzone
7	Wed, 07 Feb 2018 10:45:16 GMT	US	20.10.0.11		US	20.30.0.15		ICMP	60	mitigator2	ddos action:forward, entryzone
8	Wed, 07 Feb 2018 10:45:06 GMT	AU	1.1.1.1	60998	US	20.30.0.15	0	TCP	154	mitigator2	ddos action:drop, entryzone, reason...
9	Wed, 07 Feb 2018 10:45:14 GMT	US	20.10.0.11	61001	US	20.30.0.15	8080	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
10	Wed, 07 Feb 2018 10:45:11 GMT	US	23.109.26.113	60999	US	20.30.0.15	1111	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
11	Wed, 07 Feb 2018 10:45:04 GMT	US	20.10.0.11	60999	US	20.30.0.15	8080	TCP	60	mitigator2	ddos action:drop, entryzone, reason...
12	Wed, 07 Feb 2018 10:45:16 GMT	AU	1.1.1.1	61000	US	20.30.0.15	0	TCP	154	mitigator2	ddos action:drop, entryzone, reason...

```

*-----*
* Ethernet: 02:45:86:12:49:97 <-> 02:45:86:12:49:97 (UTC) 154 bytes *
*-----*
* MAC Source : 00:0c:29:07:81:26 --> Dest : 00:0c:29:8c:fa:95 Ether Type : 0x8000 (IPv4)
*-----*
* IP Ver: 4 Fwd: 1.1.1.1 To : 20.30.0.15 Total Len: 148 Hdr Len: 20 bytes
*-----*
* Type of Service : 0x00 Identification : 24537 Flags : 0x00
* Fragment Offset : 0 Protocol : 0x06 TCP TTL : 63
*-----*
* TCP
*-----*
* Source Port : 60998 Destination Port : 0
* Sequence number : 274354200 Acknowledgment : 0
* Control bits : 0x0000 FIN (No more data from sender)
* .0..... SYN (Synchronize sequence number)
* ..0... RST (Reset the connection)
* ...0.. PSH (Push function)
* ....0.. ACK (Acknowledge field sign.)
* .....0.. URG (Urgent pointer field sign.)
*-----*
* PAYLOAD
*-----*
0000 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0010 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0020 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0030 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X
0040 50 50 50 50 50 50 50 50 50 50 50 50 XXXXXXXX X

```

## Capture Template

---

Packet capture template provides controls such as the types of packets to capture, maximum packets per device, size of the capture, capture timeout, and so on.

To create a new packet capture template, perform the following:

1. Go to Monitoring & Reporting >> Packet Capture >> Template.
2. In the **Name** field, enter a unique name for the capture template.
3. In the **Description** field, enter a description of this capture template.
4. In the **Length Per Packet** field, configure the allowable length per packet that can be captured.
5. For **Packet Direction**, select whether you want to capture all packets, capture only forward packets, or capture only dropped packets.
6. In the **Berkely Packet Filter** field, specify the Berkeley Packet Filter to filter the packet capture.
7. In the **File Size** field, configure the maximum size the packet capture file can grow before the capture is stopped.
8. In the **Max Packet Per Device** field, configure the maximum allowable number of packets that can come from a device for the packet capture.
9. In the **Capture Timeout** field, configure the time duration in seconds when the packet capture must timeout.

SecDevice ships with a default “A10\_Default” capture template that cannot be deleted.

## Capture Policy

---

Packet capture policy is assigned to a zone. It binds the packet capture template with the policy controls for enabling packet capture at incident start or during the ongoing incident, and for sending packet capture complete notification to the configured email recipients.

To create a new packet capture policy, perform the following:

1. Go to Monitoring & Reporting >> Packet Capture >> Policy.
2. In the **Name** field, enter a unique name for this capture policy.
3. In the **Description** field, enter a description of this capture policy.
4. For **Enable Policy**, select the option if you want the policy to be enabled.
5. For **At Incident Start**, select the option if you want this policy to be activated at the start of zone incident.
6. From the **Capture Template** drop-down list, select a capture template to be associated with this policy.
7. Select **During Ongoing Incident** to enable periodic packet capturing policy during the ongoing incident.
  - a. In the **Every** field, enter the packet capture interval in minutes. By default, the time is set to 10 minutes. You can enter from 10 to 1440 minutes.
  - b. In the **Max Overall Capture Size** field, enter the maximum capture size in MB.
  - c. From the **Capture Template** drop-down list, select a capture template to which you want to associate this policy.
8. In the **Email Recipients** template, select a comma-separated list of email addresses to be notified when automatically created packet captures take place.

SecDevice ships with a default “A10\_Default” capture policy that cannot be deleted.

## Logging

The following features are available under Logging:

- [Device Logs](#)
- [SecDevice Logs](#)

## Device Logs

---

The Device Logs page displays syslog messages for the managed devices and possibly from other devices.

**NOTE:** SecDevice's syslog receiver does not filter out traps from non-managed devices, and the GUI does not filter out traps from non-managed devices, so it's possible this list could contain syslog messages from sources other than the managed devices.

---

To access the Device Logs page, navigate as follows:

1. Select **Monitoring & Reporting >> Logging**, and click **Device Logs**.
2. Specify the scope of the search by selecting any of the following:
  - Device—searches the syslogs generated from all devices or from a specific device. Click the Device drop-down and select a device.
  - Severity—searches the syslogs based on the type of severity selected from the Severity drop-down list.
  - Start Time—searches the syslogs based on the start time when the syslog was generated.
  - End Time—searches the syslogs based on the end time when the syslog generation was completed.
3. (Optional) Click the **Reset** button to reset the search criteria.
4. (Optional) Click the **Refresh** button to update the list.
5. (Optional) Select a check box for a log and click the **Delete** button to delete a log message.

## SecDevice Logs

---

The SecDevice Logs page displays actions that SecDevice has taken or noticed as it handles device management providing information on what component was involved, the severity of the action, and user. For example, this page displays information on logins, logging out of users and modifications to configurations, and actions such as deleting a backup device configuration.

Note that this page displays logs associated with events on the SecDevice, and this page does not display logs associated with the managed devices (to learn about logs associated with the managed devices, see [Alerts](#)).

To access the SecDevice Logs page, navigate as follows:

1. Select **Monitoring & Reporting >> Logging** and click on **SecDevice Logs**.
2. Click the **Component** drop-down menu to filter the information.
3. Click the **Severity** drop-down menu to filter which logs are displayed based on the severity of the associated event. Severity levels are standard for SYSLOG and include the following:
  - ALL
  - DEBUG
  - INFO
  - NOTICE
  - WARNING
  - ERROR
  - CRITICAL
  - ALERT
  - EMERGENCY
4. You can further filter the logs displayed by entering a date and time in the **Start Time** and **End Time** fields.
5. Click the **Search** button to run the search and filter down the list, or click **Reset Filters** to start again.

## Events

The Events page enables you to view activities that have transpired on SecDevice as it operates. Each tracked activity includes the time, type, severity level of the specific action, and managed device involved. Most tracked events will be device management activities in addition to external device SNMP traps.

To access to the SecDevice Events page, select **Monitoring & Reporting >> Events** and click Unacknowledged Events or Acknowledged Events.

## Details:

You can use filters to reduce this list of events such that only events containing a particular word or phrase are displayed. To do so, simply enter a string in the Search field at upper left and then click the drop-down menu and specify which field should be searched. Choices include the following:

- Type
- Device IP
- Description

Action buttons appear across the right-most side of this Unacknowledged Events:

- Refresh – Refreshes the current events page by retrieving a list of events from the database.
- Acknowledge/Unacknowledge – You can acknowledge an event so that it is moved to the “Acknowledged Events” to indicate that the event has been looked at, or “acknowledged.” An acknowledged event can similarly be “unacknowledged” to move it back to the “Unacknowledged Events” if you wish to flag it for later review. Click on the v icon next to Acknowledge, and click on Acknowledge All Events to acknowledge all events.

Table 79 : Column Headings in the Events page

Column heading	Description
Created Time	Indicates the date and time when the event was created.
Type	Indicates the type of the event. This is an internal definition.
Severity	Indicates the severity of the event. This can include: <ul style="list-style-type: none"><li>• Critical – An event that threatens to take down numerous network devices. Requires immediate action.</li><li>• Major – An event that has taken down at least one network device. Requires action.</li><li>• Minor – An event associated with partial failure of a device. The device requires attention.</li><li>• Warning – An event that may require action. Non-urgent.</li></ul>

Table 79 : Column Headings in the Events page

Column heading	Description
	<ul style="list-style-type: none"><li>• Normal – An event that has occurred but does not warrant action. Used for information purposes only.</li><li>• Cleared – An event which occurred but for which the underlying cause has been addressed.</li><li>• Unknown – An event for which the severity level cannot be determined by SecDevice.</li></ul>
Source IP	Indicates the IP address of the internal or external machine that triggered the event.
Description	This is a free-form text field.
Event data	Hover over the View link to display a pop-up window containing additional details about an event. <<Typically blue text with underline means clickable. However only hovering functions. Is this functionality correct?>>

# Dashboard

---

The following topics are covered:

<a href="#"><u>Dashboard Overview</u></a> .....	214
<a href="#"><u>Alerts</u></a> .....	217
<a href="#"><u>System</u></a> .....	218
<a href="#"><u>Dashboard Customization</u></a> .....	219

## Dashboard Overview

The Dashboard Overview page offers real-time monitoring for situational analysis and actions. It is intended to be a centralized location to view zone services under SecDevice management, providing an “at a glance” summary of top zone services, allowing the operator to quickly take action against potential attacks based on the reported data provided by the various widgets on this page. The key widgets that the Dashboard Overview provides are:

- [Threat Protection Services Objects](#)

Assess the number of configured zone and destination entry objects and number of zones and destination entry incidents currently under mitigation.

- [Service Protection Status](#)

View a chart that displays the percentage of zone services that are currently under mitigation.

- [Total Mitigator Traffic](#)

View a graph showing the sum of the traffic handled by the TPS mitigator(s) managed by SecDevice.

- [Top Sources](#)

View a global map that pinpoints the country of origin for source IP addresses and source IP addresses that have been dropped by using the Packet Rate and Packet Drop Rate button respectively for zones and destination entries.

- [Current Device Health](#)

View a graph showing the overall percentage of devices in “good” health.

- [High Traffic Destinations](#)

View the zones and destination entries with the highest amount of traffic.

- [Top Attacked Destinations](#)

View the zones and destination entries with the heaviest amount of traffic being mitigated.

The above widgets on the Dashboard can be moved, added or removed from the page as per your requirement by using the  Lock or  Unlock icon at the top right corner of the page. For more information, see [Dashboard Customization](#)

## Threat Protection Services Objects

---

The number of protected zones, protected destinations, active zone incidents and active destination incidents is displayed, allowing the administrator to see at a glance, the number of configured protected objects and the number of incidents currently undergoing mitigation. Each of these objects can be selected, where the operator will be taken to the appropriate protected object (zone or destination entry) or incident (zone incident or destination entry incident) page.

## Service Protection Status

---

Provides a chart of the number of services that are currently under protection, the number of services undergoing mitigation, and number of services that are in a state that require operator action. A hyperlink at the top right corner allows the operator to go directly to the zone incidents page.

## Total Mitigator Traffic

---

Displays a graph showing the amount of traffic that has gone through mitigator(s). The display can show the traffic that has occurred by the hour, by the day, or for a week by clicking on the appropriate time span button (1 Hour, 1 Day, 1 Week). The packets per second (pps) tab shows the number of packets that have passed successfully or have been dropped by mitigator(s), using color indicators (green for passed packets, red for dropped packets). The bits per second (bps) shows the same traffic, but by bits, using the color indicators of cyan for passed, and magenta for dropped.

**NOTE:** This graph differs from all other zone based graphs displayed, such as those that appear on the Zone Mitigation Console, Zone Charts page, where graphs on those pages show incoming traffic.

---

Other exceptions include Dst Entry graphs for TCP, UDP, ICMP and Other Indicator traffic. All other Dst Entry traffic show incoming traffic.

## Top Sources

---

Offers a global map to identify where the top sources of attacks have occurred. When the cursor is on this section, the scroll wheel can be used to zoom in or zoom out of the global map. Click the Details icon to view the source IP attack addresses originating from the highlighted country, city, and Autonomous System Number (ASN) depending on the selection of Packet Rate or Packet Drop Rate button respectively. Top Sources is based off the combination of protected zone services and protected destination services.

## Current Device Health

---

Shows the general health status of the TPS devices managed by SecDevice. A hyperlink to the Device Inventory page is offered at the top right hand corner of this section.

## High Traffic Destinations

---

Shows the top ten destinations (either zones or destination entries) that have the highest amount of traffic. The “Details” icon will open the Destination Received Statistics page that displays statistics on the number of received bytes and packets for all zones and destination entries. Clicking on a Zone or a destination entry name will lead to the Zone Charts page.

The “Go to” icon opens the Zone Configuration page. Click the Received Bytes or Received Packets to view the respective information, available by hovering over a zone.

## Top Attacked Destinations

Shows the top ten destinations (either zones or destination entries) that have come under attack. The “Details” icon will open Destination Dropped Statistics page that displays the statistics on the bytes dropped and packets dropped for all zones and destination entries. Clicking on a Zone or a destination entry name will lead to the Zone Charts page.

The “Go to” icon goes to the Zone Incident page. Click the Dropped Bytes or Dropped Packets to view the respective information, available by hovering over an attacked zones.

## Alerts

The Alerts page displays issues of high severity where administrators can configure what alerts are shown based on the type and severity through the Configure Alerts feature.

To access the Alerts page, select **Dashboard >> Alerts**

Figure 31 : Dashboard >> Alerts

Dashboard >> Alerts						
Search		Source IP	Description			
<input type="checkbox"/>	Created Time	Source	Component	Type	Severity	Description
<input type="checkbox"/>	2015-12-03 15:36:24	localhost	Health Monitor	Internal	CRITICAL	Device unreachable: 10.6.100.95 (tps-95)
<input type="checkbox"/>	2015-12-03 15:35:48	localhost	Health Monitor	Internal	CRITICAL	Device unreachable: 10.6.100.95 (tps-95)
<input type="checkbox"/>	2015-12-03 15:35:12	localhost	Health Monitor	Internal	CRITICAL	Device unreachable: 10.6.100.95 (tps-95)
<input type="checkbox"/>	2015-12-03 15:34:36	localhost	Health Monitor	Internal	CRITICAL	Device unreachable: 10.6.100.95 (tps-95)

Total 4 items

Items per page: 20

You can reduce the list of alerts displayed by entering a string in the **Search** field at upper left.

## Configure Alerts

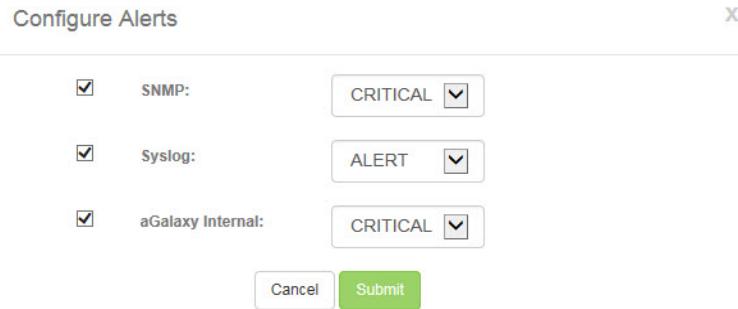
You can configure the notification severity of SNMP, Syslog, and SecDevice internal alerts.

To configure the Alerts:

1. Select **Dashboard >> Alert** and click **Configure Alerts**.

A window similar to that shown below appears.

Figure 32 : Dashboard >> Configure Alerts



2. Click on the SNMP check box for to enable or disable SNMP alerts. Choose the severity of the alert from the drop-down menu.
3. Click on the Syslog check box for to enable or disable Syslog alerts. Choose the severity of the alert from the drop-down menu.
4. Click on the SecDevice Internal check box for to enable or disable SecDevice Internal alerts. Choose the severity of the alert from the drop-down menu. Severity from highest to lowest is as follows: EMERGENCY, ALERT, CRITICAL and ERROR. So if you select "ERROR", then alerts would be displayed for ERROR, CRITICAL, ALERT and EMERGENCY.
5. Click Submit.

---

**NOTE:** Alert severities greater than the one chosen from the drop-down menu will be shown as well.

---

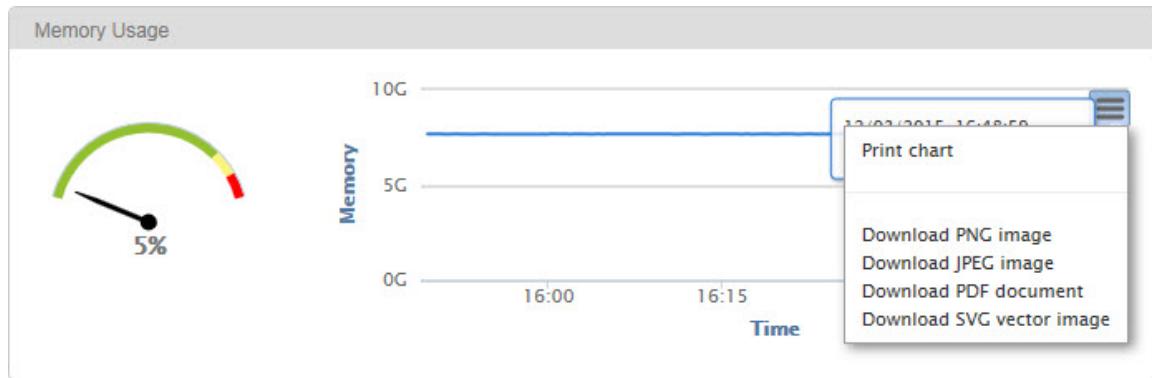
## System

The System page provides a summary of information on the SecDevice. It is updated every 10 seconds and displays System Info, System Services, Memory Usage, CPU Usage and Disk Usage.

To access the SecDevice System page, select **Dashboard>>System**.

You can print charts (as well as download the image in a variety of formats) by clicking the menu icon at the upper-right of the chart for Memory Usage, Disk Usage, and CPU Usage.

Figure 33 : Print Chart/Download Images



The above widgets on the System tab can be moved, added or removed from the page as per your requirement by using the Lock or Unlock icon at the top right corner of the page. For more information, see [Dashboard Customization](#)

## Dashboard Customization

The widgets on the Dashboard >> Overview and Dashboard >> System can be moved,

added or removed from the page as per your requirement by using the Lock or Unlock dashboard icon at the top right corner of the page.

1. To customize the dashboard, perform the following:

2. Click icon to unlock the dashboard.
3. Click to remove a widget from the page.

After unlocking the dashboard, 'Add Widget' is displayed next to the icon.

4. Click on 'Add Widget' to add a missing pre-defined widget on the page. If all the pre-defined widgets are already added on the dashboard, SecDevice displays a message to that effect.

If one or more of the pre-defined widgets are not displayed, you can select the widgets from the ‘Add Widget’ dialog box to add it to the page.

The layout of the widgets can be changed by dragging the widget to the appropriate position.

5. After updating the page as per your requirement, lock the dashboard by click on the  icon.

A confirmation message is displayed where you can select one of the following:

- Factory Reset – Select this option to place the widgets at their default locations.
- Continue Editing – Select this option if you would like to make any more updates to the page.
- Discard Changes – Select this option to discard any updates made to the page.
- Save Changes – Select this option to save the updates made to the page.

# Protected Object - Destination Entries

---

SecDevice TPS offers the ability to protect network assets against DDoS attack through protected objects and incidents.

To access the Dst Entries page, navigate as follows:

1. Hover over **Configurations >> Protected Objects** from the main menu, and click Destination Entries.
2. (Optional) The following buttons appear across the upper-right side of the Destination Entries table:
  - Refresh – Refreshes the information displayed for the Dst Entries page.
  - Delete – Select the check box at left for one or more Dst Entries, then click Delete.
  - + New Dst Entry - Create a destination entry. See Creating a Dst Entry below.

**Report** - Create a report.

Table 80 : Description of the Column Headings in the Destination Entries table

Column heading	Description
Name	Name of the destination entry/protected object.
Destination IP/Subnet	Displays the IPv4 or IPv6 address (and subnet) destination of the protected objects. This only appears when Dst Entries is selected for Protected Objects.
Incidents	The number of ongoing and total incidents is provided. If an incident is ongoing, a hyperlink to the Mitigation Console page is available.
Devices	Displays the list of Devices. Hover over field for more details.
Device Group	The device group that is associated with this protected object.
View	Hyperlink to associated charts and statistics for the protected object is available.

Table 80 : Description of the Column Headings in the Destination Entries table

Column heading	Description
Actions	<p>Allows you to edit a protected object or generate a report.</p> <p>Edit - Make changes to a protected object configuration.</p> <p>Duplicate - Create an object that contains identical basic parameters of an existing object.</p> <p>Report - Create a report. See <a href="#">Create a Report Schedule</a> for more information.</p>

## Using Search

The list of protected objects may be extensive. To filter the information that is displayed:

1. Enter a string in the **Search** field.
2. Click the drop-down menu (default: Name) and select the type of search being done for the protected objects.
3. Click the drop-down menu and select **All Devices** or a specific managed device to search this field.
4. This will reduce the list of protected objects displayed and can make it easier to find information for a device.

## Creating a Dst Entry

To create a new destination entry:

1. In the **Name** field, enter the name of the new protected object destination entry.
2. In the **Destination IP/Subnet** field, enter the IP and subnet for the destination entry.
3. Choose the radio button for where you would like to create the new protected object.
  - Select the Device List radio button to list the available devices.
  - Select the Device Group radio button to get a drop-down menu of available device groups.
4. Select the device or device group that corresponds with where you would like to create the new protected object.
  - **Device List** - Choose from the listed devices where you would like to create the new protected object.
  - **Device Group** - Choose from the list of grouped devices where you would like to create the new protected object.

5. (Optional) Select a mitigation template from the Peacetime Template from the drop-down list. A peacetime mitigation template is a template that can be pushed to a DST entry without creating an incident. When a peacetime template is used, the logging options and countermeasures will be applied, but the Auto Bypass and BGP options are ignored.
6. (Optional) Choose the operational mode of the Peacetime Template to set on the DST entry for its deployment from the Peacetime Operational Mode drop-down list.
  - Protection (default) - Applies DDoS Mitigation security checks and rate limits to the traffic.
  - Bypass - Adds the destination to the White List when mitigation is stopped.
7. Click **Submit** to save your changes.

# Protected Object - Source Entries

---

To access the Src Entries page, navigate as follows:

1. Hover over **Configurations >> Protected Objects** from the main menu, and click Source Entries.
2. (Optional) The following buttons appear across the upper-right side of the Source Entries table:
  - Refresh – Refreshes the information displayed for the Source Entries page.
  - Delete – Select the check box at left for one or more Source Entries, then click Delete.
  - + New Src Entry - Create a source entry. See Creating a Source Entry below.

Table 81 : Description of the Column Headings in the Source Entry table

Column heading	Description
Name	The name of the destination entry.
Source IP/Subnet	The source IP address and subnet information.
Devices	Displays the device associated with the destination entry. Hovering over the device will display its ip address.
Device Group	Displays the Device Group associated with the Dst Entry.
Actions	Click on the link in the Actions column:  Click the Edit link to modify one of the previously-configured source entries.  Click the Duplicate link to create an object that contains identical basic parameters of an existing object.

## Using Search

The list of protected objects may be extensive. To filter the information that is displayed:

1. Enter a string in the **Search** field.
2. Click the drop-down menu (default: Name) and select the type of search being done for the protected objects.
3. Click the drop-down menu and select **All Devices** or a specific managed device to search this field.
4. This will reduce the list of protected objects displayed and can make it easier to find information for a device.

## Creating a Source Entry

To create a new source entry or update one for a protected object:

1. Hover over **Configurations >> Protected Objects**.
2. Click Src Entries.
3. Click the **New Src Entry** button at upper right. In the **Name** field, enter the name of the source entry for the protected object.
4. In the **IP Address** field, enter the IP and subnet for the source.
5. Choose the radio button for where you would like to create or update the source entry.
6. Select the Device List radio button to list the available devices.
7. Select the Device Group radio button to get a drop-down menu of available device groups.
8. Select the device or device group that corresponds with the protected object to add or update a source entry.
  - **Device List** - Choose from the listed devices where you would like to create the new protected object.

- **Device Group** - Choose from the list of grouped devices where you would like to create the new protected object.
9. Select the **Options** desired by clicking on the available checkboxes. Click Enable Bypass to allow Bypassed connections. Click the Enable Logging checkbox for log generation. Clicking on the Enable Logging checkbox provides an option for periodic logs by clicking on the Log Periodic checkbox.
10. In the L4 Type tab, the configurable options are:
- GLID for TCP
  - GLID for UDP
  - GLID for ICMP
  - GLID for Others
  - Protocol Template for TCP
  - Protocol Template for UDP
  - In the Application tab, the configurable options are
    - Protocol Template for HTTP
    - Protocol Template for DNS
    - Protocol Template for SSL-L4
11. Click **OK** to save your changes.

# Device Management Operations

---

The chapter describes the device management operations that can be performed from Devices:

The following topics are covered:

<a href="#"><u>Device List</u></a> .....	.229
<a href="#"><u>Device Groups</u></a> .....	.233
<a href="#"><u>Default Credentials</u></a> .....	.235
<a href="#"><u>Deleted Devices</u></a> .....	.238
<a href="#"><u>Device Upgrade</u></a> .....	.239
<a href="#"><u>Device Configs</u></a> .....	.242
<a href="#"><u>Config Backups</u></a> .....	.245
<a href="#"><u>Device Settings</u></a> .....	.252
<a href="#"><u>SSL Management</u></a> .....	.256
<a href="#"><u>CLI / File Objects</u></a> .....	.260
<a href="#"><u>CLI / File Objects</u></a> .....	.263
<a href="#"><u>Other System Settings</u></a> .....	.271
<a href="#"><u>Debugging and Support</u></a> .....	.273

## Device List

In the devices list, you can see a TPS detector and a mitigator. TPS devices can be used as a mitigator or a standalone detector. These devices are fully owned by SecDevice.

The **Devices >> Device List** page displays a list of ACOS devices that are currently being managed by SecDevice.

You can either select the device from the search bar or choose them on the basis of Name, IP address or Model from the drop-down list.

Table 82 : Description of the Column Headings in the Device List table

Column heading	Description
Status	Indicates the status of the device: <ul style="list-style-type: none"><li>• (Green, arrow up)—Indicates that both ping and http/https are running.</li><li>• (Orange, arrow up)—Indicates that the ping is running.</li><li>• (Red, arrow down)—Indicates that neither ping nor http/https are running.</li></ul>
Name	Displays the hostname of the device.
IP Address	Displays the IPv4 or IPv6 address of the managed device.
Model	Displays the model of the device. SecDevice supports the ability to manage the following types of Organization devices: <ul style="list-style-type: none"><li>• AX Series</li><li>• Thunder Series</li><li>• vThunder (formerly known as SoftAX)</li></ul>
Type	Displays the role of the device.  A TPS device can be used as a mitigator or a TPS detector.  If there is a TPS device that is yet to be configured as a detector, a warning icon is displayed.

Table 82 : Description of the Column Headings in the Device List table

Column heading	Description
	To configure the device, go to <b>Devices &gt;&gt; Device List</b> page. Under <b>Actions</b> , click the arrow next to Details and choose <b>Configure Detection</b> .
SW Info	Displays the software version and build number of the device. To view the latest version of the TPS device after upgrade, under <b>Actions</b> and choose <b>Scan from Device</b> .

Perform any of the following options under **Actions** column, that are explained here:

Table 83 : Description of the options under Actions column

Options	Description
Scan from Device	If the same object does not exist already in SecDevice, scan action will fetch protected zones, destination entries, templates, and class-lists from the TPS mitigators. In the case of TPS, ADC, or CGN detectors that can automatically discover IP addresses and services and fetch the discovered entities.
Sync to Device	Sends the initial configurations such as the following to the selected device when the device is out-of-sync with SecDevice's configuration: <ul style="list-style-type: none"> <li>• Device global settings and management configuration such as sFlow, SNMP, Syslog information, and DDoS notification template</li> <li>• Zones and dependent objects such as templates, GLIDs, and class-lists etc</li> <li>• BGP Routes, flowspecs and route-maps associated with Zones</li> <li>• Dst entries and dependent objects</li> <li>• Geo Location Databases</li> </ul>

Table 83 : Description of the options under Actions column

Options	Description
	<p><b>CAUTION:</b> It may take a longer time to synchronize Geo Location databases. It is recommended to increase the HTTPS Read Timeout on <b>Device &gt;&gt; Device Settings &gt;&gt; Connection</b> to greater than 120 seconds.</p> <p>If there is a class list on the device with Geo Location, you must remove the entries. Else, an error is displayed while synchronizing the device</p>
	Click <b>Submit</b> .
Device Backup	<p>Allows you to take the backup of the device. Select the following options to complete the backup:</p> <ul style="list-style-type: none"> <li>• <b>Schedule Type</b>—Select either <b>Immediate</b> or <b>Schedule</b>, if you select schedule you will further see fields for <b>Start Datetime</b> and <b>Schedule Options</b>.</li> <li>• <b>Save Config before Backup</b>—Select either <b>Yes</b> or <b>No</b>.</li> <li>• <b>Description</b>—Add the appropriate description</li> <li>• <b>Remote</b>—Enable the check box if you want the remote backup.</li> </ul> <p>Click <b>Submit</b>.</p>
Configure Detection	Allows you to configure a device as a detector. To configure a device as a detector, see <a href="#">Setting Up a Detector</a> .
Remove Detection	Allows you to remove the detector configuration.
Login	Allows you to log in to the device.
	A Save Configuration pop-up is displayed. Choose <b>Partition</b> and click <b>Submit</b> .
Reboot	Allows you to save the configuration and reboots the device.
Update Credential	Allows you to update the device credentials.
Configure Mitigation	<p>Allows you to configure a device as a mitigator. To configure a device as a mitigator, perform the following:</p> <p><b>Global ZAPR Settings</b></p>

Table 83 : Description of the options under Actions column

Options	Description
	<p>Dedicated Control CPUs for pattern recognition can be assigned only if the device has more than 3 data CPUs.</p> <ul style="list-style-type: none"> <li>• <b>Pattern Recognition</b>—Choose <b>Enable</b> to configure the global ZAPR setting.</li> <li>• <b>CPU(s) Dedicated</b>—Choose the number of data CPUs for pattern recognition.</li> <li>• <b>Reboot</b>—Choose yes or no from the drop-down menu.</li> </ul> <hr/> <p><b>NOTE:</b> The device reboots for the dedicated CPU control to come into effect.</p> <hr/> <p>Click <b>Submit</b> to save the ZAPR settings configuration.</p> <h4>BGP Flowspec Settings</h4> <p>If using the BGP Flowspec to redirect the traffic to TPS, enter the DDoS outside interface of the mitigator device.</p> <ul style="list-style-type: none"> <li>• <b>DDoS Outside Interface IPv4</b>—Enter the IPv4 address.</li> <li>• <b>DDoS Outside Interface IPv6</b>—Enter the IPv6 address.</li> </ul> <p>Click <b>Submit</b> to save the BGP Flowspec settings configuration.</p> <h4>BGP Route</h4> <p>When a TPS device is added to SecDevice and if ‘BGP AS number’ is already configured, it is scanned from the mitigator device and then persisted in SecDevice database. If ‘BGP AS number’ is not configured on the TPS mitigator device, user can manually enter ‘BGP AS number’ here.</p> <ul style="list-style-type: none"> <li>• <b>AS Number</b>—Enter AS Number, which is associated with the device. This helps to push the route to the specified device.</li> </ul> <p>Click <b>Submit</b> to save the BGP Route setting.</p>

On the top right of the Device List window, click to perform any of the following:

Table 84 : Action buttons on Device List page

Actions	Purpose
<b>Save Config</b>	<b>Select one or more devices and click Save Config to save the current configuration for the device.</b>
Refresh	Select the option to refresh the current device list by retrieving the list of devices from database and querying each device for the latest operational statistics on memory usage, CPU usage, and up-time.
Report	Enter the details to create an inventory report of the devices on SecDevice. For more information about creating a report, follow the instructions from step 2 to 7 in the <a href="#">Create a Report Schedule</a> section.
Delete	<p>Select one or more devices and click <b>Delete</b>. The selected devices are deleted.</p> <hr/> <p><b>NOTE:</b> The default delete function performs a soft delete, meaning that the deletion can be recovered by going to the Deleted Device List tab and clicking on Restore with that configuration selected. If the Do you also want to delete the backup configs of this device? check box is selected, a hard delete will be executed, meaning that the device cannot be restored from the Deleted Device List.</p>
Add Devices	Displays the Add Device window. For more information about adding devices, follow the instructions specified in the <a href="#">Add Devices</a> section.

- **Device CLI:** Select or enter the show commands that you want to execute on TPS devices directly from SecDevice GUI.

## Device Groups

A Device Group can be used to create a Mitigator Group or a Detector Group.

The Device Groups page displays a list of devices. You can select a set of devices to create a new mitigator group or a detector group. You can also add devices to an existing device group or delete a device group.

A mitigator group helps to streamline the configuration process. For example, you could push a config file to all devices in the group at once.

A detector group helps to ensure a reliable operation and provides redundancy of the detectors for a zone. In case of a failure of one of the detectors, the Detector Group ensures SecDevice continues to receive DDoS detection events from the other detectors in the group and thus achieve uninterrupted DDoS Protection.

When a detector group is associated to a zone, all the detectors within the group will receive xFlow (sFlow or NetFlow) traffic from the edge router for traffic monitoring. If any of the detectors within the group detects an attack or an increase in the configured threshold, it sends an escalation notification to SecDevice, and then SecDevice will create an incident and start the mitigation.

---

**NOTE:** At least, one device group must be created and used as a mitigator group or a detector group.

---

To access the device groups page, navigate to **Devices >> Device Groups**

Table 85 : Description of the Column Headings in the Device Groups table

Column heading	Description
Group Name	Displays the Group Name of the Device Group.
Devices	Lists the devices in the Device Group. Hover over the specific field to see list of devices and their IP address that is associated with the group.
Type	Displays the type of the device group. It can be either a Detector Group or a Mitigator Group.
Description	Displays the text from the Device Group Description.
Actions	Click Edit to modify the device selection and other details in a group.

From this page, you can select one of the following buttons at the top right of this window:

- Click Refresh to update the list of device groups.
- Click Delete to delete one or more selected device groups from the list.
- Click Create to create a new device group. Enter a Group Name, select one or more devices, enter the description, and click Submit.

## Default Credentials

Editing a membership of a device group will also modify DDoS Dst entry configurations of devices accordingly, resulting in the addition or deletion of these configurations for the devices.

When discovering devices, you can specify the default device credentials SecDevice can use. These default credentials should be used to access devices if no other credentials have been provided for the managed devices.

You can create and update the credentials for the devices. This topic covers the following:

- [Creating the Default Credentials](#)
- [Updating the Default Credentials](#)

## Creating the Default Credentials

---

You can add or delete the default credentials SecDevice will use when attempting to discover a device via HTTPS or CLI.

To create the default credentials, perform the following:

1. Select **Devices >> Default Credentials**.

Figure 34 : Devices >> Default Credentials

The screenshot shows a table titled "Devices >> Credentials". The table has columns: Type, Timeout, Retries, Port, User Name, and Actions. There are two rows: one for "HTTPS" (Timeout 10, Retries 3, Port 443, User Name "admin") and one for "CLI" (Timeout 10, Retries 3, Port 22, User Name "admin"). At the bottom of the table, it says "Total 2 items" and "Items per page: 20".

Type	Timeout	Retries	Port	User Name	Actions
HTTPS	10	3	443	admin	Edit
CLI	10	3	22	admin	Edit

2. From the Default Credentials tab, select one of the following buttons along the upper right-most corner of the page:
  - Click **Refresh** to update the list of default device credentials.
  - Click **Delete** to delete one or more selected default device credentials from the list.
  - Click **Create** to open a Default Credentials window. In Credentials For, HTTPS, CLI and SNMP are available.
    - Select HTTPS in Default Credential Window to enter a new set of default device credentials to be used to access the device via HTTPS.
    - Click Submit when done

From this modal window, configure the options shown in .

Table 86 : Default Device Credentials (HTTPS)

Button	Description
Username	Enter the default administrative username needed to access the managed device.
Password	Enter the default password for the administrative user needed to access the managed device.
Confirm Password	Confirm the default password for the administrative user needed to access the managed device.
Timeout	Enter the timeout period. This is the number of minutes the CLI session can be idle before it times out and is terminated.
Retries	Enter the number of attempts SecDevice can repeatedly attempt to establish a connection if the first try fails.

Or

- Select CLI in the Default Credential Window to enter a new set of default device credentials to be used to access the device via CLI.
- Click Submit when done.

From this modal window, configure the options shown in .

Table 87 : Default Device Credentials (CLI)

<b>Button</b>	<b>Description</b>
Username	Enter the default administrative username needed to access the managed device.
Password	Enter the default password for the administrative user needed to access the managed device.
Confirm Password	Confirm the default password for the administrative user needed to access the managed device.
Enable User Name	Enter the default administrative username needed to access Privileged EXEC level for the managed device. This level is also called the “enable” level because the enable command is used to gain access. Privileged EXEC level can be password secured.
Enable Password	Enter the default password associated with the administrative username needed to access Privileged EXEC level for the managed device.
Confirm Enable Password	Confirm the default password associated with the administrative username needed to access Privileged EXEC level for the managed device.
Timeout	Enter the timeout period. This is the number of minutes the CLI session can be idle before it times out and is terminated.
Retries	Enter the number of attempts SecDevice can repeatedly attempt to establish a connection if the first try fails.

Credential Devices configurations can be edited by clicking Edit in the Action column for the default device credentials.

## Updating the Default Credentials

You can update the username and password of the device credentials. There are two ways you can update the device credentials. You can either update the username and password and directly submit the changes without verifying if SecDevice can log in to the device or you can update the credentials and verify if SecDevice can log in and scan the device.

To update the device credentials, perform the following:

1. Navigate to **Devices >> Device list**.
2. For the device that you wish to update the credentials, under **Actions**, click **Details** and select **Update Credential**.
3. In the Update Device Credential window, enter the user name and password in the respective fields.
4. Perform one of the following:
  - Click **Update**. The username and password are updated without verifying if SecDevice can login to the device.
  - Click the arrow next to Update and select **Update & Scan from device**. The username and password are updated only after verifying the login credentials and scanning the device. If SecDevice is unable to login, then the credentials are not changed and an error is displayed.

## Deleted Devices

The Deleted Devices page displays the managed devices have been soft deleted from this SecDevice. From this page, you can view the managed devices that have been removed from this SecDevice, or you can restore a device that was deleted.

To access the SecDevice's Deleted Devices page, navigate as follows:

1. Select **Devices >> Deleted Devices**.
2. (Optional) To remove a previously-deleted device from the list of deleted devices, select the check box to the left of the deleted device and then click the **Delete** button.
3. (Optional) To restore a previously-deleted device, click the Restore button under the Actions column. The device is removed from the Deleted Device List, and a confirmation message appears, indicating that the device has been restored.

You can confirm that the device was indeed restored by clicking the **Device List** tab. You should see the restored device under the Device List table.

For more information about the Device List page, please see [Device List](#).

4. (Optional) To move the device back to the Deleted Device List, select the check box next to the device and click the **Delete** button.

5. From here, you can perform a hard delete or a soft delete. A “hard delete” means the check box is selected, whereas a “soft delete” means the check box is clear. The results of the “hard delete” and “soft delete” are shown below:

- Selecting “hard delete”:
  - deletes the device, as well as removes the device from the device-group (if applicable).
  - deletes the device's backup configuration from the “Config Backups” list
  - deletes the device's configurations from the “Device Configs” (including CLI, aFleX, WAF, SSL, BW-list, etc.)
- Selecting “soft delete”:
  - deletes the device, as well as removes the device from the device-group (if applicable).
  - Moves the device's backup configuration from the “Config Backups” to the Deleted Device Config Backups list.
  - does NOT delete the device's configuration from the “Device Configs” (CLI, aFleX, WAF, SSL, BW-list, etc.)

---

**NOTE:**

Therefore, if you are deleting a managed device which you may later want to restore, it is recommended that you perform a “soft delete” in order to make sure the various configuration files will still be available, if/when you decide to restore.

---

## Device Upgrade

The Device Upgrade feature allows you to transfer software release images from a remote server onto the SecDevice device and then perform a device image upgrade by deploying a device upgrade job against a device.

### Uploading an Image

---

To use the device image upgrade feature:

1. Select **Devices >> Device Upgrade** from the main menu.

The table lists the upgrade images that have been copied to SecDevice. These files can be used to upgrade the SecDevice-managed devices. If the table is empty, you can upload a device image into SecDevice using the following options:

- **SCP Image** - To download the device image from a remote server using the SCP option, click SCP Image at the upper-right corner and enter the following in the Device Image Load window:
  - a. In the SCP File Name field, enter the name of the image you want to upload.
  - b. In the SCP File Path field, specify the exact image store path starting from the server root.
  - c. In the SCP Host Name field, enter the IP address of the server from which the image will be uploaded.
  - d. In the SCP User Name field, enter the username to access the server from which the image will be uploaded.
  - e. In the SCP Password field, enter the password to access the server. For protection purposes, this field is not displayed in plain text.

---

**NOTE:** The characters supported for user name and password are: A-Z a-z 0-9 ! " # \$ % ' ( ) \* + , - . / ; < = > ? ^ \_ ` { | } ~. The characters that are not supported are: @ , & and :

---

- f. In the Description field, enter a description for the image.
  - g. Click **Submit**.
- **Upload Image**: To upload the device image from a file location in your local system, click Upload Image at the upper-right corner. The Device Image Upload window appears. Enter the following:
    - a. Click Choose File to navigate to the file location in your local system and select an image file to upload.
    - b. Enter an appropriate description for the device image.
    - c. Click **Submit**.

SecDevice will attempt to add the image to the Device Upgrade page using the information you provided.

- If successful, a confirmation message appears at the top of the screen and the image is added to the table.
- If unsuccessful, an error message appears at the top of the screen, and the image is not added to the table.

Image files will appear in the “Device Upgrade” table.

Table 88 : Description of columns in the Device Upgrade list

<b>Button</b>	<b>Description</b>
File Name	Displays the name of the image file.
Created	Displays the date and time that the image file was created.
Description	Displays the description information entered when the image file was copied to SecDevice.
Size	Displays the size of the image file.
Actions	<p>Displays the available actions that can be performed with the image file:</p> <ul style="list-style-type: none"> <li>• Edit – click the edit button to edit the information associated with this image.</li> <li>• Upgrade – To upgrade one or more of the managed devices using this image, click the upgrade link. A pop-up window appears, containing device upgrade information. Select the target device that you wish to upgrade from the drop-down menu.</li> </ul>

## Upgrading a Device

Once you have loaded upgrade images onto your SecDevice device, you can push the upgrade images out to your managed devices.

1. Click on the Upgrade link in the Actions column of the desired upgrade image. The Device Upgrade window will appear.
2. Select the device or configured device group you wish to upgrade from the corresponding fields.
3. Select your schedule type. You can choose to upgrade your device immediately or at a later date. If you wish to schedule the upgrade at a later date, select the

Schedule option and the Start Datetime field will appear for you to select when the upgrade will take place from the drop-down calendar. You will also need to enter a specific time on your selected date for when the upgrade will take place

4. Select where the upgrade image will be stored using the Primary/Secondary radio buttons.
5. Select whether to save the configuration prior to the upgrade.
6. Indicate whether you wish to reboot your selected device/device group after the upgrade is successful.
7. If you wish to add a description of the upgrade you can do so in the corresponding field.
8. Click Submit.
9. Click Confirm if the task is configured correctly.

## Device Configs

The Device Configs page has an inventory of the most recent backup configuration files. From this page, you can edit portions of a backup configuration file, then save it locally to SecDevice, see [CLI / File Objects](#), and push it to a managed device.

Note: To see all available configuration backup files of a specific device, navigate to Devices >> Config Backups, and click Contents for that device.

To edit portions or snippets of a backup configuration file, navigate as follows:

1. Select **Devices >> Config Backups**.
2. Click the **Contents** hyperlink under the Actions column, at far-right.

**NOTE:** A new window similar to [Figure 36](#) appears, listing the contents of the backup file. By default, the CLI Configs tab is selected.

Figure 35 : Configurations &gt;&gt; “Device” &gt;&gt; CLI Configs

The screenshot shows a navigation bar with tabs: Device, All Devices, Partition, All Partitions, CLI Configs (which is highlighted), and Class-Lists. Below the navigation bar, the path is shown as Devices >> Device Configs >> CLI Configs. A search bar and a 'Save As' button are also present. The main area displays a table with columns: Name, Device, Partition, Size, and Actions. The table contains several entries, with one entry's name being highlighted and a red arrow pointing to it, accompanied by the text "Click the name of a configuration to view a non-editable version.". Another red arrow points to the "Save As" link in the Actions column of the same row, with the text "Click Save As to access an editable version of the config file.".

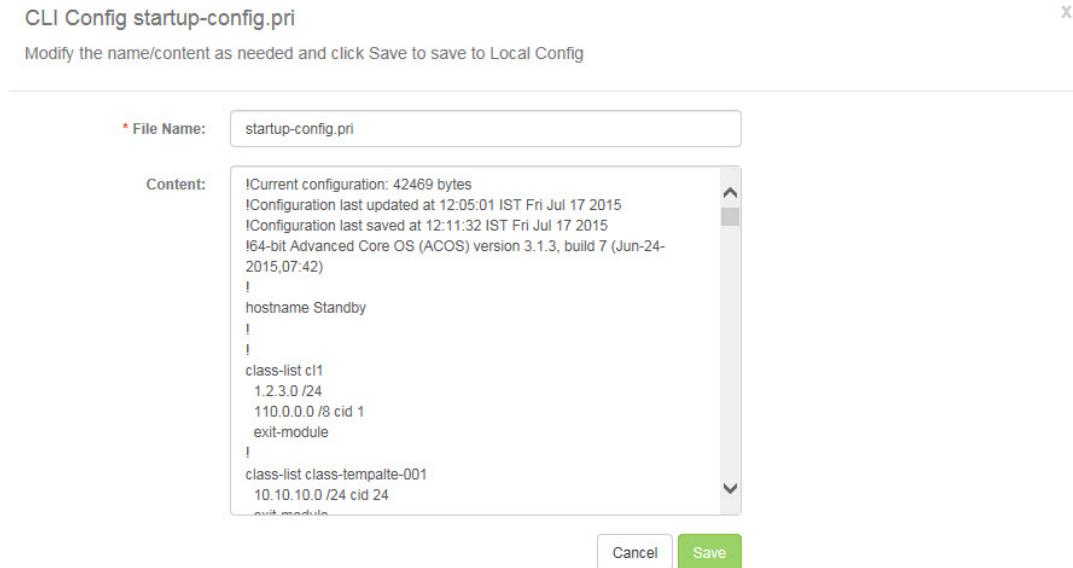
Name	Device	Partition	Size	Actions
startup-config.pri	TH5435S-322P1SP2 (10.6.15.96)	shared	151048	<a href="#">Save As</a>
startup-config.sec	TH5435S-322P1SP2 (10.6.15.96)	shared	1127	<a href="#">Save As</a>
startup-config.pri	TH6435-322P4 (10.6.15.95)	shared	128353	<a href="#">Save As</a>
startup-config.sec	TH6435-322P4 (10.6.15.95)	shared	1090	<a href="#">Save As</a>
ddos.init	TH5435S-322P1SP2 (10.6.15.96)	shared	4101	<a href="#">Save As</a>

Table 89 : Columns in Configuration Backups Contents table

Button	Description
Name	Displays the name of this portion of the config file.
Partition	Displays the partition (shared or private) of this portion of the config file.
Size	Displays the size (in bytes) of this portion of the config file.
Actions	<p>The Action column displays the available actions that can be performed with this portion of the config file.</p> <p>Save As – click the <b>Save As</b> link to modify this portion of the configuration backup file.</p>

3. Select one of the tabs under the menu bar to specify which portion of the config file you would like to work on, for example: CLI Configs or Class-Lists.
  - To view a non-editable version of the “chunk” of the config file, click the hyperlinked name of the config file from the Name column of the table.
  - To view an editable version of the “chunk” of the config file, click the **Save As** link from the Actions column of the table. A window similar to that shown below appears:

Figure 36 : Configurations &gt;&gt; “Device” &gt;&gt; CLI Config &gt;&gt; Save As




---

**NOTE:** When naming a file to be saved as a Local Config, do not enter special characters, (such as '?', '#', '\*', and so on) in the File Name, as this could cause issues when attempting to push the file to other devices.

---

4. (Optional) You can enter a modified name for the config portion in the **File Name** field.
5. Edit the configuration that appears in the Content area, similar to that shown above in [Configurations >> “Device” >> CLI Config >> Save As](#).
6. Click **Save** when done.

The modified section of the config file (such as the CLI sample shown above), is saved locally on the SecDevice device. For this reason, it can be found by navigating to the Configurations >> Local Configs page. (See [CLI / File Objects](#) for details on pushing a configuration snippet to another managed device.)

To delete a device configuration file, navigate as follows:

1. Select **Devices >> Device Configs**.
2. Select the CLI Configs or Class-Lists tab.

From here, select the checkbox next to the file you wish to delete from a device and click on Delete.

**NOTE:**

Note: In order to use the delete functionality, a configuration backup must first be done at least once following an upgrade to 3.0.4-P2 if upgrading from a version older than 3.0.4-P1 to allow SecDevice to create a working copy of the files on the devices. Files that are part of a backup cannot be individually deleted, but an entire backup configuration can be deleted. Upon upgrade to 3.0.4-P2, SecDevice automatically triggers a backup configuration task for all devices.

---

## Config Backups

This section covers the process of creating a backup configuration file for a managed device, viewing previously saved backup config files, modifying the contents of a backup config file, restoring an SecDevice-managed device using a previously saved backup config file, or deleting all configurations.

Note: The backup and restore process applies to start up configurations, not running configurations.

### Creating a Backup Configuration File for a Managed Device

You can create a backup configuration for TPS devices. The configuration file for the device can be saved on the SecDevice device or on a remote server, and from there, it can be modified locally on SecDevice or pushed to other devices.

To create a backup configuration file:

1. Navigate to **Devices >> Config Backups >> Configurations** or **Devices >> Device List >> Actions >> Device Backup** to access the configuration backups.
2. If you are on the Configurations page, click the **Backup Config** button at the top right corner.

The Device Configuration Backup page appears as shown below:

Figure 37 : Devices Configuration Backup

Device Configuration Backup

**Devices:**

- 10.6.100.20
- 10.6.15.95
- 192.168.122.2
- 10.6.3.133

**Device Groups:**

- detector122
- mitigator133
- mitigator\_group

Please select at least one device or device group

Schedule Type:  Immediate  Schedule

Save Config Before Backup:  Yes  No

Description:

Remote:

3. Enter the details to create a backup immediately or schedule a backup. Refer to .

Table 90 : Options in Device Configuration Backup Page

Field	Description
Devices	Select one or more devices from the Devices list. This option is displayed only when you are creating a backup from Config Backups >> Configurations.
Devices Groups	Select one or more device groups from the Device Groups list. This option is displayed only when you are creating a backup from Config Backups >> Configurations.
Schedule Type	<p>Select Immediate or schedule a backup at a recurring time.</p> <p>If Schedule is selected, enter the following details:</p> <p>Start Datetime: Click to view the calendar. From the calendar, choose a start date. To select a time, click the clock icon at the bottom of the calendar. The date and time must be entered in the following format: mm/dd/yyyy hh:mm AM/PM</p> <p>Schedule Option: Select the interval at which the backup configuration snapshots must be taken. The options include:</p>

Table 90 : Options in Device Configuration Backup Page

Field	Description
	<p>One Time – The backup config file will be created only once at the time entered in the 'Start Datetime' field.</p> <p>Every 6 Hours – The backup will be created automatically every 6-hour from the time entered in the 'Start Datetime' field.</p> <p>Every 12 Hours – The backup will be created automatically, on a 12-hour basis, starting at the time entered in the 'Start Datetime' field.</p> <p>Daily – The backup will be created automatically, on an hourly basis, starting at the time entered in the 'Start Datetime' field. The Interval time can range from 1-6 days.</p> <p>Weekly – The backup will be automatically created every week, starting at the day of week entered in the 'Start Datetime' field.</p> <p>Bi-weekly – The backup will be automatically created every other week, starting at the day of week entered in the 'Start Datetime' field.</p> <p>Monthly – Select a number ranging from 1–12 in the Interval field. The backup will be created automatically, on a monthly basis, starting from the date entered in the 'Start Datetime' field.</p>
Save Config Before Backup	Select Yes if you wish to save your configuration prior to the initial backup.
Description	Enter the description for the device configuration backup.
Remote	<p>De-select this check box if you wish to save the backup config file on the SecDevice device.</p> <p>Select this check box to specify a remote destination for the backup job.</p> <p><b>Note: If the Remote option is selected, configuration backups will not be shown in the SecDevice Device Configuration Backup</b></p>

Table 90 : Options in Device Configuration Backup Page

Field	Description
	<p><b>list.</b></p> <p>To specify a remote destination, enter the following:</p> <ul style="list-style-type: none"> <li>• <b>Backup Methods</b> - Select scp, ftp or tftp. Selecting tftp prompts only the Host and File Name fields that are required to fill in.</li> <li>• <b>Username</b> – User name used to log on to the remote device. The characters supported are: A-Z a-z 0-9 ! " # \$ % ' ( ) * + , - . / ; &lt; = &gt; ? ^ _ ` {   } ~. The characters that are not supported are: @ ,&amp; and :</li> <li>• <b>Password</b> – Password needed to access the remote device. See the supported and unsupported characters specified under Username.</li> <li>• <b>Host</b> – IP address of the remote device.</li> <li>• <b>File Location</b> – Absolute path to the directory where you want to store your backup.</li> <li>• <b>File Name</b> - Name of the Device Configuration Backup File.</li> </ul>

4. Click **Submit** to send the device configuration backup request.

If the backup was set to occur immediately, a confirmation message will appear, indicating whether the backup was successful.

---

**NOTE:** You can view the saved configuration backup files by following the procedure here:  
[Viewing Saved Configuration Backup Files](#).

---

## Remote Restore

You can remotely restore a configuration onto a device. To perform remote restore, perform the following:

1. On the **Devices >> Config Backups >> Configurations** page, click the **Remote Restore** button.

The Remote Restore Configuration window is displayed.

2. Enter the following details to remotely restore a configuration as shown in .

Table 91 : Remote Restore Configuration Window

Field	Description
Device	Select the device from the drop-down list.
Schedule Type	<p>Select whether you want to perform an immediate remote restore backup or schedule a remote restore backup at a recurring time.</p> <p>If Schedule is selected, enter the following:</p> <p>Start Datetime: If scheduling the remote restore backup for a future time, then enter the desired time in the field to specify the date and time when the remote restore backup should begin. Enter the date/time in the following format: mm/dd/yyyy hh:mm AM/PM</p> <p>Schedule Option: Click the drop-down menu and select the interval at which the remote restore backup configuration snapshots will be taken. Options are:</p> <p>One Time – The remote restore will be done at the time entered in the 'Start Datetime' field.</p>
Description	Text description for the remote restore job.
Restore Methods	<p>Select from the available methods: scp, ftp or tftp.</p> <p>Enter the following information</p> <ul style="list-style-type: none"><li>• Username – User name on the remote server. (Appears for scp and ftp) The characters supported are: A-Z a-z 0-9 ! " # \$ % ' ( ) * + , - . / ; &lt; = ? ^ _ ` {   } ~. The characters that are not supported are: @ ,&amp; and :</li><li>• Password – Password for the account used to access the</li></ul>

Table 91 : Remote Restore Configuration Window

Field	Description
	<p>remote server. (Appears for scp and ftp)</p> <ul style="list-style-type: none"> <li>• Host – IP address where the remote server is running.</li> <li>• File Path – File path on the remote server where the backup file is located.</li> </ul>

3. Click Submit.

## Deleting all Configurations

If you wish to delete all configurations, click on the “v” check box to expand and then click on “Delete all Configurations”.

## Viewing Saved Configuration Backup Files

When you have finished saving backup configuration files for one or more managed devices, you can view the inventory of backup files from the Configuration Backups page.

To view the previously saved Backup Configuration files, navigate as follows:

Select **Devices >> Config Backups**.

Table 92 : Description of the columns in the Configuration Backups table

Button	Description
Backup ID	Displays the auto-generated name of the backup config file. This identifier is a combination of the device model number and the timestamp associated with the backup config file.
Device	Displays the host name of the managed device.
Source IP	Displays the IP address of the managed device.
Description	<p>Displays the description information entered when the image file was copied to SecDevice.</p> <p><b>Note:</b> A default configuration backup file is automatically created when a managed device is first discovered by SecDevice. The Description field for this default file is, “Auto Config Backup”. An example appears in the figure above.</p>

Table 92 : Description of the columns in the Configuration Backups table

Button	Description
Created Time	Displays the date and time that the backup config file was created.
Actions	<p>Displays the available actions that can be performed with the backup config file:</p> <p>Contents – click the <b>Contents</b> link to modify the contents of a backup config file.  This is discussed in <a href="#">CLI / File Objects</a>.</p> <p>Restore – click the <b>Restore</b> link to restore a managed device using a saved config file.  This process is further discussed in <a href="#">Restoring a Device from a Backup Configuration File</a>.</p>

## Restoring a Device from a Backup Configuration File

You can use a previously-saved backup configuration file to restore an SecDevice-managed device to a previous state. This may be helpful if, for example, you need to roll back recent changes to a configuration file.

To restore a managed device using a previously-saved backup configuration file, navigate to the SecDevice GUI's Configuration Backup page as follows:

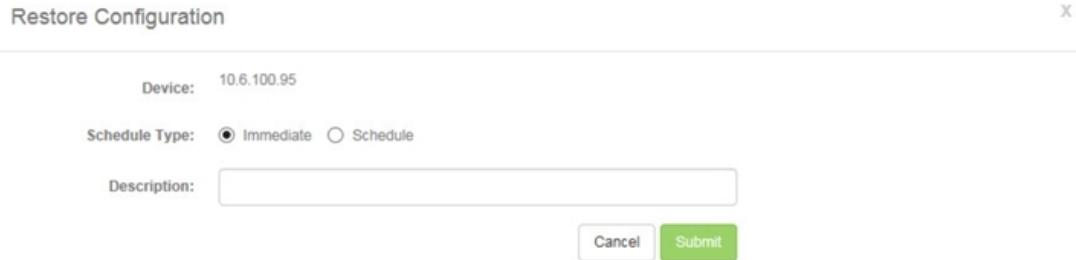
1. Select **Devices >> Config Backups**.

The inventory of backup configuration files appears in the Config Backups table.

2. Click the **Restore** link in the far-right Actions column, for the config file you wish to use to restore the managed device.

The Restore Configuration modal window appears, similar to that shown below:

Figure 38 : Devices >> Config Backups >> Restore



3. The Devices field list is populated with the IP of the managed device for which you selected the Restore hyperlink.
4. For the Schedule Type, select the **Immediate** radio button.
5. Enter a description in the Description field.
6. When finished configuring the options in the Restore Configuration window, click **Submit** to send the device restore request.
7. Navigate to Administration >>Job Execution Results to see if the restore operation has succeeded or failed. If it has succeeded, an ACOS device reboot without a saving the configuration is needed to allow the restored configuration to take effect.

**Additional Notes about the Configuration Backups table:**

- The most recent Backup Config files appear near the top of the Backups table.
- Instead of creating a configuration backup from the **Device List** page, as discussed in [Device Groups](#), you can also create a configuration backup file from this page by clicking **Backup Config** at the upper, right-most corner of the page. A pop-up modal window appears, as discussed in [Creating a Backup Configuration File for a Managed Device](#), but you must choose the devices or device group you want to back up from the list of currently-available devices.

## Device Settings

The Device Settings page allows you view existing settings as well as configure them. When Settings is highlighted, the following are selectable:

- [Connection](#) - Configure the port, timeout and retry attempts allowed for CLI, SNMP and HTTPS.
- [Device Rescan](#) - Configure a specific time and interval for SecDevice to rescan devices.
- [Health Monitor Settings](#) - Configure Health Monitor settings.
- [sFlow](#) - Configure SecDevice as an sFlow collector.
- [Statistics Display](#) - Set up an automatic refresh for the index table and statistics that are displayed in the SecDevice GUI.

Click on the feature you wish to use to navigate to the appropriate page.

## Connection

---

Connection allows you to enter the basic parameters that will define the sessions when SecDevice is attempting to discover managed devices. You can modify the properties for CLI, SNMP, or HTTPS sessions, and you can indicate which protocol port should be used, the duration of the idle timeout value, and the number of retry attempts.

1. To modify the Connection properties for the CLI, do as follows:
  - a. Enter the port number SecDevice should use when attempting to establish a CLI session with a managed device. For example, to use SSH enter port 22.
  - b. Type the value in the field to specify the idle Timeout period for the CLI session.
  - c. Type the value in the field to specify the Retry Attempts for the CLI session. This will specify how many times SecDevice should attempt to establish a CLI session with a managed device before giving up.
  - d. Click Save to store your changes.
2. To modify the Discovery properties for SNMP, do as follows:
  - a. Enter the port number SecDevice should use when attempting to use SNMP to communicate with a managed device. For example, to use the standard SNMP port, enter a value of 161.
  - b. Type the value in the field to specify the idle Timeout period for the SNMP session.

- c. Type the value in the field to specify the number of Retry Attempts. This will specify how many times SecDevice should attempt to establish an SNMP session with a managed device before giving up.
  - d. Click Save to store your changes.
3. To modify the Discovery properties for HTTPS, do as follows:
- a. Enter the port number SecDevice should use when attempting to use HTTPS to communicate with a managed device. For example, to use the standard HTTPS port, enter a value of 443.
  - b. Type the value in the field to specify the idle Timeout period for the HTTPS session.
  - c. Type the value in the field to specify the number of Retry Attempts. This is the number of times SecDevice should attempt to establish an HTTPS session with a managed device before giving up.
  - d. Click Save to store your changes.

## Device Rescan

---

The Device Rescan page allows you to set up periodic rescans from SecDevice. When a device rescan job has been created, the job can be viewed from the Scheduler (Administration >> Scheduler), and past jobs can be viewed from Job Execution Log.

To configure this, do the following:

1. In the Start Datetime field, enter the scheduled time for the device rescan in the following format: mm/dd/yyyy hh:mm AM/PM
2. In the Schedule Option drop-down list, select a time interval.
3. In the Description field, enter any information you wish to include regarding this action.
4. Click Save to finish.

## Health Monitor Settings

---

The Health Monitors page allows you to configure basic SecDevice health monitors, which SecDevice uses to poll for devices under its management. In the current

release, the following health monitors are supported:

- PING
- HTTPS

Navigate to Devices >> Device Settings and click on Health Monitor.

1. To modify the properties for the PING health monitor:
  - a. In the Retry Attempts field, enter the number of times SecDevice should attempt to PING a managed device before determining that the device has failed the health check. The up and down arrows may be used to increase or decrease the value in this field by 1.
  - b. In the Timeout (In seconds) field, enter the number of seconds SecDevice should wait after sending a PING to a managed device before determining that the device has failed the health check. The up and down arrows may be used to increase or decrease the value in this field by 1.
  - c. Click Save to store your changes.
2. For HTTPS health monitor properties:

Although HTTPS health checks are supported, their properties (such as Retry Attempts and Timeout value) cannot be modified in the current release.
3. (Optional) You can modify the Interval, which is the period at which the health monitor will repeat the check.

By default, the interval is set to 30 seconds.
4. Click Save to store your changes.

## sFlow

---

The sFlow page allows you to set up SecDevice as an sFlow collector, with the managed devices sampling random packets and sending statistics in an sFlow datagram to SecDevice for analysis.

Navigate to Devices >> Device Settings, and click on sFlow.

To configure sFlow, do the following:

1. Click on the sFlow Collector IP gear icon and select the IP address to be used as an sFlow collector in the Pick an IP window, or enter an IP address manually in the sFlow Collector IP field.
2. Enter the Polling Interval value for sFlow collection.
3. Click Save to finish.

---

**NOTE:** When an sFlow's IP is changed, it is updated to all managed devices. In order to remove the configuration, input 0.0.0.0 in the sFlow Collector IP field, as 0.0.0.0 is recognized to push SecDevice's management interface address (for example, eth0's IPv4 address) to devices as the sFlow collector IP.

---

## Statistics Display

---

The Statistics Display page allows you to set up an automatic refresh for the index table and statistics that are displayed in the SecDevice GUI. If desired, you can change the automatic refresh rate of index tables and stats by doing the following:

1. Navigate to Devices >>Device Settings, and click on Statistics Display.
2. To configure the Index Table automatic refresh rate interval, enter the interval rate in the Index Table field. The number of repeated attempts ranges from 5-30 seconds.
3. To configure the Statistics automatic refresh rate interval, enter the interval rate in the Stats field. The range is 5-30 seconds.
4. Click Save to save any changes.

## SSL Management

SSL Management is made up of two sections:

- [SSL Management Local SSL Certs](#)

View SSL Certs on SecDevice and push them to devices.

- [SSL Management Device SSL Certs](#)

View SSL Certs on devices and save them locally onto SecDevice.

## SSL Management Local SSL Certs

The SSL Management Local SSL Certs page has an inventory of the SSL files that you have saved locally on SecDevice. From this page, you can push the files to other managed devices.

describes the columns in the SSL Management Local SSL Certs page:

Table 93 : Description of columns in Local SSL Certs

Button	Description
Name	Name of the system file.
Last Modified Time	Shows the date and time when the file was last modified.
Expiration Date	Indicates the expiration date of the certification or key.
Type	For SSL certs, indicates if certificate or key is selected.
Actions	Edit - Allows you to edit the content of the selected SSL file.  Push - Allows you to push the file to a managed device or device group.

### Editing an SSL file

From the Local SSL Certs tab, click the Edit link under the Actions column for the file you wish to edit.

### Pushing an SSL file

From the Local SSL Certs tab, click the Push link under the Actions column for the file you wish to push.

Figure 39 : Configuration &gt;&gt; SSL Management &gt;&gt; Local SSL Certs &gt;&gt; Push

**Push**

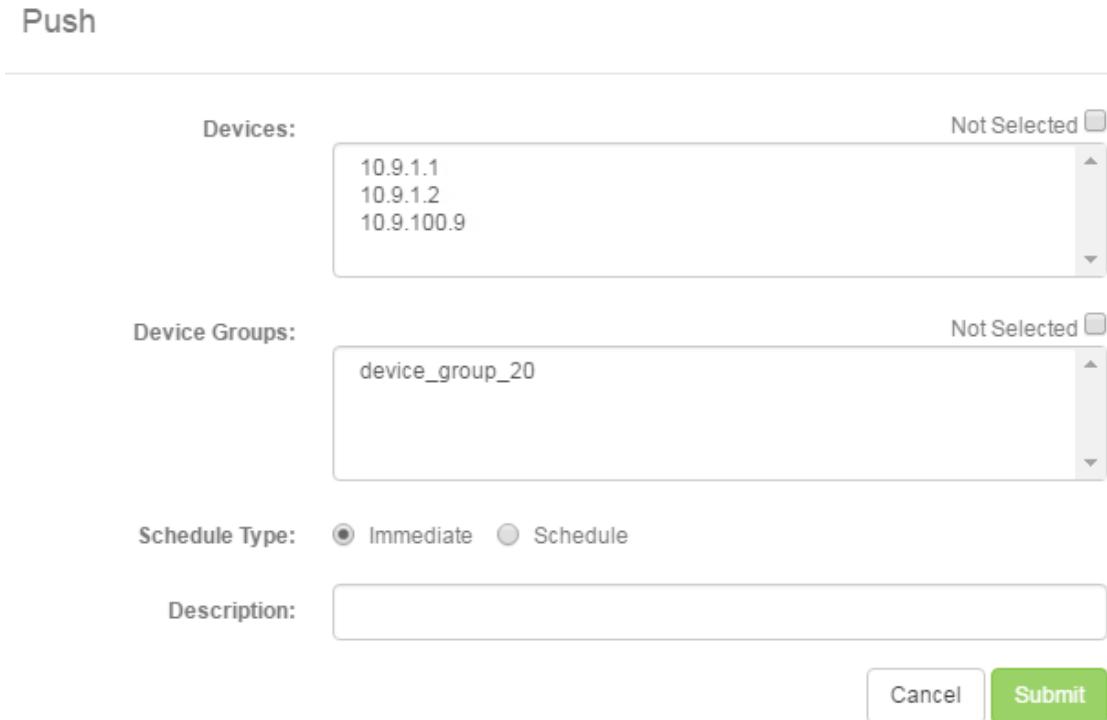
**Devices:** Not Selected   
10.9.1.1  
10.9.1.2  
10.9.100.9

**Device Groups:** Not Selected   
device\_group\_20

**Schedule Type:**  Immediate  Schedule

**Description:**

**Cancel** **Submit**



1. Select one or more devices to determine where the file will get pushed.
2. Select the group from the Device Groups section of the page.
3. Configure the Schedule Type by selecting Immediate, if not already selected.
4. Configure the Interval, and any other mandatory options in the Push Configuration window.  
For more information about these options, see [Config Backups](#).
5. When finished configuring the Push Device Configuration window, click **Submit**.

### Creating an SSL Cert

Take the following steps after clicking Create.

1. Click on the SSL Cert type: Certificate, Key
2. Enter the name in the Name field.
3. Enter the Content in the Content field.
4. Click Submit.

## Import an SSL Cert

Take the following steps after clicking Import.

1. Click on the SSL Cert type: Certificate, Key
  2. Enter the name in the Name field.
  3. In File Upload, click Choose File and select the file to import.
  4. Click Submit.

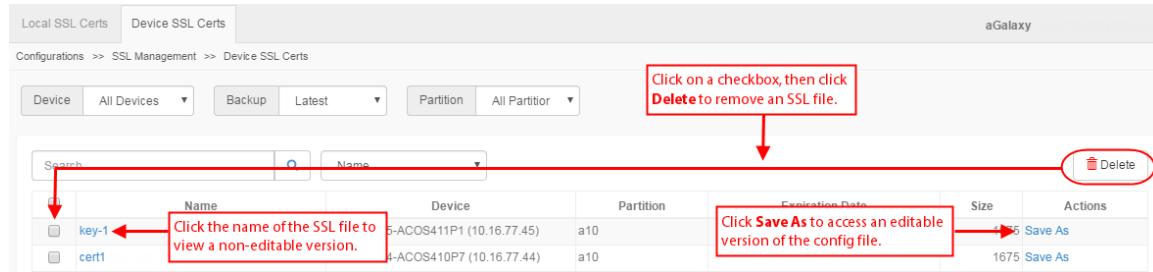
## SSL Management Device SSL Certs

The SSL Management Device SSL Certs page has an inventory of the most recent SSL files. From this page, you can edit an SSL file, then save it locally to SecDevice, see [SSL Management Local SSL Certs](#), and push it to a managed device.

To edit an SSL file, navigate as follows:

1. Select **Configurations >> SSL Management** and click on **Device SSL Certs**.
  2. Click the **Save As** hyperlink under the Actions column, at far-right.
  3. When done editing, click Save.

Figure 40 : Configurations >> SSL Management >> Device Config



To delete a device's SSL certificate, key, or CRL file, navigate as follows:

1. Select **Configurations** >> SSL Management
  2. Click on the Device SSL Certs tab.

From here, select the checkbox next to the SSL related file you wish to delete from a device and click on Delete.

---

**NOTE:** A configuration backup must first be done in order to use the delete functionality following an upgrade to SecDevice 3.0.4-P2 if upgrading from a version older than 3.0.4-P1. Upon upgrade to SecDevice 3.0.4-P2, the system will automatically trigger a backup.

---

shows information about the columns of the “Configurations >> SSL Management >> Device SSL Certs” table:

Table 94 : Columns in Configuration Backups Contents table

Button	Description
Name	Displays the name of this file.
Device	Displays the name of the device.
Partition	Displays the partition (shared or private) where the file is located.
Expiration Date	Displays the expiration date of an SSL certificate.
Size	Displays the size (in bytes) of this file.
Actions	The Action column displays the available actions that can be performed with this portion of the config file.  Save As – click the <b>Save As</b> link to modify an SSL file.

## CLI / File Objects

The CLI / File Objects page allows you to create and push CLI Config Snippets, class-lists, domain-lists, scripts, and A10 threat intel to the another device.

- To work with CLI config snippets, navigate to Configurations >> CLI / Threat Intel >> CLI Config Snippets.
- To work with Class-Lists, navigate to Configurations >> IPs / Domains >> Class-Lists.
- To work with Domain-Lists, navigate to Configurations >> IPs / Domains >> Domain-Lists.
- To work with Scripts, navigate to Configurations >> TPS Other Objects >> Scripts.

- To work with A10 Threat Intel, navigate to Configurations >> CLI / Threat Intel >> A10 Threat Intel.

## CLI Config Snippets

---

The CLI Config Snippets helps to save the chunks or portions of the backup config files that you modified and push them to other managed devices.

Table 95 : Description of columns in CLI Config Snippets

Button	Description
Name	Name of the system file.
Last Modified Time	Shows the date and time when the file was last modified.
Actions	Edit—Allows you to edit the content of the selected configuration file. Push—Allows you to push the configuration to a managed device or device group.

Perform the following:

1. Select **Configurations >> CLI / Threat Intel >> CLI Config Snippets**.
2. (Optional) From the CLI Config Snippets page, you can further edit portions of the config file by clicking the **Edit** link under the Actions column. (For information about editing a CLI Config, or another portion of a config file, see [SSL Management](#).)
3. When you are finished modifying the portion of the configuration backup file, you can push that portion of the config to another device by clicking the **Push** link, which appears in the right-most Actions column.

---

**NOTE:** Note: The Push action for CLI Config applies when you wish to put a running configuration onto a device or device group. To back up or restore start up configurations, go to [SSL Management](#).

---

**CAUTION:** When pushing a CLI Config, make sure your CLI snippet is not device-specific. Also, some commands cannot be pushed as CLI config. Please see the “known issues” section of the SecDevice Release Notes for a list of restricted CLI commands.

4. Select one or more devices to choose where the CLI snippet (or other portion of the config file) will get pushed.
5. Select one or more device groups from the Device Groups section of the page to choose the group(s) to push the CLI snippet.
6. Click the Partitions drop-down menu and select Shared or the name of the private partition. This selection will determine where on the target device (i.e. which partition) the configuration snippet will be pushed. Keep in mind that the configuration snippet will be pushed to this same partition across all of the selected target devices (if multiple devices are selected).
7. Configure the Schedule Type by selecting Immediate, if not already selected.
8. Configure the Interval, and any other mandatory options in the Push Configuration window.  
For more information about these options, see [Config Backups](#).
9. When finished configuring the Push Device Configuration window, click **Submit**.

#### Details:

The process of pushing other portions of the Config file to managed devices is virtually the same as the procedure shown above. However, when pushing a CLI configuration snippet, that small snippet is merged with the running config on the target device, whereas when pushing a Class-List, then the whole file is pushed to the target device, overwriting any existing files on the target device.

#### Creating a Configuration

Perform the following steps based on the configuration you wish to create:

1. Enter the name in the **Name** field.
2. Enter the Content in the **Content** field.
3. Click **Submit**.

## A10 Threat Intel

The A10 Threat Intel page allows you to set up the A10 Threat Intel class-lists.

Perform the following to set up an A10 Threat Intel class-lists:

1. Select **Configurations >> CLI / Threat Intel >> A10 Threat Intel**.
2. In the **ThreatSTOP VM IP Address** field, enter the ThreatSTOP IP address.
3. In the **ThreatStop VM Username** and **Password** fields, enter the credentials to connect to ThreatSTOP.
4. In the **Class-List** File name, enter the name that the TPS must use while saving the class-lists imported from the ThreatSTOP.
5. In the **Number of Class-List** files to Import, enter the number of class-list files to be selected on the ThreatSTOP portal.
6. In the **Periodic Interval** field, specify the frequency at which the TPS must download the class-list.
7. For **Select a Device**, select a TPS Device to import Class-Lists.
8. On the selected TPS Device, you can perform any of the following:
  - a. Click **Apply Class-List Import** to populate the class-lists on the selected TPS device from ThreatSTOP.
  - b. Click **Show Class-List** to view all the class-lists.
  - c. Click **Show Class-Lists Import** to view all the imported class-lists.

## CLI / File Objects

The CLI / File Objects page allows you to create and push CLI Config Snippets, class-lists, domain-lists, scripts, and A10 threat intel to another device.

- To work with CLI config snippets, navigate to **Configurations >> CLI / Threat Intel >> CLI Config Snippets**.
- To work with Class-Lists, navigate to **Configurations >> IPs / Domains >> Class-Lists**.

- To work with Domain-Lists, navigate to Configurations >> IPs / Domains >> Domain-Lists.
- To work with Scripts, navigate to Configurations >> TPS Other Objects >> Scripts.
- To work with A10 Threat Intel, navigate to Configurations >> CLI / Threat Intel >> A10 Threat Intel.

## Class-Lists

The class-lists page allows you configure a list of IPv4 or IPv6 addresses.

Table 96 : Description of columns in Class-Lists

Button	Description
Name	Name of the system file.
Last Modified Time	Shows the date and time when the file was last modified.
Type (For Class-Lists)	Shows class list type.
Size	Shows class list size.
Actions	<ul style="list-style-type: none"> <li>• <b>Edit</b>—Allows you to edit the content of the selected configuration file.</li> <li>• <b>Push</b>—Allows you to push the configuration to a managed device or device group.</li> <li>• <b>Download</b>—Allows you to download the class-list as a file.</li> <li>• <b>Used in Zones</b>—Allows you to find all zones associated with the class-list.</li> </ul>

Perform the following to create or edit a class-list:

1. Select **Configurations >> IPs / Domains >> Class-Lists**.
2. (Optional) From the Class-Lists page, you can further edit the IP address by clicking the **Edit** link under the Actions column.
3. When you are finished modifying the class-list, you can push the file to another device by clicking the **Push** link, which appears in the right-most Actions column.

4. Select one or more devices to choose where the class-list will get pushed.
5. Select one or more device groups from the Device Groups section of the page to choose the group(s) to push the class-list.
6. Click the Partitions drop-down menu and select Shared or the name of the private partition. This selection will determine where on the target device (i.e. which partition) the configuration snippet will be pushed. Keep in mind that the configuration snippet will be pushed to this same partition across all of the selected target devices (if multiple devices are selected).
7. Configure the Schedule Type by selecting Immediate, if not already selected.
8. Configure the Interval, and any other mandatory options in the Push Configuration window.  
For more information about these options, see [Config Backups](#).
9. When finished configuring the Push Device Configuration window, click **Submit**.
10. To find the zones associated to the class-list, click **Used in Zones**. On the Associated Zones pop-up, the name of the associated zone is displayed.

## Creating a Class List

Perform the following to create a class list:

1. Enter the name in the **Name** field.
2. For **Type**, select one of the following:
  - IPv4-Creates a class list with IPv4 addresses
  - IPv6-Creates a class list with IPv6 addresses
  - Geo or Geo-IPv6- Creates a class list consisting of Geo Locations
3. Enter the Content in the **Content** field.

For Geo and Geo-IPv6, you can add the Geo Location from **Add from Geo Location**: drop-down list. Select the continent from the drop-down. Choose the countries from the list box and click **Apply**. To add all the countries within the continent to the class list, select **Select All Countries** and click **Apply**.

4. Click **Submit**.

## Source Based Policy

This page displays all configured source based policies, and allows you to do the following:

### Create a Source Based Policy

To create a new source based policy, click the green “New Source Policy” button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a TCP Template](#).

To create a new Source Based Policy:

1. Select **Configurations >> Templates >> General**.
2. Select the Src Based Policy tab if not already selected, then click the **New Source Policy** button at the upper right.
3. In the Name field, enter the name for the Source Based Policy.
4. For the Class list field, click Add and select a class list from the drop-down list to use for the source based policy.
5. Click **Submit** to create or update your policy.

### Edit a Source Based Policy

To edit a previously configured source based policy, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Delete a Source Based Policy

To delete a configured source based policy, select the checkbox next to the source based policy and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that item.

### View Previously Configured Source Based Policy

The main source based policy page displays a table of configured source based policy along with information about them.

Table 97 : Information About Previously Configured GLIDs

Field	Description
Name	The name of the source based policy
Actions	<p>Edit—Allows you to edit the source based policy. In order to make changes to a source based policy configuration, click edit. For information on configurable parameters, seeConfigure a Source Based Policy.</p> <p>Duplicate—Creates an object with basic parameters that are identical to the original object.</p> <p>Used in Zones—Allows you to find all zones associated with the source-based policy.</p>

## Configure a Source Based Policy

The configuration options available while configuring a source based policy are:

1. Name - Enter the Name of the source based policy. The supported value is a string of 1-63 characters.  
If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.
2. Class list - Specify the class list to apply to the source based policy.

## Domain-Lists

The domain-lists page allows you configure a domain classification list which is then added to the domain group. Under the domain group, you can either permit or deny the traffic matching the domain list configurations.

Table 98 : Description of columns in Domain-Lists

Button	Description
Name	Name of the system file.
Last Modified Time	Shows the date and time when the file was last modified.

Table 98 : Description of columns in Domain-Lists

Button	Description
File Size	Shows domain list size.
Actions	Edit—Allows you to edit the domain list. Push—Allows you to push the domain list to a managed device or device group. Download—Allows you to download the domain list as a file.

Perform the following to create or edit a domain-list:

1. Select **Configurations >> CLI / File Objects >> Domain-Lists**.
2. (Optional) From the Domain-Lists page, you can further edit portions of the config file by clicking the **Edit** link under the Actions column.
3. When you are finished modifying the portion of the configuration backup file, you can push that portion of the config to another device by clicking the **Push** link, which appears in the right-most Actions column.
4. Select one or more devices to choose where the domain list will get pushed.
5. Select one or more device groups from the Device Groups section of the page to choose the group(s) to push the domain list.
6. Click the Partitions drop-down menu and select Shared or the name of the private partition. This selection will determine where on the target device (i.e. which partition) the configuration snippet will be pushed. Keep in mind that the configuration snippet will be pushed to this same partition across all of the selected target devices (if multiple devices are selected).
7. Configure the Schedule Type by selecting Immediate, if not already selected.
8. Configure the Interval, and any other mandatory options in the Push Configuration window.  
For more information about these options, see [Config Backups](#).
9. When finished configuring the Push Device Configuration window, click **Submit**.

## Creating a Configuration

Perform the following steps based on the configuration you wish to create:

1. Enter a name in the **Name** field.
2. Under Content, enter the domain name information. Each line must contain one <match type> <domain name> entry where match type can be 'suffix' or 'equals'. If you are using zone-transfer, the zone format should be <zone-transfer> <domain name> <ip-address> <port> <refresh-interval>. Configuring zone transfer helps in mitigating DDoS attacks related to authoritative DNS subdomain.
3. Click **Submit**.

## Domain Group

---

A domain group allows you to select the domain lists and determine whether to permit or deny the traffic matching the configured domain list.

To create a domain group:

1. In the Name field, enter a name for the device group.
2. From the Domain List drop-down list, select the name of the domain list that you want to add to the domain group.
3. From the Action drop-down list, select the appropriate action.
4. For Domain Rate, select the domain list and specify the Per Suffix Rate.
5. Click **Submit**.

## IP Filtering Policy

---

IP Filtering Policy allows you to create a policy to take an action on incoming traffic and apply the policy to a zone service.

To create a new IP filtering policy, perform the following:

1. Select **Configurations >> IPs / Domains >> IP Filtering Policy**.
2. Click the green “Create IP Policy” button at the top right corner of this page.
3. In the **Policy Name** field, enter a name for the IP filtering policy.
4. For the **No Rule Match Action** rule, select one of the actions.

- **Permit:** Permits incoming traffic even if no rule matches the policy. This is the default setting.
- **Drop:** Drops the traffic if no rule matches the policy.

5. Click **Save**.

## Adding a Rule for IP Filtering Policy

After you create an IP Filtering Policy, you should add a rule with attributes for match-conditions, actions, and global limit IDs (GLIDs) for the IP filtering policy. You can add up to 100 rules to make filtering decisions for the packets.

To add a new rule for IP filtering policy, perform the following:

1. In the **Sequence** field, enter a sequence number for the filter.

You can add up to 200 sequences to prioritize the rule application. This sequence is helpful when you create multiple rules to filter the traffic.
2. From the **Action** drop-down list, select one of the actions from the following options.
  - **Drop:** Drops all the packets.
  - **Permit:** Permits all the packets.
  - **Bypass:** Bypasses the rule to accept all the packets.
  - **Blacklist:** Blacklists and drops all the packet source, when the configured GLID exceeds the set rate-limit threshold.
3. From the **Glid** drop-down list, enter a **Glid**.

The Glid drop-down list appears enabled, only if you select **Blacklist** as an action for the traffic. This list appears from predefined GLID settings to enforce the bit and packet rate limits. This rule attribute is used to detect the botnet attacks.
4. In the **Source IP Address** field, enter a source IP address from where the traffic originates.
5. From the **Source Port** drop-down list, select the source port operator either as **Equals** or in **Range**.

If you select Equals as an operator, enter a source port number. If you select Range as an operator, enter the source port range with from and to port numbers.

---

**NOTE:** Source IP Address and Source Port prevent excessive or malicious traffic from a known port or subnet.

---

6. In the **Destination IP Address** field, enter a destination IP address suspected to be under attack.
7. From the **Destination Port** drop-down list, select the destination port operator either as **Equals** or in **Range**.

If you select Equals as an operator, enter a destination port number. If you select Range as an operator, enter the destination port range with from and to port numbers.

---

**NOTE:** Destination IP Address and Destination Port regulate traffic to a host.

---

8. From the **Protocol** drop-down list, select a protocol from TCP, UDP, ICMPV4, ICMPV6, or Protocol Num (Protocol Number) for your traffic type.

Based on the selected protocol, relevant options appear. All irrelevant options appear disabled.

If you select TCP, enter TCP Flags and TCP Flags Bitmask. If you select ICMP protocol, enter ICMP Type and ICMP Code.

For detailed information about IP Filtering Policy, see [DDoS Mitigation Guide](#).

## Other System Settings

- [User Management](#) Configuration [Role Management]

This requires the configuration of:

- [Privileges](#)

- [Roles](#)
- [Users](#)

Related configurations are:

- [External Authentication Role Mapping](#)
- [RADIUS Configuration](#)
- [TACACS Configuration](#)
- [LDAP Configuration](#)
- [Authentication Sequence](#)
- [High Availability \(HA\)](#)

Configure High Availability for SecDevice 5000 hardware

#### [Recovering from High Availability Failure Events](#)

Steps to take if High Availability failure occurs.

## Miscellaneous Configurations and Features

- [Connection](#)

Configure the port, timeout and retry attempts allowed for device connections for CLI, SNMP and HTTPS sessions.

- [Health Monitor Settings](#)

Configure basic SecDevice Health Monitor settings for devices, such as retry attempts, timeouts and interval rate.

- [Consoleadmin](#)

Perform operations such as an SecDevice backup/restore and upgrading.

- [Statistics Display](#)

Change the auto refresh interval rate for index tables and stats.

- aGAPI REST API for SecDevice

General information on how to access and use aGAPI is provided.

## Debugging and Support

### Threat Protection System Debugging

- Configure a job for [Packet Capture](#).

    Navigate to Monitoring & Reporting >> Packet Capture

    or

    From the Mitigation >> Zone Mitigation Console or Mitigation >> Dest Entry Mitigation Console page, click Packet Debugger for a currently live mitigation.

### Issue with SecDevice

- Create a file for [Web](#).
- Create SecDevice System Logs file for tech support.
- Navigate to Administration >> Maintenance >> Tech Support

---

**NOTE:** For information about alerts, events, logging and job results that may also help provide additional information for debugging, see [Notification](#).

---

### Call Home

- Enable [Call Home](#) to allow SecDevice to send A10 hardware and software information to Organization to facilitate communications in identifying potential issues.
- Navigate to Administration >> Settings >> Call Home

A route to “acxis.a10networks.com” from SecDevice is required prior to enabling the Call Home feature.

---

**NOTE:** No customer specific data is sent when using this feature.

---

# TPS Zone Templates

---

Zone templates must be configured prior to binding them to the zone.

The following topics are covered:

<a href="#"><u>TCP</u></a>	275
<a href="#"><u>UDP</u></a>	283
<a href="#"><u>DNS</u></a>	288
<a href="#"><u>QUIC</u></a>	295
<a href="#"><u>HTTP</u></a>	298
<a href="#"><u>SLL-L4</u></a>	307
<a href="#"><u>ICMP-v4/v6</u></a>	311
<a href="#"><u>IP Proto</u></a>	314
<a href="#"><u>Encapsulation</u></a>	317
<a href="#"><u>SIP</u></a>	319
<a href="#"><u>Source Port TCP Template</u></a>	323
<a href="#"><u>Source Port UDP Template</u></a>	325

# TCP

The following topics are covered:

<a href="#">Manage a TCP Template</a> .....	275
<a href="#">Configure a TCP Template</a> .....	276

## Manage a TCP Template

---

### Create a TCP Template

To create a new template, click the green **New TCP Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Edit a TCP Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Delete a TCP Template

To delete a configured template, select the check box next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured TCP Templates

The main TCP Template page displays a table of configured TCP templates along with information about them.

Table 99 : Information About Previously Configured TCP Templates

Column Heading	Description
Name	Displays the name of the template.
Session Age (mins)	Displays the length of time, in minutes that a session is active.
Concurrent Connection	Indicates if Concurrent Connection option is enabled. ✓ – Enabled; ✗ – Disabled
SYN Cookie	Indicates if the SYN Cookie option is enabled. ✓ – Enabled; ✗ – Disabled
SYN Authentication	Indicates if the SYN Authentication option is enabled. ✓ – Enabled; ✗ – Disabled
Actions	<ul style="list-style-type: none"> <li><b>Edit</b>—Allows you to edit the template. In order to make changes to a template configuration, click edit.</li> <li><b>Duplicate</b>—Creates an object with basic parameters that are identical to the original object.</li> <li><b>Used in Zones</b>—Allows you to find all zones associated with the template.</li> </ul>

## Configure a TCP Template

Perform the following actions to configure a TCP template:

1. Go to **Configurations >> TPS Zone Templates >> TCP**.
2. Click **+ New TCP Template** and enter the following information:

Table 100 : Field and its purpose for Create TCP Template window.

Field	Purpose
Name	Enter a name for the template.

Field	Purpose
	<p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Session Age	Enter the maximum amount of time a TCP session can remain idle. Time should be either in minutes or seconds.
Age Out Server Reset	Select <b>Age Out Server Reset</b> to send TCP reset request to server if aging time has passed.
Half Open Timeout	Enter the maximum time in seconds for a TCP 3-way handshake to complete.
Half Open Timeout Server Reset	Select <b>Half Open Timeout Server Reset</b> to send TCP reset request to server if TCP half-open session times out.
Allow TCP Fast Open	Select <b>Enabled</b> to speed up the opening of the TCP connections between the two end points.
Concurrent Connection	<p>Select <b>Enabled</b> to enable the concurrent connection support on multiple protocol ports. The rule allows subsequent requests to other ports. However, if the entry to other ports is not allowed, this option enables the source to send a request to that particular port.</p> <p>For example, enabling concurrent connection is required for passive FTP to work, if <b>Drop On No Port Match</b> option is enabled at the Layer 4 TCP level in the destination rule for the FTP server.</p> <p><b>NOTE:</b> The concurrent command allows traffic to any port. Use this command only if you require to support the legitimate traffic.</p>
SYN Cookie	Select <b>Enabled</b> for a strict TCP authentication. SYN cookies are used to challenge the sender of every TCP-SYN, even if

Field	Purpose
	<p>the sender has already passed the authentication.</p> <p>SYN Authentication is disabled if you select this option.</p>
Connection SYN Only	<p>Select <b>Enabled</b> to create a connection on SYN only.</p>
SYN Authentication	<p>Configure SYN Authentication to enable TCP authentication for senders of TCP SYNs.</p> <ul style="list-style-type: none"> <li>• <b>Type</b>—Choose the appropriate authentication process used for SYN Authentication.</li> <li>• <b>Fail Action</b>—Choose the appropriate action to be performed when the authentication fails.</li> <li>• <b>Fail Action List</b>—Choose the appropriate action list to be applied when the authentication fails.</li> </ul> <p>If Action List is chosen, only then the Fail Action List drop-down is displayed.</p> <ul style="list-style-type: none"> <li>• <b>Type</b>—Choose the appropriate authentication process used for SYN Authentication.</li> <li>• <b>Fail Action</b>—Choose the appropriate action to be performed when the authentication fails.</li> <li>• <b>Pass Action List</b>—Choose appropriate action list to be applied when the authentication passes.</li> </ul> <p>If Action List is chosen, the Pass Action List drop-down is displayed.</p>
SYN-ACK Reset	<p>Select the check box to send reset when SYN-ACK is received.</p>
Connection Rate Limit on SYN Only	<p>Select the check box to specify whether the connection rate limit is applicable only for SYN.</p>
Allow SYN Other Flags	<p>Select the check box to treat TCP SYN+PSH as a normal TCP SYN. This option is only supported on TCP ports.</p>
Out of Sequence	<p>Enter the maximum number of TCP sequence errors</p>

Field	Purpose
Packets	allowed for a client session. If this limit is exceeded, the client is added to the Black List.
Retransmit Packets	Enter the maximum number of retransmitted TCP packets (segments) allowed for a client session. If this limit is exceeded, the client is added to the Black List.
Zero Window Packets	<p>Enter the maximum number of TCP packets with receive window size 0 allowed for a client session. The client's receive window is the maximum amount of data the client is willing to accept per TCP packet from the server.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed when the zero window packets exceed the configured threshold.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when the zero window packets exceed the configured threshold.</li> </ul> <p>If Action List is selected, only then the Action List drop-down is displayed.</p>
Known Response Source Port	<p>Select the check box to enable any well-known source port number to take action on traffic.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed on the matching traffic.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied on the matching traffic.</li> </ul> <p>If Action List is chosen, only then the Action List drop-down is displayed.</p> <p>To perform <b>Exclude identical source and destination port pair</b> function, select the check box.</p>
Per Connection Packet Rate Limit	Enter the maximum number of packets allowed for an individual connection (source-destination flow) per interval.

Field	Purpose
	<ul style="list-style-type: none"> <li><b>Action</b>—Choose the appropriate action to be performed when the rate limit exceeds the configured threshold.</li> <li><b>Action List</b>—Choose the appropriate action list to be applied when the rate limit exceeds the configured threshold.</li> </ul> <p>If Action List is chosen, only then the Action List dropdown is displayed.</p>
Per Connection Rate Interval	<p>The interval can be 100 milliseconds (ms) or 1 second (set by the Per Connection Rate Interval option), and is independent of the globally set DDoS Mitigation interval. Choose one of the following options:</p> <ul style="list-style-type: none"> <li>100ms</li> <li>10 seconds</li> <li>1 second</li> </ul> <p>The default is 1 second.</p> <p>Choose the interval for per-connection packet-rate limiting. The interval set by this option only applies to the rate limiting set by the Per Connection Packet Rate Limit.</p>
Per Connection Out of Sequence Rate Limit	<p>Enter the maximum number of TCP sequence errors allowed for a client session.</p> <p>See <a href="#">Configure a TCP Template</a> and <a href="#">Configure a TCP Template</a> fields to enter the appropriate information.</p>
Per Connection Retransmit Rate Limit	<p>Specifies the maximum number of retransmitted TCP packets (segments) allowed for a client session.</p> <p>See <a href="#">Configure a TCP Template</a> and <a href="#">Configure a TCP Template</a> fields to enter the appropriate information.</p>
Per Conn Zero Window Rate Limit	<p>Specifies the maximum number of TCP packets with receive window size 0 allowed for a client session. The client's receive window is the maximum amount of data the client is willing to accept per TCP packet from the server. If this</p>

Field	Purpose
	<p>limit is exceeded, the client is added to the Black List.</p> <p>See <a href="#">Configure a TCP Template</a> and <a href="#">Configure a TCP Template</a> fields and enter the appropriate information.</p>
ACK Authentication	<p>Select the check box to authenticate TCP ACK for which ACOS has no session-table entry. This option enables TCP authentication for client-to-server streams that are redirected to the Thunder TPS device after the 3-way handshake has occurred. When this option is enabled, ACOS drops the first ACK from a client and waits for the client to retransmit the same ACK. If enabled, this feature has the following defaults:</p> <ul style="list-style-type: none"><li>○ If the client replies with a valid ACK after a specified minimum retry gap interval and within the specified timeout period, ACOS marks the client as authenticated.</li><li>○ If the client does not reply within the timeout period, or sends an invalid reply, ACOS drops the packet.</li><li>● <b>Retransmit Check</b>—Select the check box to allow a retransmit check applying a minimum delay and ACK retransmit timeout period configuration. If Retransmit Check is selected for ACK Authentication, following options are displayed:</li><li>● <b>Minimum Delay</b>—Enter the minimum interval required between the time ACOS drops the first ACK and the time ACOS receives a retry (another copy of the same ACK from the same sender). If a retry is received before the minimum amount of time has passed, ACOS will drop the retry packet and reset the gap timer. The supported value (Type) is 1 to 80 (100 ms) [Example 100ms to 8000ms (8 seconds)].</li><li>● <b>ACK Retransmit Timeout</b>—Enter the maximum number of seconds ACOS waits for a valid ACK in reply.</li><li>● <b>RTO Authentication</b>—Select the check box to enable the</li></ul>

Field	Purpose
	<p>RTO authentication.</p> <ul style="list-style-type: none"> <li>• <b>Once Per Source</b>—Select the check box to authenticate TCP ACK only once per source entry.</li> </ul> <p>See <a href="#">Fail Action—Choose the appropriate action to be performed when the authentication fails.</a>, <a href="#">Fail Action List—Choose the appropriate action list to be applied when the authentication fails.</a> If Action List is chosen, only then the Fail Action List drop-down is displayed., <a href="#">Configure a TCP Template</a> and <a href="#">Pass Action List—Choose appropriate action list to be applied when the authentication passes.</a> If Action List is chosen, the Pass Action List drop-down is displayed. fields to enter the appropriate information.</p>
Allow SYN-ACK Skip Authentication	<p>Select the check box to allow to create sessions on SYN-ACK without syn-auth and ack-auth (asymmetric Mode only).</p> <ul style="list-style-type: none"> <li>• <b>SYN-ACK Rate Limit</b>—Specify the maximum number of SYN-ACK.</li> <li>• <b>Track together with syn</b>—Select the check box to count the SYN-ACK in destination syn rate limit.</li> </ul>
Action on ack rto retry count	Configure to take action if ack-auth RTO-authentication fail over retry time. The default is 5.
Action on syn rto retry count	Configure to take action if syn-auth RTO-authentication fail over retry time. The default is 5.
Source syn rate limit	<p>Select the check box to configure source SYN rate limiting.</p> <ul style="list-style-type: none"> <li>• <b>Rate</b>—Specify the maximum number of source SYN rate.</li> <li>• <b>Action</b>—Choose the appropriate action to be performed.</li> </ul>
Destination syn rate limit	<p>Specify the check box to configure destination SYN rate limiting.</p> <ul style="list-style-type: none"> <li>• <b>Rate</b>—Specify the maximum number of destination SYN rate.</li> </ul>

Field	Purpose
	<ul style="list-style-type: none"> <li><b>Action</b>—Choose the appropriate action to be performed.</li> </ul>

3. In the **Filter** field, content of TCP payload is filtered and specified action is applied to the matching (on non-matching) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click **Add** to include:

Table 101 : Information on Filter field.

Column Heading	Description
Name	Enter the name for the filter.
Sequence Number	Enter the sequence number for the filter.
Regex	Enter the filter string to match. A regular expression can be a string of up to 1275 characters in length. The ACOS device uses PCRE-compatible regular expressions.
Inverse Match	Select the check box to apply an inverse match for the Regex value.
Byte-offset Filter	Enter a byte-offset and a number of bytes to compare. This value is compared to the value at that byte position.
Action	See <a href="#">Action—Choose the appropriate action to be performed on the matching traffic.</a> and <a href="#">Action List—Choose the appropriate action list to be applied on the matching traffic.</a> fields to enter the appropriate information.

4. Click **Submit** to save the configuration.

## UDP

The following topics are covered:

- |  |      |
|--|------|
| <a href="#">Manage a UDP Template</a> .....    | .284 |
| <a href="#">Configure a UDP Template</a> ..... | .285 |

## Manage a UDP Template

---

### Create a UDP Template

To create a new entry, click the green “New UDP Template” button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a UDP Template](#).

### Edit a UDP Template

To edit a previously configured template, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure a UDP Template](#)

### Delete a UDP Template

To delete a configured template, select the checkbox next to the template and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured UDP Templates

The main UDP Template page displays a table of configured UDP templates along with information about them.

Table 102 : Information About Previously Configured UDP Templates

Field	Description
Name	Displays the name of the template.
Session Age (mins)	Displays the length of time, in minutes that a session is active.
Minimum Payload Size	Indicates whether the minimum payload size for a single UDP packet has been configured or not.  Status - Displays whether a Minimum Payload Size is configured.

Table 102 : Information About Previously Configured UDP Templates

Field	Description
	– Configured.  – Not Configured
Maximum Payload Size	Indicated whether the maximum payload size for a single UDP packet has been configured or not. Status - Indicates if Maximum Payload Size is configured. – Configured.  – Not Configured
Spoof Detection	Authenticates UDP clients, by dropping the first UDP request from a given client and waiting for the client to resend the request. Status - Indicates if the spoof detection option is enabled or disabled. – Enabled.  – Disabled Retry Timeout (seconds) - The configured retry timeout
Actions	Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit. Duplicate—Creates an object with basic parameters that are identical to the original object. Used in Zones—Allows you to find all zones associated with the template.

## Configure a UDP Template

Perform the following actions to configure a UDP template:

1. Go to **Configurations >> TPS Zone Templates >> UDP**.
2. Click **+ New UDP Template** and enter the following information:

Table 103 : Field and its purpose for Create UDP Template window.

Field	Purpose
Name	Enter the name of the template.

Table 103 : Field and its purpose for Create UDP Template window.

Field	Purpose
	<p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Session Age	Enter the maximum amount of time a UDP session can remain idle. The default is 2 minutes.
Minimum Payload Size	Enter the minimum payload sized allowed in a single UDP packet.
Maximum Payload Size	Enter the maximum payload sized allowed in a single UDP packet.
Spoof Detection	<p>Select the check box to enable authentication of UDP clients by dropping the first UDP request from a given client and waiting for the client to resend the request.</p> <p>If you select Spoof Detection, following fields are displayed:</p> <ul style="list-style-type: none"> <li>• <b>Retry Timeout</b>—Enter the maximum number of seconds ACOS will wait for a reply.</li> <li>• <b>Minimum Delay</b>—Enter the minimum delay between UDP retransmits for authentication to pass.</li> <li>• <b>Fail Action</b>—Choose the appropriate action from the list when authentication fails.</li> <li>• <b>Fail Action List</b>—Choose the appropriate action list to be applied when authentication fails. If Action List is chosen, the Action List drop-down is displayed.</li> <li>• <b>Pass Action</b>—Choose the appropriate action to be performed when authentication passes.</li> </ul>

Table 103 : Field and its purpose for Create UDP Template window.

Field	Purpose
	<ul style="list-style-type: none"> <li><b>Pass Action List</b>—Choose the appropriate action list to be applied when authentication passes. If Action List is chosen, the Action List drop-down is displayed.</li> </ul>
Token Authentication	Select the check box to enable the token-based authentication.
Token Authentication Formula	Select the token authentication formula from the drop-down list.
Token Authentication Previous Salt Timeout	Specify the token authentication previous salt-prefix timeout in minutes. The default is 1 minute.
Token Authentication Public Address	Select the check box to enable the server public IP address. <ul style="list-style-type: none"> <li>public-ipv4-addr—Specify the server public IPv4 address.</li> <li>public-ipv6-addr—Specify the server public IPv6 address.</li> </ul>
Token Authentication Salt Prefix	Select the check box to enable the token authentication salt prefix. <ul style="list-style-type: none"> <li>Salt Prefix Current—Specify the current token authentication salt prefix.</li> <li>Salt Prefix Previous—Specify the previous token authentication salt prefix.</li> </ul>
NTP Monlist	Select the check box to enable detection and take action against NTP monlist (or MON_GETLIST) messages. See <a href="#">Action—Choose the appropriate action to be performed on the matching traffic.</a> and <a href="#">Action List—Choose the appropriate action list to be applied on the matching traffic.</a> fields to enter the appropriate

Table 103 : Field and its purpose for Create UDP Template window.

Field	Purpose
	information.
Known Response Source Port	See <a href="#">Known Response Source Port</a> field to enter the appropriate information.
Per Connection Packet Rate Limit	See <a href="#">Per Connection Packet Rate Limit</a> field to enter the appropriate information.
Per Connection Rate Interval	Enter the interval for per-connection packet-rate limiting. The interval set by this option only applies to the rate limiting set by the Per Connection Packet Rate Limit. Select one of the following options: <ul style="list-style-type: none"> <li>• 100ms</li> <li>• 1 second</li> </ul>

3. In the **Filter** field, content of UDP payload is filtered and specified action is applied to the matching (on non matching) traffic. The traffic is filtered using regular expressions. Each UDP template can contain up to five filters. For more information to configure the parameters, click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section under [Configure a TCP Template](#).
4. Click **Submit** to save the configuration.

## DNS

The following topics are covered:

<a href="#">Manage a DNS Template</a> .....	289
<a href="#">Configure a DNS Template</a> .....	290

## Manage a DNS Template

### Create a DNS Template

To create a new entry, click the green **New DNS Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a DNS Template](#).

### Edit a DNS Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a DNS Template](#).

### Delete a DNS Template

To delete a configured template, select the checkbox next to the template and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured DNS Templates

The main DNS Template page displays a table of configured DNS templates along with information about them.

Table 104 : Information About Previously Configured DNS Templates

Field	Description
Name	Displays the name of the template.
Any Check	Indicates if Any Check option is enabled.  – Enabled;  – Disabled
Configure options for DNS client authentication	Indicates if Configure options for DNS client authentication option is enabled.  – Enabled;  – Disabled
Actions	Edit—Allows you to edit the template. In order to

Table 104 : Information About Previously Configured DNS Templates

Field	Description
	<p>make changes to a template configuration, click edit.</p> <p>Duplicate—Creates an object with basic parameters that are identical to the original object.</p> <p>Used in Zones—Allows you to find all zones associated with the template.</p>

## Configure a DNS Template

Perform the following actions to configure a UDP template:

1. Go to **Configurations >> TPS Zone Templates >> DNS**.
2. Click **+ New DNS Template** and enter the following information:

Table 105 : Field and its purpose for Create DNS Template window.

Field	Purpose
Name	<p>Enter the name of the template</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated</p>
Any Check	<p>Select the check box to block the DNS “any” requests.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be applied when the DNS Any Requests are blocked.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when the DNS Any Requests are blocked. If Action List is chosen, only then the Action List drop-down is displayed.</li> </ul>
Configure options	Select the check box to enable the DNS authentication

Field	Purpose
for DNS client authentication	<p>test method and actions for the current zone template.</p> <ul style="list-style-type: none"> <li>• <b>Type</b>—Enter the type of DNS authentication used.</li> <li>• <b>Force DNS over TCP</b>—ACOS drops the UDP DNS request from the client, and sends the client a DNS Truncate message.</li> </ul> <hr/> <p><b>NOTE:</b> To enable force DNS over TCP, the mitigation rule must be configured with a DNS TCP port and a DNS UDP port using the same port number. The DNS TCP port must be configured before the DNS UDP port. The DNS template with Force DNS over TCP must be bound to the DNS TCP Port of the mitigation rule.</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Retry</b>—Drops the initial request from the client and waits for the client's retry. If the client does not resend within the specified timeout seconds or the resend is less than the number of seconds specified by the minimum delay, authentication fails.</li> </ul> <p>Enter the appropriate information as described in <a href="#">Fail Action—Choose the appropriate action to be performed when the authentication fails</a> and <a href="#">Configure a TCP Template</a> fields.</p>
Symmetric Session Timeout	Enter the maximum amount of time a DNS session in a Symmetric deployment is allowed to remain idle, before being deleted.
Malform Query Check	<p>Select the check box to enable the scrubbing for malformed queries.</p> <ul style="list-style-type: none"> <li>• <b>Skip Multiple Packet Check</b>— Select the check box to bypasses DNS fragmented and TCP segmented queries. By default, those queries are dropped.</li> <li>• <b>Validation Type</b>—Choose the validation method for</li> </ul>

Field	Purpose
	<p>malformed queries. The supported values are:</p> <ul style="list-style-type: none"> <li>○ <b>Basic Header Check</b>—Checks the QR, OPCODE, and RCODE of the DNS header.</li> <li>○ <b>Extended Header Check</b>—Along with the Basic Header Check, checks the QDCOUNT of the DNS header.</li> <li>○ <b>Disable Malform Query Validation</b>—Bypasses fragmented DNS queries and segmented TCP queries.</li> </ul> <p>See <a href="#">Action—Choose the appropriate action to be performed on the matching traffic.</a> and <a href="#">Action List—Choose the appropriate action list to be applied on the matching traffic.</a> to enter the appropriate information.</p>
FQDN Label Length	<p>Select the check box to limit the rate for DNS requests based on characteristics of the labels in the DNS name.</p> <ul style="list-style-type: none"> <li>● <b>Action</b>—Choose the appropriate action to be performed if the configured length is exceeded.</li> <li>● <b>Action List</b>—Select the appropriate action list to be applied if the configured length is exceeded. If Action List is chosen, only then the Action List drop-down is displayed.</li> <li>● <b>FQDN Label Length</b>—This option is in the table that appears when the FQDN Label option is selected. <ul style="list-style-type: none"> <li>○ <b>Length</b>—Enter the maximum number of characters allowed in an individual label within the DNS name.</li> <li>○ <b>Suffix</b>—Position within the FQDN to begin checking label length. This value specifies how many labels, beginning at the right, to skip before checking the length of individual labels.</li> </ul> </li> </ul>
FQDN Label Count	Select the check box to limit the number of labels that can be asked for in the namespace of a DNS request.

Field	Purpose
	<ul style="list-style-type: none"><li>• <b>Action</b>—Choose the appropriate action to be applied if the configured label count is exceeded.</li><li>• <b>Action List</b>—Choose the appropriate action list to be applied if the configured label count is exceeded. If Action List is chosen, only then the Action List drop-down is displayed.</li><li>• <b>Label Count</b>—Enter the maximum number of namespace labels allowed in a DNS request.</li></ul>
Source Rate Limit	Select the check box to enable the configuration of source rate limits.
NXdomain	Select the check box to enter the maximum number of non-existent domain (NXDomain) replies to client requests within a given DDoS Mitigation interval. <ul style="list-style-type: none"><li>• <b>Rate</b>—Enter the NXdomain rate limit.</li><li>• <b>Action</b>—Choose the appropriate action to be applied for traffic that exceeds the limit.</li><li>• <b>Action List</b>—Choose the appropriate action list to be applied for traffic that exceeds the NXdomain rate limit. If Action List is chosen, only then the Action List drop-down is displayed.</li></ul>
Request	Limits the rate for DNS requests for a specific type of resource record. <ul style="list-style-type: none"><li>• <b>Action</b>—Choose the appropriate action to be applied if the rate limit is reached.</li><li>• <b>Action List</b>—Choose the appropriate action list to be applied when the rate limit is reached. If Action List is chosen, only then the Action List drop-down is displayed.</li><li>• <b>A</b>—Enter the IPv4 address record type limit.</li><li>• <b>AAAA</b>—Enter the IPv6 address record type limit.</li></ul>

Field	Purpose
	<ul style="list-style-type: none"> <li>• <b>CNAME</b>—Enter canonical name record type limit.</li> <li>• <b>MX</b>—Enter the mail exchange record type limit.</li> <li>• <b>NS</b>—Enter the name server record type limit.</li> <li>• <b>SRV</b>—Enter the service locator record type limit.</li> <li>• <b>Other Type</b>—This is a user defined request rate limit.           <ul style="list-style-type: none"> <li>◦ <b>Type</b>—Enter the numbers specifying the record type.</li> <li>◦ <b>Rate</b>—Enter the maximum number of DNS requests allowed per monitoring interval, for the specified record type.</li> </ul> </li> </ul>
Domain Group Name	Select the domain group to associate to the DNS TCP or DNS UDP template.
On-no-match Action	Choose the appropriate action to be performed when Domain Group does not match.
Destination Rate Limit	<p>Select the check box to enable configuration of destination rate limits.</p> <ul style="list-style-type: none"> <li>• <b>Domain Group Rate Exceed Action</b></li> <li>• <b>Encap Template</b></li> <li>• <b>Domain Group Rate Per Service</b></li> </ul>
FQDN	<p>Select the check box to enable the configuration of DNS rate limiting on the basis of FQDN domain-name and suffixes, source IP or both (DST support only).</p> <p>See <a href="#">Action—Choose the appropriate action to be applied if the rate limit is reached.</a> and <a href="#">Action List—Choose the appropriate action list to be applied when the rate limit is reached.</a> If Action List is chosen, only then the <a href="#">Action List drop-down is displayed.</a> fields to enter the appropriate information.</p> <p><b>FQDN Rate</b>—Enter the appropriate details in the following options:</p>

Field	Purpose
	<ul style="list-style-type: none"> <li>• <b>Rate</b>—Enter the FQDN rate limit.</li> <li>• <b>Per</b>—Choose how the DNS Queries are limited.             <ul style="list-style-type: none"> <li>◦ <b>Domain Name</b>—Applies the rate on a per-domain basis. Within a given DDoS Mitigation interval, a given domain name can receive up to the specified number of queries. The queries can be from any source</li> <li>◦ <b>Source IP Address</b>—Applies the rate on a source-IP basis. Within a given DDoS Mitigation interval, a given source IP address can send up to the specified number of queries. The queries can be for any domain name.</li> <li>◦ <b>Both</b>—In this, both Source-IP and domain-name limiting are enabled.</li> <li>◦ <b>FQDN Label Count</b>—Applies the rate on FQDN label count.</li> </ul> </li> <li>• <b>Suffix</b>—Specify how many labels of the FQDN to consider together when applying the rate.</li> <li>• <b>Count</b>—Specify how many labels of the FQDN to consider together when applying the rate.</li> </ul>
Request	See <a href="#">Request</a> field to enter the appropriate information.
Allowed Record Type	Select the check box to enable configuration for allowing certain types of DNS record requests. See <a href="#">Request</a> field to enter the appropriate information.

3. Click **Submit** to save the configuration.

## QUIC

QUIC helps to accelerate HTTP traffic securely and efficiently over UDP with fast connection establishment. QUIC supports multiplexing, which uses multiple

independent streams in the same connection, greatly reducing the amount of connection overhead.

When a QUIC template is configured for a zone, the template checks the version and performs the specified action for the non-matching QUIC version packets.

The following topics are covered:

<a href="#">Manage a QUIC Template</a>	296
<a href="#">Configure an QUIC Template</a>	297

## Manage a QUIC Template

---

### Create an QUIC Template

To create a new entry, click the green **New QUIC Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a QUIC Template](#).

### Edit an QUIC Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a QUIC Template](#).

### Delete an QUIC Template

To delete a configured template, select the checkbox next to the template and click the red Delete button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured QUIC Templates

The main HTTP Template page displays a table of configured HTTP templates along with information about them.

Table 106 : Information About Previously Configured HTTP Templates

Field	Description
Name	The name of the template.
Actions	Allows you to edit, duplicate, or delete the template. In order to make changes to a QUIC Template configuration, click edit. For information on configurable parameters, see <a href="#">Configure an HTTP Template</a> .

## Configure an QUIC Template

To configure a QUIC template:

1. Go to **Configurations >> TPS Zone Templates >> QUIC**.
2. Click **+ New QUIC Template**.
3. In the **Name** box, enter a name for the template.
4. For **Fixed bit malform check disable** option, select the check box to disable the QUIC bit check.
5. Click **+ Add Version** to configure specific version settings.

Field	Purpose
Version start	Enter the starting number of the version. For example, it can be FF000016.
Version end	Enter the ending number of the version. For example, it can be FF000018.
Action	Select the action to be performed based on the version match.
Action List	Choose the appropriate action list to be applied on the version match.  If Action List is chosen, only then the Action List drop-down is displayed.
Malformed Packet check	Select the check box to configure the malformed packet check.
Maximum Source	Enter the maximum source Connection ID (CID)

Field	Purpose
CID Length	length the packet can reach.
Maximum Destination CID Length	Enter the maximum destination Connection ID (CID) length the packet can reach.
Action	Choose the appropriate action to be performed based on the CID length match.
Action List	Choose the appropriate action list to be applied on the CID length match.  If Action List is chosen, only then the Action List drop-down is displayed

---

**NOTE:** Malformed packet check is only supported for version FF000016 - FF000018.

---

6. Click **Submit** to save the configuration.

## HTTP

The following topics are covered:

<a href="#">Manage an HTTP</a> .....	298
<a href="#">Configure an HTTP Template</a> .....	299

## Manage an HTTP

---

### Create an HTTP Template

To create a new entry, click the green **New HTTP Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an HTTP Template](#).

## Edit an HTTP Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure an HTTP Template](#).

## Delete an HTTP Template

To delete a configured template, select the check box next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

## View Previously Configured HTTP Templates

The main HTTP Template page displays a table of configured HTTP templates along with information about them.

Field	Description
Name	Displays the name of the template.
Actions	Allows you to edit or delete the template. In order to make changes to a HTTP Template configuration, click edit. For information on configurable parameters, see <a href="#">Configure an HTTP Template</a> .

## Configure an HTTP Template

---

Perform the following actions to configure a HTTP template:

1. Go to **Configurations >> TPS Zone Templates >> HTTP**.
2. Click **+ New HTTP Template**.
3. In the **Namebox**, enter the name of the template.

If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.

The **Create an HTTP** window consists of following tabs:

- [General](#)
- [Rate Limiting](#)
- [Malformed HTTP](#)
- [Filter](#)

## General

Enter the appropriate information for the following fields:

Field	Purpose
Disallow HTTP CONNECT Method	Select the check box to disallow the HTTP connect method.
Non HTTP Bypass	Select the check box to bypass the non HTTP.
Out of order queue size	Set the number of packets for the out-of-order HTTP queue. This is only applicable in asymmetric mode.
Out of order queue timeout	Set the timeout value in seconds for out-of-order queue in HTTP. This is only applicable in asymmetric mode.
HTTP Authentication	Select the check box to enable the HTTP client authentication <ul style="list-style-type: none"><li>• <b>Challenge Method</b>—This option is configurable once HTTP Authentication is selected. Specifies the method to use for delivering an HTTP authentication challenge to a client. The supported values are:<ul style="list-style-type: none"><li>◦ <b>None</b>—This is a default option which means no authentication.</li><li>◦ <b>Javascript</b>—ACOS generates a Javascript object and sends it to the client. A cookie is included along with the Javascript object. The Javascript object asks the browser to reload the page with the same URL, and sets the cookie. To pass authentication, the client must resend the request along with the cookie within the configured time frame.</li><li>◦ <b>HTTP Redirect</b>—ACOS sends an HTTP redirect message,</li></ul></li></ul>

Field	Purpose
	<p>with the selected status code, to the client. A cookie is included in the redirect message. The redirect URL in the message is the same as the client request. To pass authentication, the client must resend the request along with the cookie to the redirect URL within the configured time frame.</p> <ul style="list-style-type: none"> <li>• <b>HTTP Redirect Code</b>—This option appears once HTTP Redirect is selected as the Challenge Method. Specifies the status code that is sent with the HTTP redirect message to the client. The supported values are 302 Found and 307 Temporary Redirect.</li> <li>• <b>Challenge Cookie Name</b>—This option is configurable once HTTP Authentication is selected. Specifies the name of the cookie used in the HTTP challenges ACOS sends to clients for HTTP authentication.</li> <li>• <b>Challenge Keep Cookie</b>—This option is configurable once HTTP Authentication is selected. Does not remove the HTTP authentication cookie from a client's request before forwarding the request to a content server. ACOS removes the HTTP authentication cookie from a client's resubmitted request before forwarding the request to a content server.</li> <li>• <b>Challenge Interval</b>—This option is configurable once HTTP Authentication is selected. Specifies the maximum number of seconds ACOS waits for a client to reply to an HTTP challenge. The default is 8 seconds.</li> </ul> <p>See <a href="#">Fail Action—Choose the appropriate action to be performed when the authentication fails</a> and <a href="#">Configure a TCP Template</a> fields and enter the appropriate information.</p>
MSS Timeout	Select the check box to configure the maximum number of consecutive packets from a client that can contain less than the specified percentage of the data allowed by the maximum segment size (MSS). During the 3-way handshake, the client and server each specify the MSS (the maximum amount of data

Field	Purpose
	<p>per TCP segment) they allow during the session. This option applies only to the MSS specified by the client.</p> <ul style="list-style-type: none"> <li>• <b>MSS Percent</b>—Enter the minimum percentage of a request packet's data capacity (the MSS) that must contain data.</li> <li>• <b>Number of Packets</b>—Enter the maximum number of packets that can contain less than the specified percentage of data.</li> <li>• <b>Action</b>—Choose the appropriate action to be performed when percentage exceeds the limit.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when percentage exceeds the limit. If Action List is chosen, only then the Action List drop-down is displayed.</li> </ul>
Idle Timeout	<p>Select the check box to configure the maximum number of seconds an HTTP session can remain idle.</p> <ul style="list-style-type: none"> <li>• <b>Ignore Zero Payload</b>—Select the check box if you wish to choose to ignore zero payload length so the idle timer does not reset when a zero payload is received.</li> <li>• <b>Timeout</b>—Enter the maximum number of seconds an HTTP session can remain idle.</li> <li>• <b>Action</b>—Choose the appropriate action to be performed when client traffic exceeds the configured idle timeout.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when the client traffic exceeds the configured idle timeout. If Action List is chosen, only then the Action List drop-down is displayed.</li> </ul>
Request Header Timeout	<p>Select the check box to configure the maximum number of seconds allowed for the TPS device to receive all parts of a given request from a client. If the Thunder TPS device does not receive all parts of the header within the specified time, all parts of the request are dropped.</p> <ul style="list-style-type: none"> <li>• <b>Timeout</b>—Enter the maximum number of seconds allowed to</li> </ul>

Field	Purpose
	<p>receive all parts of a given request.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed when the TPS device does not receive all parts of the header within the configured time.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when the TPS device does not receive all parts of the header within the configured time.</li> </ul> <p>If Action List is chosen, only then the Action List drop-down is displayed.</p>
Slow Read	<p>Select the check box to configure Receive Window enforcement. This is useful for mitigating attack types such as Slow Read.</p> <ul style="list-style-type: none"> <li>• <b>Minimum Window Size</b>—Enter the minimum window size allowed.</li> <li>• <b>Number of packets</b>—Enter the maximum consecutive number of times a client can attempt to advertise a window size smaller than the allowed minimum size.</li> </ul> <p>See <a href="#">Action—Choose the appropriate action to be performed when the TPS device does not receive all parts of the header within the configured time.</a> and <a href="#">Action List—Choose the appropriate action list to be applied when the TPS device does not receive all parts of the header within the configured time.</a> If <a href="#">Action List is chosen, only then the Action List drop-down is displayed.</a> fields and enter the appropriate information.</p>
Client Source IP	<p>Select the check box to mitigate traffic based on the source IP address specified by the HTTP header.</p> <p><b>HTTP Header Name</b>—Specify the HTTP Header Name.</p>

Click **Submit** to save the configuration.

## Rate Limiting

- Source Rate Limit**—Select the check box to configure source rate limits.

Table 110 : Configure Source Rate Limit

Field	Purpose
HTTP Post	<p>Select the check box to configure the maximum of HTTP Post requests allowed.</p> <ul style="list-style-type: none"> <li><b>Rate Limit</b>—Enter the maximum number of HTTP Post requests allowed per DDoS monitoring interval.</li> <li><b>Action</b>—Choose the appropriate action to be performed if the rate limit for HTTP Post requests is exceeded.</li> <li><b>Action List</b>—Choose the appropriate action list to be applied if the rate limit for HTTP Post requests is exceeded. If Action List is chosen, only then the Action List drop-down is displayed.</li> </ul>
HTTP Request	<p>Select the check box to configure the maximum number of HTTP requests allowed per DDoS monitoring interval.</p> <ul style="list-style-type: none"> <li><b>Rate Limit</b>—Enter the maximum number of HTTP requests allowed per DDoS monitoring interval.</li> <li><b>Action</b>—Choose the appropriate action to be performed if the rate limit for HTTP requests is exceeded.</li> <li><b>Action List</b>—Choose the appropriate action list to be applied if the rate limit for HTTP requests is exceeded. If Action List is chosen, only then the Action List drop-down is displayed.</li> </ul>

- Destination Rate Limit**—Select to configure destination rate limits.

Enter the appropriate information for HTTP Post and HTTP Request, as described in

**Response Rate by Size**—Select to configure the rate of HTTP responses from a server (destination) based on the size of the object (payload) within the response.

See [Action—Choose the appropriate action to be performed if the rate limit for HTTP Post requests is exceeded.](#) and [Action List—Choose the appropriate action list to be applied if the rate limit for HTTP Post requests is exceeded.](#) If Action List is chosen, only then the Action List drop-down is displayed. fields to enter the appropriate information.

**Rate Limit**—The supported values are as follows:

Table 111 : Information on Rate Limiting

Column Heading	Description
Type	<p>Choose the rule type for the response rate.</p> <ul style="list-style-type: none"> <li>• <b>Greater</b>—Matches on responses containing objects that are larger than the specified size.</li> <li>• <b>Less</b>—Matches on responses containing objects that are smaller than the specified size.</li> <li>• <b>Between</b>—Matches on responses containing objects that are between two configured sizes.</li> </ul>
Size	Configure the size to apply for the type rule (Greater, Less, Between). When Between is selected for Type, two sizes must be configured.
Rate	Configure the rate to apply for the type rule (Greater, Less, Between).

3. Click **Submit** to save the configuration.

## Malformed HTTP

1. **Malformed Header Checking**—Select the check box to enable the checking of malformed HTTP headers. The ACOS HTTP parser checks the validity of the HTTP request header. Disabled by default.

Field	Purpose
Maximum line length	Enter the maximum number of characters allowed on a single line.
Maximum	Enter the maximum number of headers a requests can

Field	Purpose
number of headers	contain. If a packet contains multiple instances of the same header, each instance is counted separately.
Maximum Request line length	Enter the maximum number of characters allowed on an individual line in the request.
Maximum header name length	Enter the maximum number of characters allowed for a header name. This includes the ":" part of the name.
Maximum content length	Enter the maximum amount of data allowed in a request payload.
Bad Chunk Monitor	Select the check box to enable the scrubbing of invalid chunk formats. The ACOS HTTP parser checks for validly formed chunk data.
Action	Choose the appropriate action to be performed if the rate limit for the configured malformed header checks has been exceeded.
Action List	Choose the appropriate action list to be applied if the rate limit for the configured malformed header checks has been exceeded.  If Action List is chosen, only then the Action List drop-down is displayed.

2. Click **Submit** to save the configuration.

## Filter

Set the HTTP filter configuration. This filters the content of HTTP headers and applies the specified action to matching (on non-matching) traffic. Click the **Plus sign (+)** to add the information.

Table 113 : Information on Filter section

Column Heading	Description
Filter Name	Enter the name of the filter.
Sequence	Enter the sequence number to assign a priority for the

Table 113 : Information on Filter section

Column Heading	Description
Number	configured filter with 1 being the highest priority. Enter the appropriate information in the following filters: <ul style="list-style-type: none"> <li>• HTTP header               <ul style="list-style-type: none"> <li>◦ <b>Regex</b>—Enter the string you want to run the match on. The ACOS device uses PCRE-compatible regular expressions.</li> <li>◦ <b>Inverse Match</b>—Select the check box to apply the inverse match on regex value.</li> </ul> </li> <li>• Referrer, URI, User Agent</li> </ul>
Destination Rate Limit	Set the destination rate limit.
Action	Choose the appropriate action to be performed on the matching (or non-matching) traffic.
Action List	Choose the appropriate action list to be applied on the matching (or non-matching) traffic.  If Action List is chosen, only then the Action List drop-down is displayed.

Click **Submit** to save the configuration.

## SLL-L4

The following topics are covered:

- |  |     |
|--|-----|
| <a href="#">Manage an SLL-L4 Template</a> .....    | 308 |
| <a href="#">Configure an SSL-L4 Template</a> ..... | 309 |

## Manage an SLL-L4 Template

### Create an SSL-L4 Template

To create a new entry, click the green **New SSL-L4 Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an SSL-L4 Template](#).

### Edit an SSL-L4 Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure an SSL-L4 Template](#).

### Delete an SSL-L4 Template

To delete a configured template, select the check box next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured SSL-L4 Templates

The main SSL-L4 Template page displays a table of configured SSL-L4 templates along with information about them.

Column Heading	Description
Name	Displays The name of the template.
Renegotiations	Displays the number of renegotiations.
Actions	<p>Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit.</p> <p>Duplicate—Creates an object with basic parameters that are identical to the original object.</p> <p>Used in Zones—Allows you to find all zones associated with the template.</p>

Column Heading	Description
	For information on configurable parameters, see <a href="#">Configure an SSL-L4 Template</a> .

## Configure an SSL-L4 Template

Perform the following actions to configure a HTTP template:

1. Go to **Configurations >> TPS Zone Templates >> SSL-L4**.
2. Click **+ New SSL-L4 Template**.

Field	Purpose
Name	<p>Enter the name of the template.</p> <p>If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Renegotiation	<p>Select the check box to enable configuration of the maximum number of re-key or renegotiations requests allowed.</p> <ul style="list-style-type: none"> <li>• <b>Number</b>—Enter the maximum number of re-key or renegotiation requests allowed per DDoS Mitigation interval.</li> <li>• <b>Action</b>—Choose the appropriate action to be performed on client traffic that exceeds a policy set by this template.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied on client traffic that exceeds a policy set by this template.</li> </ul> <p>If Action List is chosen, only then the Action List drop-down is displayed.</p>
Allow Non-TLS	Allows Non-TLS traffic (SSLv3 and lower).

Field	Purpose
Source Request Rate Limit	<p>Select the check box to enable configuration of the maximum number of new SSL requests.</p> <p><b>Rate</b>—Enter the maximum number of new SSL requests allowed per DDoS Mitigation interval.</p> <p>See <a href="#">Action—Choose the appropriate action to be performed on client traffic that exceeds a policy set by this template</a>, and <a href="#">Action List—Choose the appropriate action list to be applied on client traffic that exceeds a policy set by this template</a>. If Action List is chosen, only then the Action List drop-down is displayed. fields to enter the appropriate information.</p>
Destination Request Rate Limit	<p>Select the check box to enable configuration of the maximum number of new SSL requests.</p> <p>See <a href="#">Rate—Enter the maximum number of new SSL requests allowed per DDoS Mitigation interval</a>, <a href="#">Action—Choose the appropriate action to be performed on client traffic that exceeds a policy set by this template</a>, and <a href="#">Action List—Choose the appropriate action list to be applied on client traffic that exceeds a policy set by this template</a>. If Action List is chosen, only then the Action List drop-down is displayed. fields to enter the appropriate information.</p>
SSL Traffic Check	<p>Select the check box to enable the SSL header check configuration.</p> <ul style="list-style-type: none"> <li>• <b>Header Inspection</b>—Select the check box to verify the header.</li> <li>• <b>Action</b>—Choose the appropriate action to be performed: <ul style="list-style-type: none"> <li>◦ Drop—Drops packets with bad ssl header.</li> <li>◦ Ignore—Forwards packets with bad ssl header.</li> </ul> </li> <li>• <b>Check Resumed Connection</b>—Select the check box to verify the resumed connections.</li> </ul>
SSL Handshake	Select the check box to enable the SSL handshake policy:

Field	Purpose
Policy	<ul style="list-style-type: none"><li>• <b>Action</b> — Choose the appropriate action to be performed when the SSL handshake policy criteria are not met.</li><li>• <b>Cipher Suits Limit</b>—Select the maximum number of Cipher Suites to be included in Client Hello.</li><li>• <b>Client Extensions Limit</b>—Maximum number of Client Extensions to be included in Client Hello</li><li>• <b>Source Handshaking Connection Limit</b>—Maximum number of connections per Src-IP for which the TLS handshake has not been completed.</li><li>• <b>ClientHello To Appdata Timeout</b>—Maximum wait time from the start of TLS negotiation until the receipt of the first encrypted application data.</li><li>• <b>Finished to Appdata Timeout</b>—Maximum wait time between the completion of TLS negotiation and the receipt of the first encrypted application data</li></ul>

3. Click **Submit** to save the configuration.

## ICMP-v4/v6

The following topics are covered:

- [Manage an ICMP-v4/v6 Template](#) ..... 311  
[Configure an ICMP-v4/v6 Template](#) ..... 313

## Manage an ICMP-v4/v6 Template

### Create an ICMP-v4/v6 Template

To create a new entry, click the green **Create** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an ICMP-v4/v6 Template](#)

## Edit an ICMP-v4/v6 Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure an ICMP-v4/v6 Template](#)

## Delete an ICMP-v4/v6 Template

To delete a configured template, select the checkbox next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

## View Previously Configured ICMP-v4/v6 Templates

The main ICMP-v4/v6 Template page displays a table of configured ICMP-v4/v6 templates along with information about them.

Field	Description
Name	Displays the name of the template.
Type	Displays any types that have been configured.
Actions	<ul style="list-style-type: none"><li><b>Edit</b>—Allows you to edit the template. In order to make changes to a template configuration, click edit.</li><li><b>Duplicate</b>—Creates an object with basic parameters that are identical to the original object.</li><li><b>Used in Zones</b>—Allows you to find all zones associated with the template.</li></ul> <p>For information on configurable parameters, see <a href="#">Configure an ICMP-v4/v6 Template</a>.</p>

## Configure an ICMP-v4/v6 Template

Perform the following actions to configure a **ICMP-v4/v6** template:

1. Go to **Configurations >> TPS Zone Templates >> ICMP-v4 or Configurations >> TPS Zone Templates >> ICMP-v6**.
2. Click **+ New ICMP-v4 Template** or **+ New ICMP-v6 Template** and enter the following information:

Field	Purpose
Name	<p>Enter the Name of the template.</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Type	<p>Use the check box to select existing configured types. Click the <b>Plus sign (+)</b> to add, or the trashcan icon to delete configured ICMPv4/ICMPv6 types.</p> <p><b>Type</b>—Enter the ICMPv4/ICMPv6 type value. (See <a href="http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml">http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml</a>).</p> <p><b>Action</b>—Choose the appropriate action to be performed on configured ICMP type traffic.</p> <p><b>Action List</b>—Choose the appropriate action list to be applied on configured ICMP type traffic.</p> <p>If Action List is selected, only then the Action List drop-down is displayed.</p>
Type Other	<p>Select to check box to configure ICMPv4/ICMPv6 other type values.</p> <p>See <a href="#">Action—Choose the appropriate action to be performed on configured ICMP type traffic</a>, and <a href="#">Action List—Choose the appropriate action list to be applied on configured ICMP type traffic</a>.</p>

Field	Purpose
	<p>fields to enter the appropriate information.</p> <ul style="list-style-type: none"> <li>• <b>Source Rate</b>—Apply the source rate limit for ICMP traffic of the specified type per DDoS Mitigation interval.           <ul style="list-style-type: none"> <li>◦ <b>Source Rate Exceed Action</b>—Choose the appropriate action to be performed for exceeding source rate.</li> <li>◦ <b>Source Rate Exceed Action List</b>—Choose the appropriate action list to be applied for exceeding source rate. If Action List is selected, only then the Source Rate Exceed Action List drop-down is displayed.</li> </ul> </li> <li>• <b>Destination Rate</b>—Apply the destination rate limit for ICMP traffic of the specified type per DDoS Mitigation interval.           <ul style="list-style-type: none"> <li>◦ <b>Destination Rate Exceed Action</b>—Choose the appropriate action to be performed on exceeding destination rate.</li> <li>◦ <b>Destination Rate Exceed Action List</b>—Choose the appropriate action list to be applied for exceeding destination rate. If Action List is selected, only then the Destination Rate Exceed Action List drop-down is displayed.</li> </ul> </li> </ul>

3. **Filter** option, filters the content of ICMPv4/ICMPv6 payloads and applies the specified action to matching (on non matching) traffic. The traffic is filtered using regular expressions. Each ICMPv4/ICMPv6 template can contain up to five filters. For more information to configure the parameters, click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section under [Configure a TCP Template](#).
4. Click **Submit** to save the configuration.

## IP Proto

The following topics are covered:

[Manage an IP Proto Template](#) ..... 315

[Configure an IP Proto Template](#) ..... 316

## Manage an IP Proto Template

---

### Create an IP Proto Template

To create a new template, click the green **New IP Proto Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an IP Proto Template](#).

### Edit an IP Proto Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Delete an IP Proto Template

To delete a configured template, select the check box next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured IP Proto Templates

The main IP Proto Template page displays a table of configured IP Proto templates along with information about them.

Table 118 : Information About Previously Configured IP Proto Templates

Field	Description
Name	Displays the name of the template.

Table 118 : Information About Previously Configured IP Proto Templates

Field	Description
Actions	<ul style="list-style-type: none"> <li><b>Edit</b>—Allows you to edit the template. In order to make changes to a template configuration, click edit.</li> <li><b>Duplicate</b>—Creates an object with basic parameters that are identical to the original object.</li> <li><b>Used in Zones</b>—Allows you to find all zones associated with the template.</li> </ul>

## Configure an IP Proto Template

Perform the following actions to configure a TCP template:

1. Go to **Configurations >> TPS Zone Templates >> IP Proto**.
2. Click **+ New IP ProtoTemplate**.
3. In the **Name** box, enter a name for the template.

**NOTE:** If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.

4. **Filter** option, filters the content of IP Proto payloads and applies the specified action to matching (on non matching) traffic. The traffic is filtered using regular expressions. Configure the following parameters and click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section and under [Configure a TCP Template](#).
5. Click **Submit** to save the configuration.

# Encapsulation

The following topics are covered:

- |   |     |
|---|-----|
| <a href="#">Manage an Encapsulation Template</a> .....    | 317 |
| <a href="#">Configure an Encapsulation Template</a> ..... | 318 |

## Manage an Encapsulation Template

---

### Create an Encapsulation Template

To create a new template, click the green **New Encapsulation Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an Encapsulation Template](#).

### Edit an Encapsulation Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Delete an Encapsulation Template

To delete a configured template, select the checkbox next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured Encapsulation Templates

The main Encapsulation Template page displays a table of configured Encapsulation templates along with information about them.

Table 119 : Information About Previously Configured Encapsulation Templates

Field	Description
Name	Displays the name of the template.
Actions	<p>Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit.</p> <p>Duplicate—Creates an object with basic parameters that are identical to the original object.</p> <p>Used in Zones—Allows you to find all zones associated with the template.</p>

## Configure an Encapsulation Template

Perform the following actions to configure a TCP template:

1. Go to **Configurations >> TPS Zone Templates >> Encapsulation**.
2. Click **+ New Encapsulation Template** and enter the following information:

Field	Purpose
Name	<p>Enter the Name of the template.</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Tunnel Encapsulation	<p>Select option to Encapsulate all client-server traffic into a Generic Routing Encapsulation (GRE) tunnel or IP-in-IP tunnel, and send the traffic to the device at the remote end of the tunnel. The supported values are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• IP-IP</li> </ul>

Field	Purpose
	<ul style="list-style-type: none"><li>◦ IP Address—Configure the IPv4 or IPv6 Address.</li><li>• GRE</li><li>◦ IP Address—Configure the IPv4 or IPv6 Address.</li></ul>
Preserve Source IP	Select the check box to preserve the source IP.

3. Click **Submit** to save the configuration.

## SIP

The following topics are covered:

<a href="#">Manage an SIP Template</a> .....	319
<a href="#">Configure an SIP Template</a> .....	320

## Manage an SIP Template

### Create an SIP Template

To create a new template, click the green **New SIP Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure an SIP Template](#).

### Edit an SIP Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure an SIP Template](#).

### Delete an SIP Template

To delete a configured template, select the checkbox next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in

the Actions column for that template.

## View Previously Configured SIP Templates

The main SIP Template page displays a table of configured SIP templates along with information about them.

Table 120 : Information About Previously Configured SIP Templates

Field	Description
Name	Displays the name of the template.
Actions	<p>Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit.</p> <p>Duplicate—Creates an object with basic parameters that are identical to the original object.</p> <p>Used in Zones—Allows you to find all zones associated with the template.</p>

## Configure an SIP Template

Perform the following actions to configure a TCP template:

1. Go to **Configurations >> TPS Zone Templates >> SIP**.
2. Click **+ New SIP Template** and enter the following information:

Table 121 : Field and its purpose for Create SIP Template window

Field	Purpose
Name	<p>Enter the Name of the template.</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>

Table 121 : Field and its purpose for Create SIP Template window

Field	Purpose
Destination Rate Limit	<p>Configure the destination rate limit for the SIP template.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed when destination rate exceeds the limit.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when destination rate exceeds the limit. If Action List is selected, only then the Action List dropdown is displayed.</li> <li>• <b>Rate Limit</b> <ul style="list-style-type: none"> <li>◦ <b>Method</b>—Choose the appropriate option to configure the destination rate method. &lt;need more info on each method&gt;</li> <li>◦ <b>SIP Rate</b>—Configure the SIP rate for the method option.</li> </ul> </li> </ul>
Source Rate Limit	<p>Configure the source rate limit for the SIP template.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed when source rate exceeds the limit.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied when source rate exceeds the limit. If Action List is selected, only then the Action List dropdown is displayed. See <a href="#">Rate Limit</a><b>Method</b>—Choose the appropriate option to configure the destination rate method. &lt;need more info on each method&gt;<a href="#">SIP Rate</a>—Configure the SIP rate for the method option. to enter the appropriate information.</li> </ul>
Idle Timeout	<p>Configure the action to be taken under an idle-timeout.</p> <ul style="list-style-type: none"> <li>• <b>Action</b>—Choose the appropriate action to be performed after the idle timeout.</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied after the idle timeout. If Action List is selected, only then the Action List drop-</li> </ul>

Table 121 : Field and its purpose for Create SIP Template window

Field	Purpose
	<p>down is displayed.</p> <ul style="list-style-type: none"> <li>• Timeout— &lt;need info&gt;</li> </ul> <p>Ignore Zero Payload option configures ACOS to continue decrementing the idle timer if a SIP packet is received for the session but the packet has no data (has a zero-length payload). By default, SIP packets for the session reset the idle timer even if they have no payload. The configurable range is (1 - 63). &lt;can't find this in GUI&gt;</p>
Malformed SIP	<p>Configures basic sanity checks for SIP packets.</p> <ul style="list-style-type: none"> <li>• <b>Maximum Call-ID Length num</b>—Enter the maximum call-id length. The default value is 32511 bytes.</li> <li>• <b>Maximum Header Name Length</b>—Enter the maximum length allowed for the header name in an HTTP request. This max value does not include heading and trailing whitespace, nor the ":" sign at the end. The maximum length allowed for the header name is 63 characters.</li> <li>• <b>Maximum Header Value Length</b>—Enter the maximum header value length. The default value is 32511.</li> <li>• <b>Maximum Line Length</b>—Enter a limit for the maximum length per line, including the \r\n at the end of each line. The default value is 32511.</li> <li>• <b>Maximum URI Length</b>—Enter a limit for the maximum URI length. The default value is 32511.</li> <li>• <b>Maximum SDP Length</b>—Enter the maximum content length, if content type is <b>application/sdp</b>. The default value is 32511 bytes.</li> <li>• <b>Malform SIP Action</b>—Choose the appropriate action to be performed for malformed SIP checks</li> <li>• <b>Action List</b>—Choose the appropriate action list to be applied for malformed SIP checks If Action List is selected, only then the Action List drop-</li> </ul>

Table 121 : Field and its purpose for Create SIP Template window

Field	Purpose
	down is displayed.

3. **Filter** option, filters the content of SIP payloads and applies the specified action to matching (on non matching) traffic. The traffic is filtered using regular expressions. Each SIP template can contain up to five filters. For more information to configure the parameters, click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section under [Configure a TCP Template](#).
4. Click **Submit** to save the configuration.

## Source Port TCP Template

The following topics are covered:

<a href="#">Manage a Source Port TCP Template</a> .....	323
<a href="#">Configure a Source Port TCP Template</a> .....	324

## Manage a Source Port TCP Template

### Create a Source Port TCP Template

To create a new entry, click the green “New Src Port TCP Template” button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a Source Port TCP Template](#).

### Edit a Source Port TCP Template

To edit a previously configured template, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure a Source Port TCP Template](#)

## Delete a Source Port TCP Template

To delete a configured template, select the checkbox next to the template and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that template.

## View Previously Configured Source Port TCP Templates

The main Src Port TCP Template page displays a table of configured Source Port TCP templates along with information about them.

Table 122 : Information About Previously Configured Source Port TCP Templates

Field	Description
Name	The name of the template.
Actions	<ul style="list-style-type: none"><li><b>Edit</b>—Allows you to edit the template. In order to make changes to a template configuration, click edit.</li><li><b>Duplicate</b>—Creates an object with basic parameters that are identical to the original object.</li><li><b>Used in Zones</b>—Allows you to find all zones associated with the template.</li></ul>

## Configure a Source Port TCP Template

Perform the following actions to configure a TCP template:

1. Go to **Configurations >> TPS Zone Templates >> Src Port TCP**.
2. Click **+ New Src Port TCP Template**
3. In the **name** field, enter the name of the template.

---

**NOTE:** If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.

---

4. In the **Filter** field, content of TCP payload is filtered and the specified action is applied to the matching (on non matching) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. For more information to configure the parameters, click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section under [Configure a TCP Template](#).
5. Click **Submit** to save the configuration.

## Source Port UDP Template

---

The following topics are covered:

<a href="#">Manage a Source Port UDP Template</a> .....	325
<a href="#">Configure a Source Port UDP Template</a> .....	327

## Manage a Source Port UDP Template

---

### Create a Source Port UDP Template

To create a new entry, click the green **New Source Port UDP Template** button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a Source Port UDP Template](#).

### Edit a Source Port UDP Template

To edit a previously configured template, click **Edit** in the Actions column for that template.

For a description of the configurable parameters, see [Configure a UDP Template](#)

## Delete a Source Port UDP Template

To delete a configured template, select the check box next to the template and click the red **Delete** button at the top right corner of this page, or click the delete icon in the Actions column for that template.

## View Previously Configured Source Port UDP Templates

The main Source Port UDP Template page displays a table of configured UDP templates along with information about them.

Table 123 : Information About Previously Configured Source Port UDP Templates

Field	Description
Name	The name of the template.
Minimum Payload Size	Shows whether the minimum payload size for a single source port UDP packet has been configured or not. Status - Indicates if Minimum Payload Size is configured.  – Configured.  – Not Configured
Maximum Payload Size	Shows whether the maximum payload size for a single source port UDP packet has been configured or not. Status - Indicates if Maximum Payload Size is configured.  – Configured.  – Not Configured
NTP Monolist	Shows the message for the action taken for a single source port UDP packet.
Actions	<ul style="list-style-type: none"><li><b>Edit</b>—Allows you to edit the template. In order to make changes to a template configuration, click edit.</li><li><b>Duplicate</b>—Creates an object with basic parameters that are identical to the original object.</li><li><b>Used in Zones</b>—Allows you to find all zones associated with the template.</li></ul>

## Configure a Source Port UDP Template

Perform the following actions to configure a UDP template:

1. Go to **Configurations >> TPS Zone Templates >> Src Port UDP**.
2. Click **+ New Src Port UDP Template** and enter the following information:

Field	Purpose
Name	<p>Enter the name of the template.</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Minimum Payload Size	Enter the minimum payload sized allowed in a single source port UDP packet.
Maximum Payload Size	Enter the maximum payload sized allowed in a single source port UDP packet.
NTP Monlist	<p>Select to enable detection and take action against NTP monlist (or MON_GETLIST) messages.</p> <ul style="list-style-type: none"><li>• Action—Choose the appropriate action to be performed on the matching traffic.</li><li>• Action List—Choose the appropriate action to be applied on the matching traffic.</li></ul> <p>If Action List is chosen, the Action List drop-down is displayed.</p>

3. In the Filter field, content of UDP payload is filtered and specified action is applied to the matching (on non matching) traffic. The traffic is filtered using regular expressions. Each source port UDP template can contain up to five filters. For more information to configure the parameters, click **Add** and see [In the Filter field, content of TCP payload is filtered and specified action is applied to the matching \(on non-matching\) traffic. The traffic is filtered using regular](#)

[expressions. Each TCP template can contain up to five filters. Configure the following parameters and click Add to include:](#) section under [Configure a TCP Template.](#)

2. Click **Submit** to save the configuration.

# TPS DST Entry Templates

---

Under TPS DST Entry Templates, you can create TCP, UDP, Other, HTTP, DNS, ICMPv4, ICMPv6, and SSL-L4 objects and manage them using SecDevice.

To create DST Entry Templates, go to **Configurations >> TPS Dst Entry Templates**.

The following buttons appear across the upper-right side of the TPS <*Protocol Template*>table:

Table 125 : Action Buttons

Options	Description
Reset	Resets the search filter for the template.
Refresh	Refreshes the information displayed for the Templates.
Delete	Select the check box at left for one or more Templates, then click Delete.
Find Default	Search for the template that is set as the SecDevice default template.
New <Protocol> Template	Click this button to create a new <Protocol> Templates.

## TPS Other Objects

---

Under TPS Dst Entry Templates you can create GLID, Action List, Logging Template, Violation Actions and Scripts and manage them using SecDevice.

## GLID

To create a new entry, click the green “New GLID” button at the top right corner of this page.

### Create a new GLID template

To create a new GLID template:

Select **Configurations >> TPS Other Objects >> GLID**.

Select the GLID tab if not already selected, then click the **New GLID** button at the upper right.

### Edit a GLID

To edit a previously configured template, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure GLID](#).

### Delete a GLID

To delete a configured template, select the checkbox next to the template and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured GLIDs

The main GLID page displays a table of configured GLIDs along with information about them.

Table 126 : Information About Previously Configured GLIDs

Field	Description
Name	Indicates the name of the GLID.
Concurrent Connections	Indicates the configured maximum number of concurrent connections.

Table 126 : Information About Previously Configured GLIDs

Field	Description
New Connections	Indicates the configured maximum number of new connections allowed per interval.
Kibit Rate	Indicates the configured maximum number of Kibits allowed within a DDoS Mitigation interval.
Packet Rate	Indicates the configured maximum number of packets allowed per interval.
Fragmented Packet Rate	Indicates the configured maximum number of fragmented packets allowed per interval.
SYN Cookie Failures	Indicates the configured maximum number SYN-cookie failures allowed per interval.
Over Limit Action	Indicates the configured action taken when traffic exceeds one or more of the configured limits.
Actions	Allows you to edit or delete the template/ In order to make changes to a GLID configuration, click edit. For information on configurable parameters, see <a href="#">Configure GLID</a> .

## Configure GLID

Perform the following steps to configure GLID:

Fields	Purpose
<b>Name</b>	Enter the Name of the GLID. The supported value is a string of 1-26 characters.  If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.
<b>Description</b>	Enter a description of the GLID parameters. The supported value is a string of 1-63 characters.
<b>Concurrent Connections</b>	Specifies the maximum number of concurrent connections. The supported value is 1-16000000.

Fields	Purpose
<b>New Connections</b>	Specifies the maximum number of new connections allowed per interval. The supported value is 1-16000000.
<b>Kibit Rate</b>	<p>Specifies the maximum number of Kibits allowed within a DDoS Mitigation interval. The GLID action for overlimit traffic is applied to bits received after the limit is reached. There are no default bandwidth rate limits. To set a bandwidth limit, you must configure the limit in a GLID and apply (bind) the GLID to a DDoS Mitigation rule. Separate bandwidth limits are configurable for each Layer 4 type (TCP, UDP, ICMP, and Other). The supported value is 1-16000000.</p> <p><b>NOTE:</b> If a GLID bound to a DDoS Mitigation rule does not specify a packet rate limit or a bandwidth rate limit, the rate for the matching traffic is unlimited.</p>
	<p><b>NOTE:</b> If there is no GLID bound to a rule, ACOS applies the applicable packet rate limit to the matching traffic.</p>
<b>Packet Rate</b>	Specifies the maximum number of packets allowed per interval. The supported value is 1-16000000.
<b>Fragmented Packet Rate</b>	Specifies the maximum number of fragmented packets allowed per interval. The supported value is 1-16000000.
<b>SYN Cookie Failures</b>	Specifies the maximum number of pSYN-cookie failures allowed per interval. A SYN-cookie failure occurs when the sequence number in a TCP ACK from a client does not pass the SYN-cookie check. The supported value is 1-16.
<b>Over Limit Action</b>	Enables the action taken when traffic exceeds one or more of the limits.
<b>Action Type</b>	<p>Specifies the action taken when traffic exceeds one or more of the limits. The supported values are:</p> <ul style="list-style-type: none"> <li>• Drop (default)</li> <li>• Blacklist Source Entry</li> <li>• Send Flowspec</li> </ul>

Fields	Purpose
	<p><b>NOTE:</b> With Send Flowspec, when this GLID is configured on a zone or zone-service or src-port, upon violation, Flowspec rules will automatically get created for all the zone IPs.</p>
<b>Blacklist Timeout</b>	<p>Specifies the amount of time the source entry is Blacklisted for. The supported value is 1-16 minute.</p> <p><b>NOTE:</b> This option appears when Blacklist Source Entry is selected as the Action Type.</p>
<b>Traffic Filtering Action</b>	<p>Choose one of the following options that must be applied if the traffic matches the configuration:</p> <ul style="list-style-type: none"> <li>• <b>Deny</b>—The router denies or blocks the traffic.</li> <li>• <b>Rate</b>—The router can apply the rate limiter, in bytes per second, to apply to the traffic.</li> </ul>
<b>Traffic Rate</b>	<p>Specify the maximum number of traffic rate limit.</p>
<b>Flowspec Timeout</b>	<p>Specify the time duration (in minutes) for Flowspec to timeout.</p>

## Action Lists

Action lists are reusable objects that group together multiple actions to be taken on given DDoS violations. These can be applied to any zone template as the authentication pass or fail actions, or actions to be taken when configured thresholds or rate limits are exceeded.

The action list can be applied to the following zone templates—TCP, UDP, DNS, HTTP, QUIC, SLL-L4, ICMP-v4/v6, IP Proto, SIP, Source Port TCP, and Source Port UDP.

You can associate a logging template and an encapsulation template while creating the action list or after creating the action list.

To associate an action list to the zone templates, see the configuration for the respective zone template.

To configure an action list:

1. Go to Configurations >> TPS Other Objects >> Action List.
2. On the top right, click +New Action List. The Action List window is displayed.

Figure 41 : Create an Action List



3. Enter the name of the action list.
4. From the Action drop-down list, select one of the following options:
  - Drop—Drops the packets
  - Ignore—Continues processing the packets
  - Reset—Resets the client's connection
  - Black-list src—Adds source IP immediately to the blacklist table.
  - The Blacklist Duration box is displayed.
  - Blacklist Duration—Determines how quickly the Black List entry can age out.
  - Authenticate-src—Authenticates the source IP.
  - Tunnel-encap-packet—Enables the packets to be encapsulated for tunneling. The Stateless check box is displayed.
  - Stateless—Enables all packets to be encapsulated for tunneling. Once the Stateless check box is selected, the Scrub Packet check box is displayed.
  - Scrub Packet—Allows the scrubbing of packets by additional DDoS mitigation configuration before being sent out.

If no action is selected, the drop action is selected by default.

5. From the Logging Templates drop-down list, select the logging template you want to associate to the action list.
6. From the Encapsulation Template drop-down list, select the encapsulation template you want to associate to the action list.
7. Click OK.

## Logging Template

### Create a Logging Template

To create a new template, click the green “New Logging Template” button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a Logging Template](#).

### Edit a Logging Template

To edit a previously configured template, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

### Delete a Logging Template

To delete a configured template, select the checkbox next to the template and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that template.

### View Previously Configured Logging Templates

The main Logging Template page displays a table of configured Logging templates along with information about them.

Table 127 : nformation About Previously Configured Logging Templates

Field	Description
Name	The name of the template.
Logging	Indicates if Logging format: CEF option is enabled.

Table 127 : nformation About Previously Configured Logging Templates

Field	Description
format: CEF	– Enabled;  – Disabled.
Use Object Name	Indicates if the Use Object Name option is enabled. – Enabled;  – Disabled.
Enable Action Logging	Indicates if the Enable Action Logging option is enabled. – Enabled;  – Disabled.
Logging Format Custom	Indicates if the Logging Format Custom option is enabled. – Enabled;  – Disabled.
Actions	Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit. Duplicate—Creates an object with basic parameters that are identical to the original object. Used in Zones—Allows you to find all zones associated with the template.

## Configure a Logging Template

To configure a logging template:

1. Navigate to **Configurations >> TPS Other Objects >> Logging Template**.
2. Click **+ New Logging Template**.
3. In the **Name** box, enter the Name of the template. The supported value is a string of 1-63 characters.

---

**NOTE:** If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.

---

4. **Logging Format: CEF**—Select to enable DDoS event messages in Common Event Format (CEF), which uses a set of named fields.
5. **Use Object Name**—Select to enable display of rule/entry names of sources and destination in logs instead of their IP addresses.

---

**NOTE:** The source and destination IP addresses are always shown in the Flow field of the message, whether display of the rule/entry names is enabled or disabled.

---

6. **Enable Action Logging**—Select to enable logging actions for policy breaches.
7. **Customize Log Format**—Select to configure your own logging format. This allows you to specify which fields you want displayed, and the order in which they appear. In the Log Format box, enter your custom log string. The following shows the syntax of a custom log format string. The order of the fields shown can be changed depending on how you want your specific log messages to be displayed. The supported value is 1-512 characters.

"Event \$event-msg\$; Protected Host \$entry-info\$; L4 info \$entry-port-num\$ \$entry-port-type\$; Event timestamp: \$event-timestamp\$; Configured limit \$config-limit\$"

## Violation Actions

### Create a Violation Action

To create a new violation action, click the green “New Violation Actions” button at the top right corner of this page.

For a description of the configurable parameters, see [Configure a Violation Action](#).

### Edit a Violation Action

To edit a previously configured violation action, click “Edit” in the Actions column for that template.

For a description of the configurable parameters, see [Configure a TCP Template](#).

## Delete a Violation Action

To delete a configured violation action, select the checkbox next to the violation action and click the red “Delete” button at the top right corner of this page, or click the delete icon in the Actions column for that item.

## View Previously Configured Violation Action

The main Violation Action page displays a table of configured Violation Actions along with information about them.

Table 128 : Information About Previously Configured Violation Actions

Field	Description
Name	Displays the name of the violation action.
Blackhole	Displays the configured BGP Blackhole duration time.
Blacklist Source	Displays the configured blacklist duration time.
Actions	Edit—Allows you to edit the template. In order to make changes to a template configuration, click edit.  Duplicate—Creates an object with basic parameters that are identical to the original object.  Used in Zones—Allows you to find all zones associated with the template.

## Configure a Violation Action

---

Perform the following steps to configure a violation action:

- Enter the appropriate information in the fields.

Table 129 : Configure Violation Actions

Field	Purpose
Name	<p>Enter the name of the violation action.</p> <p><b>NOTE:</b> If you are trying to recreate a deleted template that was previously associated to a few zones, an Associated Zones link appears next to the Name field. This Associated Zones link displays the zones with which the template was previously associated.</p>
Blacklist Source Duration	Enter the amount of time to blacklist traffic's source IP in minutes.
Script	<p>Choose a script file.</p> <p>To create a new script file, see <a href="#">Scripts</a>.</p>
BGP Blackhole Duration	Enter the amount of time to block the traffic to the zone in minutes.

- Click **Submit** to create the action.

## Scripts

The Scripts page allows you to create an executable script.

Table 130 : Description of columns in Scripts page

Button	Description
Name	Name of the scripts file.
Last Modified Time	Shows the date and time when the file was last modified.
Actions	<b>Edit</b> —Allows you to edit the content of the selected configuration file.

Table 130 : Description of columns in Scripts page

Button	Description
	<b>Push</b> —Allows you to push the configuration to a managed device or device group. <b>Download</b> —Allows you to download the class-list as a file.

Perform the following to create or edit a script:

1. Select **Configurations >> TPS Other Objects >> Scripts**.
2. (Optional) From the Scripts page, you can further edit portions of the config file by clicking the **Edit** link under the Actions column.
3. When you are finished modifying the portion of the configuration backup file, you can push that portion of the config to another device by clicking the **Push** link, which appears in the right-most Actions column.
4. Select one or more devices to choose where the scripts will get pushed.
5. Select one or more device groups from the Device Groups section of the page to choose the group(s) to push the scripts.
6. Click the Partitions drop-down menu and select Shared or the name of the private partition. This selection will determine where on the target device (i.e. which partition) the configuration snippet will be pushed. Keep in mind that the configuration snippet will be pushed to this same partition across all of the selected target devices (if multiple devices are selected).
7. Configure the Schedule Type by selecting Immediate, if not already selected.
8. Configure the Interval, and any other mandatory options in the Push Configuration window.  
For more information about these options, see [Config Backups](#).
9. When finished configuring the Push Device Configuration window, click **Submit**.

## Creating a Configuration

Take the following steps based on the configuration you wish to create:

1. Enter the name in the **Name** field.
2. Under Content, enter the script.

3. Click **Submit**.

# Administration

---

The following topics are covered:

<a href="#"><u>Scheduler</u></a> .....	344
<a href="#"><u>Job Execution Results</u></a> .....	346
<a href="#"><u>Settings</u></a> .....	347
<a href="#"><u>User Management</u></a> .....	365
<a href="#"><u>Maintenance</u></a> .....	375

## Scheduler

The Scheduler page displays a list of all of the jobs that SecDevice has scheduled for its managed devices. For example, if you configured SecDevice to create a backup configuration for a particular ACOS device at a future time, then the task will appear in the schedule list.

From the Scheduler page, you can perform the following tasks:

- Viewing scheduled tasks – For example, you can view details associated with scheduled tasks, such as the name of the task, when it is scheduled to run, and when the job was first created. In addition to displaying future tasks, the Schedule page also includes past tasks that have already been triggered.
- Scheduling a task to be added to the scheduler – The Scheduler page appears anytime you begin a workflow to perform a task (such as creating a device configuration backup or performing a device upgrade) at a future time.

### Viewing scheduled tasks

To access the Scheduler page and view the tasks that have been scheduled, navigate as follows:

1. Select **Administration >> Scheduler**.

---

**NOTE:** This page just displays jobs you already scheduled elsewhere in the GUI, and you cannot initiate the process of scheduling a job or task from this window.

---

2. (Optional) To remove a yet-to-be-fired job from the schedule, select the check box next to the job and then click the **Unschedule** button at the upper right corner of the page.

describes the column headings in the Scheduler list:

Table 131 : Column Headings in the Scheduler List

Column Heading	Description
Status	Indicates status of a scheduled job.
Name	Name of the scheduled task.
Created Time	Indicates the date and time when the scheduled task was originally created.
Executor	Process that scheduled the job.
Description	Optional user-configured description of scheduled job.
Details	Clicking and hovering over the View link will give you more details on about the job, including the managed device ID and IP address.
Scheduled	Indicates the date and time when the task had been scheduled to be fired.
Start Time	Indicates that the task has been scheduled to run at future time, but has not been fired.
Next Run Time	Indicates the time and date that this task will run in the future.

## Scheduling a Task <can't find>

1. Navigate to the relevant link for the task you would like to schedule, such as [Creating a Backup Configuration File for a Managed Device](#) or [Web](#).
2. Configure the following options:
  - Schedule Type - Schedules a backup job to be taken immediately or at a later scheduled time and date.
    - Immediate - Schedules a backup job to be taken immediately.
    - Schedule - Schedules a backup job to be run in the future. The parameters for a Schedule type of back up will be displayed.

- Start Datetime - The starting date/time of the job.
- Schedule Option - One Time, Every 6 Hours, Every 12 Hours, Daily, Weekly, Bi-weekly, or Monthly.
- Description - A free-form textual description for the job.
- Remote - If checked, allows user to specify an external destination for the backup job. Note that if this option is used, configuration backups will not be shown in SecDevice's Device Configuration Backup listing.

## Job Execution Results

The Job Execution Results page displays a listing of the job executions and their results.

A job is simply a common task performed by the SecDevice device for one of its managed devices, such as creating a backup config file. The Job Execution Results page displays information about the status of that task, as well as whether it has completed, and whether or not it was successful.

---

**NOTE:** A job can be composed of multiple results. For example, if SecDevice is scheduled to perform a device backup job that includes two or more devices, the backup operation could succeed for one device while failing for the other.

---

To access the Job Execution Results page, go to **Administration >> Job Execution Results** from the main menu.

Table 132 : Column Headings in the Job Execution Result list

Column heading	Description
Name	Name of the scheduled job.
Created Time	Indicates the date and time when the job was originally created.
Trigger Time	Indicates the date and time when the job is scheduled to actually occur.
Results Summary	This column lists the total number of jobs scheduled in that selected log, and divides those jobs into Successes, Failures,

Table 132 : Column Headings in the Job Execution Result list

Column heading	Description
	Exceptions, and Pending executions.
Description	Free form text field that describes the job.
Task Executor	Specifies the page there the job was configured.

Click the **Plus sign (+)** icon next to a Name of the job to expand it and show the following additional fields.

Column Heading	Description
Data	Lists the administrator who set up the job, host IP, and encrypted password.
Finish Time	Indicates the date and time when the job was finished.
Result Status	Indicates the status of the job. A job result can be in one of the following states: <ul style="list-style-type: none"> <li>Job has started, but the results have not yet been recorded because the job has just started and is in progress.</li> <li>Job has completed, with successful results (Result Status = 1).</li> <li>Job has completed, with error results (Result Status = 2).</li> </ul>
Result Data	Provides the summary result. If additional information is available, a “+” icon appears, which can be selected to get detail on the result.

## Settings

The following topics are covered:

<a href="#">Network</a> .....	348
<a href="#">Access Management</a> .....	349
<a href="#">Route</a> .....	350
<a href="#">Clock</a> .....	351

<a href="#"><u>Licensing</u></a>	352
<a href="#"><u>SNMP</u></a>	353
<a href="#"><u>Notification</u></a>	356
<a href="#"><u>External Logging</u></a>	359
<a href="#"><u>TPS</u></a>	361
<a href="#"><u>Call Home SERT</u></a>	362
<a href="#"><u>Web Certificate</u></a>	364
<a href="#"><u>Geo Location</u></a>	364

## Network

---

The Network page allows you to configure the hostname, IP address, application type, and network settings for the SecDevice device.

To access the Network page, navigate as follows:

1. Select **Administration >> Settings** from the main menu and click on Network. From here, you can make the following configurations:
  - Hostname – name of this SecDevice device
  - IPv4 Default Gateway – IPv4 gateway this SecDevice device will use to access the network
  - IPv6 Default Gateway – IPv6 gateway this SecDevice device will use to access the network
2. In the eth0 bar, click the (>) symbol to expand that section, perform the following configurations:
  - DHCP – select this check box to allow DHCP to configure basic network settings. When DHCP is used, the IP field will be grayed-out.
  - If not using DHCP, enter values for the following fields:
    - IP
    - Netmask

- Broadcast
- DNS
- Auto – select this check box to allow IPv6 to auto-configure basic network settings. When Auto is selected, the IPv6 field will be grayed-out.
- IPv6
- Netmask

3. Click Submit to save your configurations.

---

**NOTE:** Typically, SecDevice uses its management IP on eth0 which is used as the sFlow collector IP seen on the TPS device. This is now configurable beyond eth0 with options for eth1 through eth8.

---

## Access Management

---

SecDevice allows an administrator to drop or allow the management traffic destined to SecDevice's interfaces.

By default, the policy for SSH, SNMP, and HTTP/HTTPs is ACCEPT. You can help secure the interfaces by configuring a DROP target from a specific source IP or subnet

SecDevice allows you to parse the syslog messages that are coming from Arbor SP, infer if an IP address is under attack, and trigger DDoS mitigation on Thunder TPS accordingly.

The workflow for Arbor to inter-operate with SecDevice is as follows:

- Configure zones with IPs or subnets that must be protected.
- Configure Arbor SP to send the Syslog to SecDevice IP.
- Add the IP address of Arbor appliance by navigating to **Administration >> Settings >> Access Management** to allow SecDevice to receive the Syslog.

When syslog containing host attack alert is received, SecDevice starts mitigation for the zone containing the host.

- If auto-start is enabled in zone operational policy associated with the zone, SecDevice then automatically starts mitigation for that zone.

Perform the following steps to add the IP address of Arbor appliance:

Column Heading	Description
Type	Choose one of the following from the drop-down list: <ul style="list-style-type: none"><li>• SYSLOG</li><li>• SSH</li><li>• SNMP</li><li>• HTTP/HTTPS</li></ul>
Target	Choose one of the following from the drop-down list: <ul style="list-style-type: none"><li>• Accept</li><li>• Drop</li></ul>
Protocol	Choose one of the following from the drop-down list: <ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li></ul>
Port	Enter 514 as the port number for UDP or 22 as the port number for TCP.
Source	Enter the IP address that you want to block.
Action	You can perform the following functions: <ul style="list-style-type: none"><li>• <b>Plus sign (+)</b>—Allows you to add a specific host.</li><li>• <b>Edit</b>—Allows you to edit the previously entered host information.</li><li>• <b>Delete</b>—Allows you to delete the information.</li></ul>

## Route

The Route page allows you to configure static routes for SecDevice.

Perform the following steps to access the Route page:

1. Go **Administration >> Settings >> Route**
2. Click the **Plus sign (+)** and enter the appropriate information

Column Heading	Description
Type	Indicates the type of IP address selected.
Destination	Enter the host or subnet prefix.
Netmask	<p>Perform one of the following:</p> <ul style="list-style-type: none"> <li>• Enter the netmask of the IP.</li> <li>Or</li> <li>• Enter “255.255.255.255” to indicate a static route to a target host. The type indicator will change from subnet to host.</li> </ul> <p>Configuring Route to Target Host</p>
Gateway	Enter the Gateway IP address.
Intf Out	Enter the interface name.
Action	Displays the Trash icon and allows you to delete an existing route.

## Clock

The Clock page allows you to manually specify the date/time, time zone, and NTP settings.

Perform the following steps to access the Clock page:

1. Go to **Administration >> Settings >> Clock**.
2. In the upper portion of the page, which is called “Clock”, click the Date field and enter the Date in the format -MM-dd. For example, January 24, 2016 would be entered as 2016-01-24. Note that you will not be able to manually set the Time unless you disable the NTP servers below.
3. Click the Time Zone drop-down menu and select the region where your SecDevice device is located.
4. In the NTP Servers section of the page, select the NTP Server Status check box to get the time from an NTP server instead of manually configuring it.

5. Select one of the pre-defined NTP servers, or click the **+More** sign to add a new NTP server.
6. Click **Submit** to save your changes.

## Licensing

---

Before using SecDevice, you must enter a license to activate the software. To get the license, you must copy the UUID from the SecDevice Licensing page, create an account with A10's license manager, enter the UUID into the license manager, and this will create your license. Then upload this license into SecDevice's Licensing page.

Go to **Administration >> Setting >> Licensing**, to access the page.

1. Create or access your account on Organization' License Manager at the following URL:  
[https://glm.a10networks.com/wizard/glm\\_welcome/create\\_account](https://glm.a10networks.com/wizard/glm_welcome/create_account)
  - If you already have an account, click **Log into Your Account**.
  - If you do not have an account, click **Register an Account**.

---

**NOTE:** An account should have been created for you, so confirm before creating one.

---

2. Once you have set up an account, copy the UUID (see bottom of [Administration >> Setting >> Licensing](#) below) and paste the UUID into the License Manager. The license manager will generate your license token.

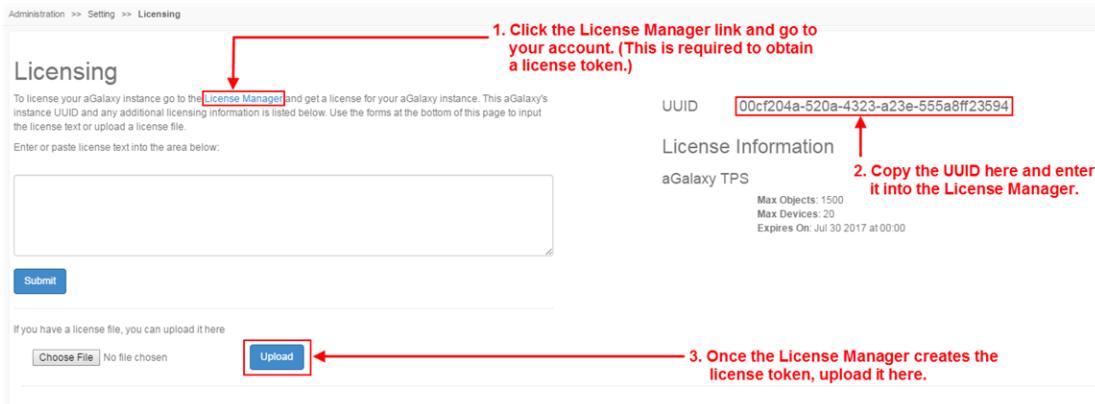
---

**NOTE:** Take care not to include any extra spaces when inputting this value.

---

3. Return to SecDevice's License page by navigating as follows: Select **Administration >> Settings >> Licensing**.

Figure 42 : Administration &gt;&gt; Setting &gt;&gt; Licensing



4. Enter the license. There are two ways to do so:
5. Upload text file – If the license is saved as a text file, you can click the **Browse** button, navigate to the text file, and then click the **Upload** button.
6. Copy/Paste – Copy the text of the license and paste it into the blank field. Then, click **Submit**.
7. Click **Submit**.

## SNMP

Simple Network Management Protocol (SNMP) is an IETF standards-based network management protocol that provides a consistent message format for communication between SNMP agent (in this case, SecDevice) and SNMP managers.

SecDevice allows SNMP to gather information such as notification messages, primary hard disk failure, high hard disk usage, high system control CPU, high memory usage, high system temperature, system power supply failure, and so on.

You can set thresholds for CPU high temperature and CPU, memory, and disk utilization. When the threshold exceeds, an SNMP trap is sent to the configured SNMP server.

You can also set the time interval for which the system resources such as CPU, memory, hard disk, hardware, link health, disk failure, and power supply should be monitored.

Perform the following steps to set up an SNMP Service:

1. Go to **Administration >> Settings >> SNMP**.
2. Under **General** tab, enter the following information:

Field	Purpose
<b>System SNMP Service</b>	Select the check box to enable the third-party systems to poll the SecDevice device for health checks and statistical monitoring information. Deselect the checkbox to disable the option.
System Contact	Enter the system administrator's email address who handles the third-party SNMP system.
System Location	Enter the location of the SNMP polling system.
SNMPv2 Community Read	Enter the (public) community string for authentication on the third-party SNMP server.

3. Click **Download** to download the SecDevice MIBs, button.
4. Under **SNMPv3 Users** tab, click **Add New User** to add a new SNMPv3 user,
5. In the **New User Name** box, enter the user name. The user name can be 5 to 20 characters long.
6. From the **Authentication Type** drop-down, choose the Authentication type from the following choices:

Options	Purpose
noAuthNoPriv	If noAuthNoPriv is selected, click <b>Add</b> to create the new user.
authNoPriv	If authNoPriv is selected, the Authentication Algorithm drop-down and Password field is displayed. <ul style="list-style-type: none"> <li>• From the <b>Authentication Algorithm</b> drop-down list, select SHA (Secure Hash Algorithm) or MD5 (Message Digest). The recommended algorithm is SHA.</li> <li>• In the <b>Password</b> field, enter your password. The password can be 8 to 20 characters long. It can contain the</li> </ul>

Options	Purpose
	following characters - a to z, A to Z, 0 to 9, and special characters such as !@#\$%^&*().
authPriv	<p>If authPriv is selected, the Authentication Algorithm drop-down, Password, Encryption Algorithm, and Encryption Passphrase field is displayed.</p> <ul style="list-style-type: none"> <li>From the <b>Authentication Algorithm</b> drop-down list, select SHA or MD5. The recommended algorithm is SHA.</li> <li>In the <b>Password</b> field, enter your password. The password can be 8 to 20 characters long. It can contain the following characters - a to z, A to Z, 0 to 9, and special characters such as !@#\$%^&amp;*().</li> <li>From the <b>Encryption Algorithm</b> drop-down list, select DES (Data Encryption Standard) or AES (Advanced Encryption Standard). The recommended Encryption algorithm is AES.</li> <li>In the <b>Encryption Passphrase</b> field, enter the password. The password can be 8 to 20 characters long. It can contain the following characters - a to z, A to Z, 0 to 9, and special characters such as !@#\$%^&amp;*().</li> </ul>

7. Click **Add** to create the new user.'

---

**NOTE:** Be aware that when the Engine ID is changed, any existing SNMP users will be cleared and these users will need to be recreated. This is because the SNMP Engine ID is used in conjunction with the MD5 or SHA security digest for a SNMP user's password. An Engine ID is automatically generated if one is not specified.

---

8. Under **SNMP Trap Hosts** tab, enter the following information:

Field	Purpose
Trap Host	Enter the IPv4 host address that receive the traps.
Trap Version	Choose one of the following versions: <ul style="list-style-type: none"> <li>v2c</li> </ul>

Field	Purpose
	<ul style="list-style-type: none"> <li>v3</li> </ul>
SNMPv2 Community String	Enter the community string. <b>NOTE:</b> _____ It is displayed only when v2c is chosen.
SNMPv3 User Name	Enter the user name. <b>NOTE:</b> _____ It is displayed only when v3 is chosen.
Engine ID	Enter the ID for the SNMPv3 protocol engine.
Authentication Type	See <a href="#">From the Authentication Type drop-down, choose the Authentication type from the following choices:</a> to enter the appropriate information.

9. Click **Add** to create the new user.

## Notification

The Notification page displays a list of all email notification events and the number of times these events have occurred (when Notification Events tab is selected).

To receive email notifications, a SMTP server must be configured through the **Mail Settings** tab.

Perform the following steps to access the notification page:

1. Go to **Administration >> Settings >> Notifications**.
2. (Optional) Click the Reset, Refresh, or Delete button to perform the corresponding action.

After a notification event has been created, it can be enabled or disabled by clicking on the check box for the object and clicking on Enable or Disable.

Table 133 : Column Headings in the Email Notification Events page

Column heading	Description
Name	Displays the name of the configured notification event.
Event Type	Displays the event type set for the notification event.

Table 133 : Column Headings in the Email Notification Events page

Column heading	Description
Count	Indicates the number of times the event occurred.
Notify Every N	Displays the number you have selected to be notified after every n event.
Email Notification	Displays the status as disabled or enabled.
HTTP Post Notification	
SNMP Trap Notification	Displays the status as disabled, enabled or unsupported.
Actions	Click Edit to modify a configured notification event.

For configuration of events, see [Notification Events](#) For configuration of the SMTP server for notification, see [Notification Settings](#).

## Notification Events

Perform the following steps to create a notification event:

1. From **Administration >> Settings >> Notifications**, select the **Notification Events** tab.
2. Click **Create**.

Field	Purpose
Name	Enter the name for the event alert.
Event Type	Choose the event type that triggers a notification.
Email Enable	Select the check box to enable email notification.
HTTP Post Enable	Select check box to enable HTTP Post.
SNMP Trap Enable	Select or deselect the check box to either enable or disable the event. By default, notification events are enabled (selected).

3. Click **Submit**.

## Notification Settings

The Notification Settings allow you to set up the information about the sender and the recipient. It also allows you to set up the HTTP POST. The HTTP POST is JSON. You can provide the URL and the parameters such as an authentication API Key in the headers.

A new event is created on incident start, incident stop, mitigation start, and mitigation stop with different event data under incident status payload.

To configure the SMTP server for sending Emails, perform the following:

1. Go to **Administration >> Settings >> Notification**, select the **Notification Settings** tab.
2. Under **Email Settings** section, enter the appropriate information:

### For Set up Sender

Field	Purpose
SMTP Server	Enter the name of the SMTP server.
Secure Connection	Choose a security protocol from the drop-down list.
SMTP Port	Enter a Port value. <ul style="list-style-type: none"><li>• If SSL/TLS is selected for Secure Connection, set the port to 465.</li><li>• If STARTTLS is selected for Secure Connection, set the port to 587.</li></ul>
Sender Mail Address	Enter the email address of the sender.
SMTP Authentication	select the appropriate option based on whether you want to allow the email server access to be authenticated or unauthenticated.
Include sender in BCC	Select the check box to include the sender in a blind carbon copy.

### For Set up Recipient

In the **Default Address** field, enter the default email address of the recipients for sending the email notifications.

3. Under **HTTP POST Settings** section, enter the appropriate information:
  - In the **URL** field, enter the server URL.
  - In the **Headers** field, enter the parameters to be added to the JSON header.
4. Under **Set up Subscriber Portal**, perform the following:
  - In the **URL** box, enter the URL of the Subscriber Portal in the following format:  
`https://<Subscriber Portal IP>/portalapi/import/data/`  
This is a prerequisite step for adding this SecDevice device as a controller to the Subscriber Portal. If this set up is not complete, then Subscriber Portal cannot communicate with this SecDevice device.  
For more information, see Subscriber Portal 1.0 documentation.
5. Click one of the following:
  - Send a test mail—Checks SMTP settings.
  - Send a test http post request—Sends the HTTP POST request.
  - Submit—Completes the configuration.

## External Logging

---

SecDevice cannot sometimes store log messages locally due to the high volume of logs. Therefore, the log messages can be sent to the external Syslog hosts. The log messages can be exported either as CEF or as raw messages. You can configure up to 8 Syslog hosts to export the log messages.

You can configure external logging under **Administration >> Maintenance >> External Logging**.

Perform the following:

1. On the External Logging page, the External Syslog Hosts are the external Syslog servers. SecDevice sends the logs to the hosts configured in this table. A table is displayed under ‘External Syslog Hosts’ with the details mentioned below:

Field	Description
External Host IP	Displays IP for the external syslog server added
Port	Displays port of the external syslog server.
Action	After entering the details for the IP and port, click the 'Add' icon to add the external syslog server. Click the 'Delete' icon to delete a configured syslog server.

---

**NOTE:** The messages are transported only using UDP.

---

- From the Output Log Format drop-down, select the format in which the SecDevice audit logs should be exported. The following options are available:

- CEF

The log messages are sent to the hosts in CEF format.

For example,

```
CEF:0|A10|SecDevice|1.0|Logstash|Logstash|1|rt=1616537445000
dvchost=aGalaxy5000-box69 spid=24126 dvc=10.16.23.69 cs1=reports
cs1Label=component suser=admin msg=zone_incident report for object
QA_ZONE111-53-dns-udp-20210324-140239 with file name tps-zone-inc-
20210324-141043.pdf generated successfully
```

Mapping for the terms used in CEF messages is mentioned below:

CEF	Mapped to
rt	timestamp
spid	pid
suser	username
msg	message
dvchost	hostname
dvc	SecDevice Management IP

cs1	Component
cs1Label	String ‘component’
HEADER:SEVERITY	severity

- Raw messages

Original log messages are sent to the hosts.

For example,

```
2021-03-24 08:13:47 aGalaxy5000-box69 INFO [packet_capture]
source=unknown, pid=5788, tn=Dummy-4, qn=packet_capture.file_
transfer_subscriber, mn=file_transfer_subscriber, fn=extract_file,
un=unknown, msg=Extracted /tmp/9603856e-8f78-4e77-a3a1-974f797e85ab_
pcapdata.tar.gz to /a10data/packet_capture/job/3bf2f496-3124-4866-
99ca-f382a46e711c/task/9603856e-8f78-4e77-a3a1-
974f797e85ab/3bf2f496-3124-4866-99ca-f382a46e711c_merge.pcapng
```

- For Export SecDevice Audit Logs, select ‘Yes’ to export the SecDevice audit logs in the format selected under ‘Output Log Format’. The logs are exported to the external servers configured under ‘External Syslog Hosts’.
- Click ‘Save Config’ to save the updates.

A message is displayed to reconfirm the settings. After selecting ‘Yes’, applying the configuration may take some time and the logs may not be sent to the external hosts till the configuration is saved.

## TPS

The TPS page allows you to configure the automation of Zone Mitigation.

To access the TPS page, navigate as follows:

- Go to **Administration >> Settings >> TPS**.
- Select the **Use API Key for Notification** checkbox to enable the feature. It allows

the device to send notifications to SecDevice using an API key instead of logging in with the password.

---

**NOTE:** Applicable to newly added devices and existing devices after doing an ‘Sync to Device’.

---

## Call Home SERT

---

The Call Home Security Engineering Research Team (SERT) service allows SecDevice to periodically download A10 provided threat intelligence and keep the DDoS countermeasure configuration objects like class-lists, zone templates, zone service protection profiles, and other objects up to date.

### Settings

To enable the Call Home SERT Service:

1. Go to **Administration >> Settings >> Call Home SERT**.
2. In the Call Home SERT Service, click the **Enable Callhome SERT Service** check box to enable the Call Home SERT service.
3. Select the Enable Incident export option to export the incident information to A10 SERT. On selecting this option, the “Is Production data” option is displayed.
4. Select the “Is Production data” option to flag the incident information coming from the customer’s production environment or setup.
5. From **Download Class-Lists**, **Download Zone Templates**, and **Download Zone Service Protection Profiles** drop-down lists, select one of the following options:
  - **Disabled**—Specifies that the option to download the selected object is disabled. You can choose this option when you do not want to override your class-to lists when a zone is saved.
  - **Download only**—Specifies that the selected object will be downloaded periodically to the following location:

/a10data/callhome/sert/downloads/<timestamp>/

You can manually save the downloaded object to the SecDevice database by clicking Save on the Call Home SERT >> Download History page. For more details, see [Download History](#).

- **Download and save to SecDevice config DB**— Specifies that the selected object will be downloaded and then saved to the SecDevice's database.
6. In the Download Interval box, enter the time interval in hours the specified objects must be downloaded.
  7. In the SERT API Key box, enter the SERT key provided by A10 support. Contact A10 Support to obtain a SERT API key. To contact A10 Support, go to <https://support.a10networks.com>.
  8. Click Update Settings to update the changes made to the Call Home SERT Service. The changes could be enabling or disabling the objects and changing the download interval.
  9. Click **Download Now** to download the objects.
  10. Click **Test Connectivity** to test whether agalaxy.a10protects.com can be reached from the GUI.

## Download History

To view the download history and to save the new or updated object to the SecDevice's database:

1. Click **Download History**.
2. Under Save to SecDevice DB, click **Save** to create or update the objects in SecDevice's database.

You can use the objects downloaded from the Call Home SERT > Settings page to manually update the older version of the objects.

For example, let's assume you have the latest version 'y' of the class-list in the SecDevice database. For the version 'x' of the same class-list, you can click Save (with the 'update object if it already exists' checkbox selected) to update the database with the older version of the class-list.

3. In the pop-up, enter a name you want to associate with the object.
4. On clicking **Save**, if a zone template of subtype HTTP with a name "A10" is saved,

you can view this object in the HTTP Zone Template tab. The template can be used like any other zone template.

It is recommended you do not change the default name of the object. This is because if you change the mode of the object from Level 1 to Level 2 or 3, then call home SERT tracks and updates the SecDevice object. If you change the SERT object name in the Level 1 Save workflow, then you must manually update this object to SecDevice and then push it to the devices.

5. Select **Update object if it already exists** check box if the object already exists on SecDevice's database.
6. Click **Submit**.

## Web Certificate

---

The Web Certificate page allows the import of certificate and key on SecDevice GUI.

To access the Call Home page, navigate to **Administration >> Settings >> Web Certificate**.

1. Click on **Choose File** to select the Certificate Source and Key Source.
2. Click **Apply** to apply the web certificate.
3. When prompted to restart, click on **Proceed**.

SecDevice automatically logs out the user and restart Apache. The login page appears.

---

**NOTE:**

Web Certificate can be reset using Consoleadmin. For more information, refer to step 14 in [Consoleadmin](#).

---

## Geo Location

---

The Geo Location page allows you to view all the GeoLite2 databases used in SecDevice. You can search for Geo Location using the IP address, Autonomous System Number (ASN), and Country. You can also download GeoLite2 databases from <https://www.maxmind.com> and upload them on the Geo Location page.

To view the Geo Location databases for SecDevice, go to Administration >> Settings >> Geo Location. The database names and the versions are displayed.

To import Geo Location databases, perform the following:

1. Click Import Geo Location databases. The Upload Geo Location Databases pop-up screen is displayed.

The supported file formats for uploading the databases are .zip and .tar.gz files.

2. Click Choose Files and select a database. Then, click Upload.

To search for the geographically located databases, select one of the following options from the drop-down list:

- IP address- Searches the databases based on the IP address entered in the search box.
- ASN- Searches the databases based on the Autonomous System Number.
- Country-Searches the databases based on the continent and the country selected from the drop-downs.

## User Management

The User Management page contains the following tabs described in :

Table 134 : Access Management Tab

Tab	Description
Users	View configured RBA user accounts or configure one. Make sure a role exists that you want to apply before creating a user.
Roles	View, edit or create system-defined roles. To create a role, you will need to select an existing permission. Creating permissions is done on the Privileges page.
Privileges	Add new privileges or edit the existing system-defined privileges to create permissions. Privileges determine which actions an SecDevice administrator is allowed to perform.
Ext Auth Role Mapping	Allows viewing, editing or deletion of all remote authentication servers (RADIUS, TACACS, LDAP) that have been configured on SecDevice.

Table 134 : Access Management Tab

Tab	Description
RADIUS Config	View, edit, delete or create RADIUS server.
TACACS Config	View, edit, delete or create TACACS server.
LDAP Config	View, edit, delete or create LDAP server.
Auth Seq	<p>Change the sequence by which external authentication protocols are used to authenticate users.</p> <p>By default, SecDevice checks its local database to authenticate an administrative user before checking RADIUS, TACACS, and finally LDAP.</p>

The Users, Roles and Privileges tabs allow you to configure which users are allowed to access SecDevice, their roles, and the privileges associated with each role.

To configure Access Management, navigate as follows:

Select **Administration >> User Management** from the main menu.

The default tab is set to Users. To create a new user with different permissions than the administrator, it is recommended to go through the sequence of tabs as follows:

1. Click the Privileges tab and Create a privilege.
2. Click the Roles tab and Create a role.
3. Click the Users tab and Create a user.

In the section, the following topics are covered:

- [Users](#)
- [Roles](#)
- [Privileges](#)
- [External Authentication Role Mapping](#)
- [RADIUS Configuration](#)
- [TACACS Configuration](#)

- [LDAP Configuration](#)
- [Authentication Sequence](#)

## Users

Perform the following steps to create a User:

1. Go to **Administration >> User Management >> Users**.
2. Click **Create** and enter the appropriate information in each field:

Field	Purpose
User Name	Enter a user name.
Password	Enter the password.
Confirm Password	Re-enter the password to confirm.
Role	Choose a suitable Role(s) from the drop-down list. Option to choose multiple roles is also available. For more information, see <a href="#">Roles</a> .

3. Click **OK** to save.

## Roles

Perform the following steps to create a role:

1. Go to **Administration >> User Management >> Roles**.
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Role Name	Enter the name of the role.
Permissions	Choose a suitable Privilege(s) from the drop-down list. Option to choose multiple privileges is also available. For more information, see <a href="#">Privileges</a> .

3. Click **OK** to save.

## Privileges

Perform the following steps to create a privilege access list to create a Role:

1. Go to **Administration >> User Management >> Privileges**.
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Privilege Name	Enter the name of the privilege.
View Only Mode	Select the check box to create a privilege where the user can only view information and is unable to make any changes.
Permission List	Select the check boxes for the appropriate Permissions.

3. Click **OK** to save.

## External Authentication Role Mapping

In this section, user can map privilege levels or administrative groups defined in an external authentication and authorization server to the roles defined within SecDevice.

Perform the following steps to assign a role to an externally authenticated user:

1. Go to **Administration >> User Management >> Ext Auth Role Mapping**.
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Authentication Type	Choose the type of authentication from the drop-down menu.
Privilege Level	For TACACS+ and RADIUS, enter the privilege level that corresponds to the SecDevice role. For LDAP, enter the name of the LDAP group that corresponds to the SecDevice role.

Field	Purpose
SecDevice Role	Assign a role to the externally authenticated user.

3. Click **OK** to save.

## Privilege Levels for RADIUS and TACACS+

The following table lists the RADIUS and TACACS+ privilege levels that matches the GUI privileges.

GUI Access Role	Privilege Levels	
	RADIUS	TACACS+
ReadWriteAdmin	2	15
SystemAdmin	3	14
NetworkAdmin	4	13
NetworkOperator	5	12
SIbServiceAdmin	6	11
SIbServiceOperator	7	10
ReadOnlyAdmin	1	0
PartitionReadWrite	8	9
PartitionNetworkOperator	9	8
PartitionSIbServiceAdmin	10	7
PartitionSIbServiceOperator	11	6
PartitionReadOnly	12	5

For more information, see *ACOS Management Access and Security Guide*.

## RADIUS Configuration

Add an external Remote Authentication Dial-In User Service server, or edit an existing one by using the RADIUS Configuration feature.

Perform the following steps to add a RADIUS server:

1. Go to **Administration >> User Management >> Radius Config.**
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Host	Enter the Host IP address of the RADIUS server.
Authentication Method	Enter the Authentication method.
Authentication Port	Enter the Authentication Port number.
Retries	Enter the number of allowable retries.
Shared Secret	Enter the Shared Secret (password) expected by the server when it receives the requests.
Accounting Port	Enter the Accounting Port value.

3. Click **OK** to save.

## Setup RADIUS Users

1. Install a RADIUS daemon. For instance, FreeRADIUS.
2. Create a new dictionary file in `/etc/radb/dictionary.a10`.  
Use include syntax with the dictionary file as follows:  
`$INCLUDE /etc/radb/dictionary.a10`  
The following is saved under dictionary file:

```

# Organization dictionary.
# Version: 1.1 08-Nov-2012
# $Id: Setup_RADIUS_users.htm 27776 2023-03-28 14:08:51Z sshettigar $

#
VENDOR A10 22610
BEGIN-VENDOR A10
ATTRIBUTE A10-App-Name 1 string
ATTRIBUTE A10-Admin-Privilege 2 integer
VALUE A10-Admin-Privilege Read-only-Admin 1
VALUE A10-Admin-Privilege Read-write-Admin 2
VALUE A10-Admin-Privilege Reports-Readonly 3
# VALUE A10-Admin-Privilege <custom-privilege> <unique integer>
Custom privileges can be added

END-VENDOR A10

```

3. Add a secret for the client application. For testing, you can use `vi /etc/raddb/clients.conf` and add the following:

```

client 0.0.0.0/0 {
    secret          = your-secret
    shortname       = SecDevice
}

```

4. Add Users in RADIUS. For testing, you can add users manually here:

```

vi /etc/raddb/users
a10 Cleartext-Password := "a10"
A10-Admin-Privilege = Read-write-Admin
pgupta Cleartext-Password := "pgupta"
User-Name = "pgupta",
A10-Admin-Privilege = Read-only-Admin
reportsonly Cleartext-Password := "a10"
User-Name = "reportsonly",
A10-Admin-Privilege = Reports-Readonly

```

---

**NOTE:** Access privilege should match the privileges described in `dictionary.a10` file.

---

**NOTE:** You may need to restart the RADIUS server after adding a new user “service raddb restart”.

---

5. In SecDevice, create [RADIUS Configuration](#) and add RADIUS Server IP and shared secret created in Step 3 above.
6. In SecDevice, create [External Authentication Role Mapping](#) using the integer mapped with each privilege. For instance, External Privilege = 1 should be mapped with SecDevice role (agallery-admin).
7. Log in to SecDevice with your user-name and password.

## TACACS Configuration

---

Terminal Access Controller Access Control System (TACACS) configuration lets you add or edit an external TACACS server. SecDevice supports two types of authentication for TACACS configuration:

- Password Authentication Protocol (PAP)
- ASCII

Perform the following steps to add a TACACS server:

1. Go to **Administration >> User Management >> TACACS Config.**
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Host	Enter the Host IP address of the TACACS server.
Port	Enter the Port number.
Shared Secret	Enter the Shared Secret (password) expected by the server when it receives the requests.
Retries	Enter the number of allowable retries.
Timeout	Enter the number of seconds when the server will timeout.
Remote	Enter the Remote Address.

Field	Purpose
Address	

3. Click **OK** to save.

## LDAP Configuration

Perform the following steps to add an external LDAP server:

1. Go to **Administration >> User Management >> LDAP Config**.
2. Click **Create** and enter the appropriate information in each field.

Field	Purpose
Host	Enter the Host IP address of the LDAP server.
Port	Enter a Port number.
ID Attr.	Enter the LDAP attribute used for user identification. For example, sAMAccountName.
Authenticating Attr.	Enter the LDAP attribute used for user authentication.
BIND DN User-name	Enter the username for BIND DN account. This account is used to search user in the provided DN String(s)
BIND DN Pass-word	Enter the password associated with the BIND DN.
LDAP Version	Enter the LDAP Version.
Distinguished Name String	Enter LDAP Distinguished Name (DN) string(s) used to search and authenticate users.  Multiple DN strings can be added, each from a new line.  <b>NOTE:</b> Do not include the DN attribute in this string. For example: <u>ou=Users,DC=corp,DC=companyname,DC=com</u>

3. Click **OK** to save.

## LDAP Authentication

In LDAP Authentication, BIND operations are performed to authenticate the user against the LDAP server. During the authentication process, BIND DN and user credentials are searched in the LDAP server to identify and authenticate the user for subsequent action requests.

Perform the following steps to setup the user authentication and authorization using LDAP:

1. Add an external LDAP server. For more information, see [LDAP Configuration](#).
2. Create a privilege access list. For more information, see [Privileges](#).
3. Create a role that includes one or more privileges. For more information, see [Roles](#).
4. Map the external authentication role to the local SecDevice role. For more information, see [External Authentication Role Mapping](#).
5. Change the server sequence for authentication, if required. For more information, see [Authentication Sequence](#).

## Authentication Sequence

---

By default, SecDevice checks its local database to authenticate an administrative user. The Authentication Sequence page allows for changes to the server authentication sequence.

---

**NOTE:** Configure a RADIUS, TACACS or LDAP server, and the server(s) will appear in the Available Servers column.

---

Perform the following steps to set up the authentication sequence:

1. Go to **Administration >> User Management >> Auth Seq**.
2. To choose which server(s) to use, click on a server to toggle it between the Available Servers and Selected Servers column.

**NOTE:** Under **Selected Servers** column, it is recommended to use SecDevice (local authentication) first in the sequence and then the LDAP authentication mechanism.

---

3. Click **Save** to store your changes.

## Maintenance

---

The Maintenance page allows you to schedule a reboot of SecDevice, perform an upgrade, or create/download a Tech Support file. Select Administration >>Maintenance to navigate to this page.

### Reboot

---

Perform the following steps to schedule a reboot for your SecDevice appliance:

1. Go to **Administration >> Maintenance >> Reboot**.
2. Under **Schedule SecDevice Reboot**, in the **Time Interval** field, enter the number of hours and minutes that must pass before reboot.
3. (Optional) In the **Reason** field, enter the reason for the reboot
4. Click **Schedule Reboot** to complete action.

### Upgrade

---

Perform the following steps to upgrade your SecDevice appliance:

1. Go to **Administration >> Maintenance >> Upgrade**.
2. Under **Upgrade SecDevice** tab, click **Select a file** button to upload the file.
3. Click **Upgrade**.

Under **Upgrade History** tab, you can view the logs of the previous upgrades.

---

**NOTE:** SecDevice does not support software downgrade to a previous version.

## Backup

---

To perform backup configuration for SecDevice appliances, see [Backup Setup](#), [Periodic Backup Setup](#), and [Backup Log](#).

## Data Management

---

Data Management allows you to clean up alerts, audit logs, device logs, and events. It shows the size of “other” files to maintain sufficient disk space on /a10data. To ensure optimal performance, it is recommended to delete unnecessary files and keep only the required number of files.

Data Management provides a list of major categories and the disk space used by each category. On clicking a category, you can further view sections of each category broken down by date and the disk space used. You can either delete a section that is consuming more space or perform disk rotation. Disk rotation helps to retain the latest files and remove the old files.

To perform data rotation:

1. Go to **Administration >> Maintenance >> Data Management**.
2. Select **Data Rotation**.
3. In **Keep the latest**, enter the number of months of data files to be maintained in the system. You can enter from 1 to 60 months. For example, if you specify 12 months, the files older than 12 months are deleted from the system.

---

**NOTE:** For Audit and Device logs from earlier releases (SecDevice 5.0.6 and earlier), the data rotation is performed based on the size.

---

## Tech Support

---

The Tech Support page allows you to quickly provide Tech Support with information to help assist with any issues that are encountered.

To compile log information that may assist in problem solving an issue, navigate as follows:

1. Select **Administration >> Maintenance >> Tech Support**.
2. Click on **Create Download**. A “Please Wait” message momentarily appears.
3. Click **Download** in the Action column to download a tar file containing various log information that can be provided to technical support.

## SecDevice Monitor

---

Perform the following steps to set up a SecDevice Monitor:

1. Go to **Administration >> Maintenance >> SecDevice Monitor**.
2. Under **General**, select the check box for **SecDevice Monitor SNMP Trap** to enable the traps for SecDevice system monitoring events.
3. Go to **Administration >> Settings >> SNMP**, and see **SNMP Trap Host**. The following information is displayed here:
  - **Trap Host**—Displays the IPv4 host address that receive the traps.
  - **Trap Version**—Displays the trap version between v2c and v3.
  - **Community (v2c)/Authentication (v3)**—Displays the (public) community string for authentication on the third-party SNMP server.
4. Under Threshold, enter the following information:

Field	Purpose
CPU High Temperature Threshold	Enter the threshold for CPU high temperature. If the CPU high temperature crosses the configured threshold, an SNMP trap is generated and sent to the configured SNMP host.
<b>CPU Usage Critical Threshold</b>	Enter the threshold for CPU utilization. If the CPU utilization crosses the configured threshold, an SNMP trap is generated and sent to the configured SNMP host.
Memory Usage Critical Threshold	Enter the threshold for memory usage. If the memory utilization crosses the configured threshold, an SNMP trap is generated and sent to the configured SNMP host.
Disk Usage Critical Threshold	Enter the threshold for disk utilization. If the disk utilization crosses the configured threshold, an SNMP

Field	Purpose
	trap is generated and sent to the configured SNMP host.

5. Under **Interval**, enter the following information:

Field	Purpose
<b>CPU Monitor Interval</b>	Enter the number of seconds SecDevice should monitor the CPU utilization.
<b>Memory Monitor Interval</b>	Enter the number of seconds SecDevice should monitor the memory utilization.
Disk Monitor Interval	Enter the number of seconds SecDevice should monitor the disk utilization.
<b>Hardware Monitor Interval</b>	Enter the number of seconds SecDevice should monitor the hardware utilization.
Link Monitor Interval	Enter the number of seconds SecDevice should monitor the health of the links or interfaces.
<b>Disk Failure Monitor Interval</b>	Enter the number of seconds SecDevice should monitor the disk failure errors.
Power Supply Monitor Interval	Enter the number of seconds SecDevice should monitor the power supply status.

6. Click **Save** to store your changes.

# High Availability (HA)

---

SecDevice physical or virtual appliance can be deployed as an Active-Standby pair to provide High Availability (HA) as a protection against the failure of either node.

Active Node is the node that runs SecDevice services, communicates with TPS devices and is accessible through GUI. Data is continuously synced from Active node to the Standby node.

Standby node is the node that does not run SecDevice services and there is no communication between TPS devices and standby SecDevice. Also, GUI is not accessible. You can log in as **consoleadmin** through SSH or console terminal to monitor or make limited changes on standby.

For more information on the status of the nodes in HA pair, see [View High Availability](#).

SecDevice's synchronization mechanism ensures that the following configurations are synchronized from Active node to the Standby node, in the near real-time.

- All configuration objects such as zones, templates, and policies.
- All the generated or monitored data such as incidents, reports, and packet captures.
- All the logs and metrics from SecDevice and TPS devices.

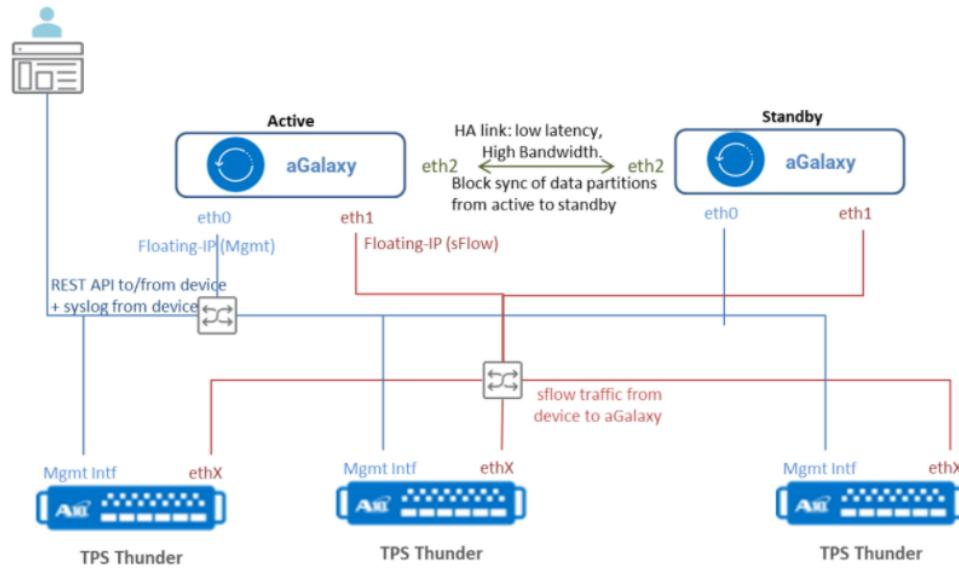
If the active node fails, the standby node automatically becomes the new active node.

---

**NOTE:** High Availability setup and SecDevice + Detector (combo) features are mutually exclusive.

---

Figure 43 : Topology Diagram



## Known Limitation

The current HA configuration supports only a cold fail-over. In the cold fail-over, when the current active node goes down, the standby node takes 2-3 minutes for the current standby node to become active. When the switch-over happens, services are accessible after a brief outage.

# Prerequisites

## System Requirements

The two SecDevice nodes in a High Availability (HA) setup must have the same system specifications for the following:

- Disk capacity
- Performance
- Memory
- CPU count

For more information, refer SecDevice installation guide for disk sizing guidelines.

## Networking Requirements

The HA setup must have the following networking specifications:

- Each node must have a unique host name. The following interfaces are required for the setup:
  - **Management interface**—This interface is for GUI HTTPS access or **consoleadmin** SSH access. SecDevice communicates with TPS device through management interface to push the configuration and TPS device sends the attack notifications and syslog to SecDevice. The eth0 interface of SecDevice appliance is by default the management interface.
  - **sFlow interface**—TPS device sends traffic metrics to SecDevice using the sFlow protocol. TPS device can send sFlow to SecDevice through the management network. However, to ensure lossless transmission of metrics when the number of protected objects are high, it is highly recommended to have a separate interface to receive sFlow traffic from the TPS data interface.
  - **HA interface**—Active SecDevice uses this interface to sync data to the standby SecDevice.
- A total of eight IP addresses are required. This includes:

- You need three different /24 subnets for management, sFlow and HA interfaces.
- Management interface—Must have one IP address per node and one additional floating IP address.
- sFlow interface—Must have one IP address per node and an additional floating IP address.
- HA link interface—Must have two IP addresses, one for each node.

## HA Link Connectivity

Latency must be less than 1 msecs and bandwidth of ideally at least 1 Gbps. If possible, it is recommended to directly connect the HA link interfaces of the two SecDevice appliances in the HA pair.

## SecDevice and Device Connectivity for Management

Latency must be less than 200 msecs. Bandwidth available impacts the time taken to push the configuration and the large files to the device.

## SecDevice and Device Connectivity for sFlow

Latency must be less than 200 msecs. Bandwidth requirement depends upon the number of zones and zone services configured on the managed devices.

## Known Limitation

When HA is configured, only IPv4 addresses must be used. Support for IPv6 addresses in a HA setup is currently not available.

## Software Requirements

During initial setup and during steady state, both nodes must be running on the same SecDevice version.

## Licensing Requirements

Two licenses of the same type (SecDevice TPS) must be installed on each of the SecDevice versions you plan to configure as an HA pair.

## System Backup

It is strongly recommended that SecDevice backup is done prior to HA setup.

For more information, see [Backup](#).

## High Availability Setup

To prepare for High Availability (HA) setup, ensure the following requisites:

- The time taken by initial HA setup mostly depends upon the size of the data already present. On a freshly installed setup without much data, it may take less than thirty minutes. On a setup with gigabytes of run-time data such as reports, packet captures, and device metrics, several hours can be consumed. Ensure that enough time is available to complete HA setup without interruption.

---

**NOTE:** Do not interrupt the HA setup process once it has begun. Interrupting DRBD setup may render the setup in a state that requires manual intervention to recover.

---

- Ensure to have all the IP addresses ready as mentioned in the [Prerequisites](#) section.
  - HA IP address for SecDevice A and the corresponding ethernet interface
  - HA IP address for SecDevice B and the corresponding ethernet interface
  - Management floating IP address

---

**NOTE:** Do not configure the HA interface and sFlow interfaces prior to the HA setup. If already configured, please unconfigure them prior to HA setup.

---

- sFlow collector IP address for SecDevice A and corresponding ethernet interface
- sFlow collector IP address for SecDevice B and corresponding ethernet interface
- sFlow floating IP address

- Both SecDevice nodes should be configured with the same system time zone and clock. For more information on clock settings, see [Clock](#).

## Pairing SecDevice 5000 with SecDevice VM

Downgrading from current SecDevice version to a previous version is not supported.

## HA Setup Overview

The High Availability (HA) setup process consists of three stages:

### Stage 1. Network Setup

- The management, HA link, and sFlow interfaces on both nodes get configured. HA link interface is used primarily for data synchronization.
- From Node A (the node where the HA setup was initiated), you can configure network settings required for HA on Node B as well.

### Stage 2. DRBD Setup for Data Synchronization

1. Checks file system and LVM data volumes sizes.
2. Shrinks file system and LVM data volumes.
3. Generates DRBD configuration from network configuration.
4. Creates DRBD block devices.
5. Initial data synchronization occurs from the local node to peer node at the block device level.
6. Expands LVM data volumes and file systems.

### Stage 3. Pacemaker Setup for Resource Monitoring and Failover Actions

1. Generates Pacemaker configuration based on network configuration.
2. Configures Pacemaker resource agents, which in turn manage the data sync, file systems, Floating IPs, and the SecDevice application services. A resource agent's role is to start, stop, and monitor a resource on the active node.

3. Start the pacemaker resource agents which, among other things, start SecDevice services on the local (active) node.

## Configure HA Settings

Choose one of the SecDevice nodes as the primary.

---

**NOTE:** If SecDevice node is chosen as the secondary node (Peer node), data from the primary node overwrites it.

---

Perform the following steps to configure the HA settings:

1. On the primary SecDevice node, access the GUI using its management IP address or hostname.
2. Go to **Administration >> Settings**, and click **HA**.
3. Click **Configure HA Settings**.
4. In the new browser tab or window, enter the following information:

Table 142 : Configure HA Settings

Field	Purpose
Mgmt floating IP	Enter the management floating IP address
Peer mgmt IP	Enter the peer management IP address.
<b>HA local IP</b>	Enter the HA interface IP address of the primary SecDevice.
HA peer IP	Enter the HA interface IP address of the secondary SecDevice.
HA local interface	Select the ethernet interface of the primary SecDevice.
HA peer interface	Select the ethernet interface of the secondary SecDevice.
sFlow local IP	Enter the IP address for the sflow interface of the primary SecDevice.
sFlow peer IP	Enter the IP address for the sflow interface of the secondary SecDevice.
sFlow local interface	Select the ethernet interface of the primary SecDevice.
sFlow peer interface	Select the ethernet interface of the secondary SecDevice.
sFlow floating IP	Enter the sFlow floating IP address.

5. Click **Setup**. At this point, the page URL changes to **/ha/log**. A text area periodically refreshes, displaying debugging text during the HA setup. The HA setup should go through the following three stages without any user input.

1. Network
2. DRBD
3. Pacemaker

At the end of Pacemaker setup, the message “HA Setup Complete” appears along with the management floating IP address.

## View High Availability

Perform the following steps to view the High Availability (HA) status of an SecDevice setup:

1. Log in to SecDevice GUI using the management floating IP address.
2. Go to **Administration >> Settings** and click **HA**.  
The HA page displays the parameter provided during the setup along with the current HA status information.
3. When HA is active and healthy:
  - Pacemaker Online Status is displayed as “Both Up”.
  - Connection state is displayed as “Connected” and Disk State is displayed as “UpToDate” on both the nodes.

Figure 44 : HA Settings

HA Settings		
<input type="checkbox"/> Configure HA settings		
<b>Basic HA Settings and Status</b>		
Local Hostname	aGalaxy	
Local Mgmt. IP	10.16.27.69/24	
Local HA IP	17.10.16.69/24	
Local sFlow IP	17.17.17.69/24	
Peer Hostname	AG-10-16-27-70	
Peer Mgmt. IP	10.16.27.70/24	
Peer HA IP	17.10.16.70/24	
Peer sFlow IP	17.17.17.70/24	
Floating IP	10.16.27.37/24	
sFlow Floating IP	17.17.17.37/24	
Pace Maker Online Status	Both Up	
<b>HA Status on Local Machine (aGalaxy)</b>		
Connection State #0	<b>Connected</b>	
Local Resource Role #0	Primary	Secondary
Disk State #0	UpToDate	UpToDate
Connection State #1	<b>Connected</b>	
Local Resource Role #1	Primary	Secondary
Disk State #1	UpToDate	UpToDate
<b>HA Status on Peer Machine (AG-10-16-27-70)</b>		
Connection State #0	<b>Connected</b>	
Local Resource Role #0	Secondary	Primary
Disk State #0	UpToDate	UpToDate
Connection State #1	<b>Connected</b>	
Local Resource Role #1	Secondary	Primary
Disk State #1	UpToDate	UpToDate

## Disable High Availability

Perform the following steps to disable the High Availability (HA):

1. Log in to SecDevice GUI using the management floating IP address.
2. Go to **Administration >> Settings**, and click **HA**.
3. Click **Disable HA**.

The page URL changes to **/ha/log** and a text area appears and refreshes during the HA disabling process. Once the disabling is complete, links for SecDevice A and SecDevice B are displayed.

## Upgrade SecDevice High Availability Pair

Perform the following steps to upgrade the SecDevice High Availability (HA) Pair:

1. On Node A (Active Node), perform the upgrade from **consoleadmin** user account. It is recommended to connect to the node through SSH at its management interface IP rather than the management floating IP.
2. Choose to reboot Node A after the upgrade.
3. After Node A is rebooted, Node B becomes Active.
4. After Node B becomes active, perform the upgrade from **consoleadmin** user account. Again, it is recommended to connect to the node through SSH at its management interface IP rather than the management floating IP.
5. Choose to reboot after upgrade.
6. After Node B is rebooted, Node A becomes active.

## Troubleshoot Common High Availability Issues

Perform the appropriate actions to troubleshoot the High Availability (HA) issues:

### Setup Failure during Data Sync Phase

**Cause:**

In HA setup process, data sync from the chosen Active node to Standby node (Peer node) takes place. As part of this process, the content on the disk is shrunk and then the data is replicated on to the secondary node. Once the replication is complete, contents on the disk are restored. In such cases, a setup failure may occur.

## Solution:

- Restore the chosen Active SecDevice node from the backup. For more information, see [Prerequisites](#).
- After the backup is restored on the chosen primary node, HA setup process can be restarted.

## Setup Failure due to Data Corruption

### Cause 1: Undetected Data Corruption

The setup may fail due to undetected data corruption during data sync operation.

## Solution:

Restore the chosen Active SecDevice node from the backup. For more information, see [Prerequisites](#)

### Cause 2: Detected Data Corruption

The setup may fail due to detected data corruption or if any data fails during the data sync operation, the latest data resides on the surviving disk.

## Solution:

The recommended course of action is to take the following steps for recovery:

1. Reset both the nodes to standalone mode.

From **consoleadmin** menu, choose <14> Reset, and then <2> Reset HA to standalone mode. Perform this step on both nodes if possible.

---

**NOTE:** The node with the bad disk may not properly start up.

---

2. Verify the correct functioning of the surviving node.
3. Replace disk(s) on the failed node.
4. Re-install the failed node from ISO.
5. Upgrade this replacement node to the same release(version) as the surviving

node.

6. Perform HA setup from the surviving node.

# SecDevice + Detector (SecDevice Combo)

---

An SecDevice 5000 can be used as one form factor that operates as both an SecDevice centralized management system and a TPS DDoS detector as a virtual machine.

The following topics are covered:

<a href="#"><u>SecDevice Combo Overview</u></a>	392
<a href="#"><u>Internal Detector Set Up for SecDevice Combo</u></a>	394
<a href="#"><u>Upgrading the Internal TPS</u></a>	397
<a href="#"><u>Changing SecDevice Mode</u></a>	397
<a href="#"><u>Using the Detector in an SecDevice + Detector Form Factor</u></a>	399

## SecDevice Combo Overview

The SecDevice Combo is a SKU that requires an SecDevice 5000 hardware, which has built in support for an internal VM instance of a TPS detector. This feature is not available for the virtual form factor of SecDevice. The SecDevice Combo SKU also does not support the SecDevice High Availability feature in versions 3.2.2, 3.2.3, and 3.2.4.

---

**NOTE:** High Availability setup and SecDevice + Detector (combo) features are mutually exclusive.

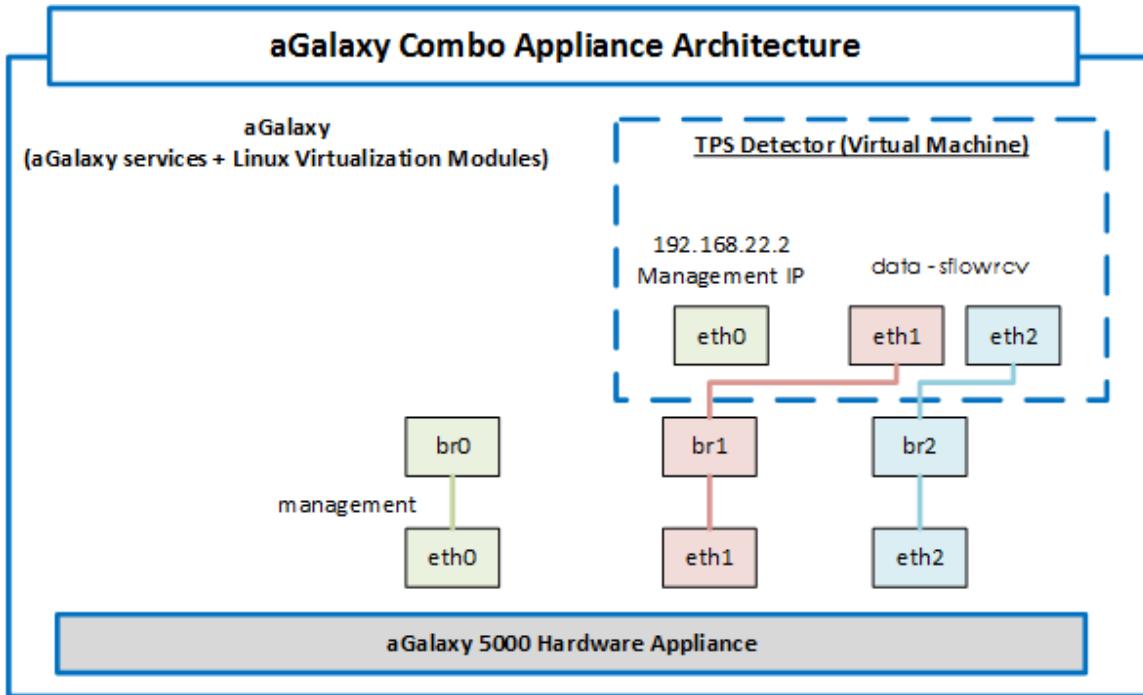
---

## SecDevice Combo Specifications

SecDevice 5000 includes a virtual machine (VM) instance that runs a TPS detector. SecDevice 5000 treats this instance in the same way as other devices managed by SecDevice. The VM instance has 3 interfaces, one which is the management interface with the other two being data interfaces as illustrated in [Figure 45](#). The data interfaces can be configured to receive sFlow from routers.

A limitation of this internal TPS detector is that the management interface cannot be accessed externally. To access the internal TPS detector, follow the [Access the Internal TPS Detector](#) instructions.

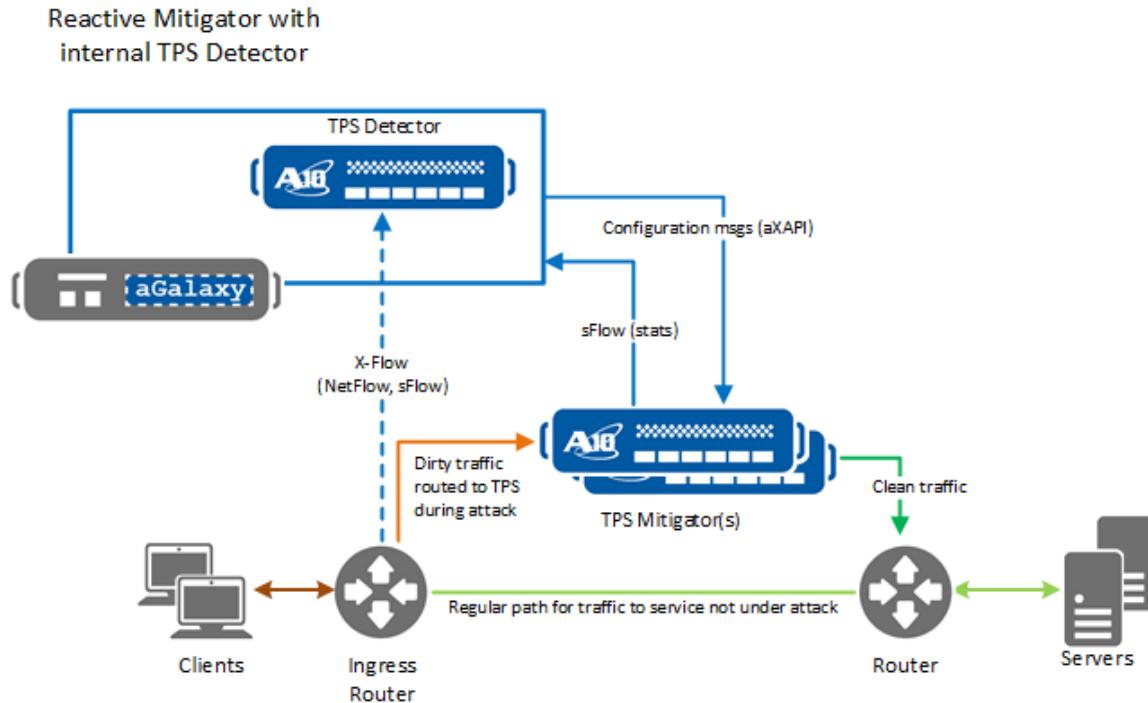
Figure 45 : SecDevice 5000 Combo SKU Appliance Architecture



The internal TPS detector acts in the same way as any other current Organization TPS device in its deployment. An example deployment with A10 Network devices is discussed in [Figure 46](#). The deployment with an SecDevice Combo SKU is the same, with the only difference being that the TPS detector being a VM instance existing within the SecDevice 5000 as illustrated in [Reactive Mitigator with Internal TPS Detector Deployment](#).

The management IP address of the internal is 192.168.122.2 by default.

Figure 46 : Reactive Mitigator with Internal TPS Detector Deployment



## Internal Detector Set Up for SecDevice Combo

The following steps should be taken to set up the internal TPS detector

- [Verify the SecDevice Mode](#) (optional)
- [Access the Internal TPS Detector](#)
- [Configure the TPS Detector](#)

### Verify the SecDevice Mode

From the consoleadmin, the SecDevice mode can be confirmed by doing the following:

1. Login to the SecDevice console using consoleadmin. See the [Consoleadmin](#) section for more information.

2. Select the option of “Switch SecDevice mode”
3. Examine the current mode listed. See [Figure 47](#)

Figure 47 : Consoleadmin - SecDevice+Detector Combo Mode

The screenshot shows a terminal window titled "Consoleadmin - SecDevice+Detector Combo Mode". The window contains a list of numbered options from <1> to <15>, followed by a prompt "Please select the above number: 12". Below this, a message "Current mode is aGalaxy+Detector Combo" is displayed, with the text "aGalaxy+Detector Combo" highlighted and enclosed in a red oval. A secondary menu then appears, asking "Switch aGalaxy mode" and listing three options: <1> Normal mode, <2> aGalaxy+Detector Combo mode, and <0> Exit. The prompt "Please select the above number:" is shown again at the bottom.

```
<1> Change Password
<2> Enable support login
<3> Disable support login
<4> Show support login status
<5> Show services status
<6> Show network
<7> Setup Network
<8> Restart aGalaxy services
<9> Reboot
<10> Shutdown
<11> Upgrade/Backup/Restore/DB Migration
<12> Switch aGalaxy mode
<13> Licensing
<14> Reset
<15> Troubleshooting Options
<0> Quit

Please select the above number: 12

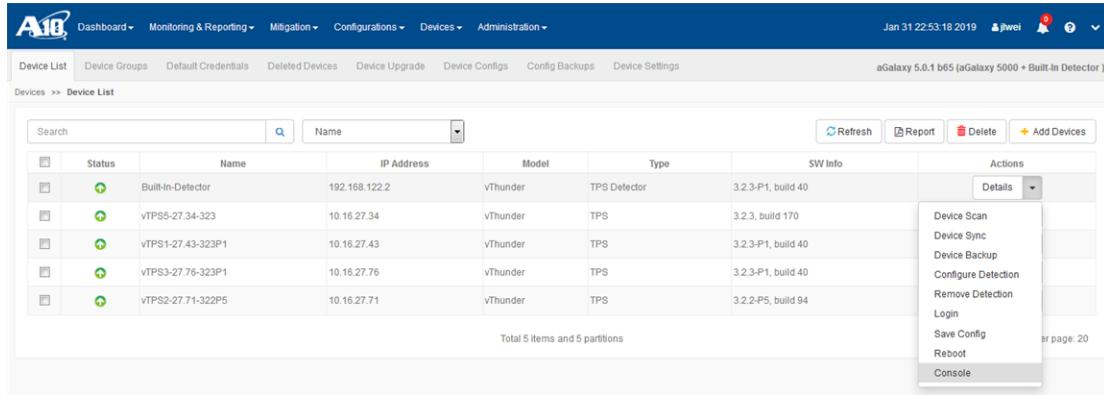
Current mode is aGalaxy+Detector Combo
Switch aGalaxy mode
  <1> Normal mode
  <2> aGalaxy+Detector Combo mode
  <0> Exit
Please select the above number:
```

## Access the Internal TPS Detector

1. Use a web browser to access the SecDevice GUI, and navigate to Devices>>Device List.

The internal TPS detector can be identified by the blue button in the Actions column as shown in [Figure 48](#).

Figure 48 : Identifying the VM instance that is the TPS Detector and accessing Console



- Click on the Actions drop-down list and select Console.

## Configure the TPS Detector

Configure the data port(s) for sFlow by taking the following steps in the console window:

- Login to the device. The username is admin, and the password is a10.
- Go to configuration mode by running the `enable` command. Hit <Enter> for the password.
- Enter the `config` command.
- Configure the data interface(s) using eth1 and/or eth2. Data interface configuration of an IP address is needed for other devices, such as a router, to reach the TPS detector for sFlow.

**NOTE:** Do not configure the management IP address nor the default gateway IP address. These are pre-configured to work with the SecDevice Combo set up.

- Save the configuration using the `write memory` command.

Example:

login as: `admin`

Using keyboard-interactive authentication.

Password:

Last login: Thu Jun 29 23:11:41 2017 from 10.254.107.17

System is ready now.

vThunder> **enable**

Password:

vThunder# **config**

vThunder(config)# **interface eth 1**

vThunder(config-if:ethernet:1)# **ip address xx.xx.xx.xx** <--IP address for sFlow

vThunder(config-if:ethernet:1)# **exit**

vThunder(config)# **write memory**

Building configuration...

Write configuration to primary default startup-config

[OK]

vThunder(config)#

6. From the SecDevice GUI, navigate back to Devices>>Device List, and from the Actions drop-down list for the internal detector, select Edit Detector and configure.

## Upgrading the Internal TPS

The virtual machine image can be upgraded in the same way as any other device by following the [Device Upgrade](#) instructions.

## Changing SecDevice Mode

To change the SecDevice function as either an SecDevice unit or as an SecDevice unit along with a DDoS TPS detector, take the following steps:

1. Open a console and login to SecDevice console using the username consoleadmin and the password a10.
- 

=====

login as: consoleadmin

consoleadmin@xx.xx.xx.xx's password:

Welcome to Organization SecDevice Management System, Version 3.2.2, Build xxx

Last login: Thu Jan 29 17:35:11 2019 from xx.xx.xx.xx

Welcome to Organization SecDevice 5.0.1, Build xxx

<1> Change Password

<2> Enable support login

<3> Disable support login

<4> Show support login status

<5> Show services status

<6> Show network

<7> Setup Network

<8> Restart SecDevice services

<9> Reboot

<10> Shutdown

<11> Upgrade/Backup/Restore/DB Migration

<12> Switch SecDevice mode

<13> Licensing

<14> Reset

<15> Troubleshooting Options

<0> Quit

Please select the above number:

=====

2. Enter 12 to change the SecDevice mode for your SecDevice appliance.

=====

Current mode is Normal

Switch SecDevice mode

- <1> Normal mode
- <2> SecDevice+Detector Combo mode
- <0> Exit

Please select the above number:

=====

3. Select the appropriate option to change the SecDevice mode.

## Using the Detector in an SecDevice + Detector Form Factor

On the SecDevice Graphical User Interface, the detector instance will appear as part of the device list on the Devices >> Device List page. It is identified by the blue button in the Action column, show in [Identifying the VM instance that is the TPS Detector and accessing Console](#).

The internal TPS detector may be configured in the same manner as any other Organization TPS detector.

Note: The management IP address and default gateway IP address configuration of the internal TPS detector should not be changed. These are pre-configured to work with the SecDevice Combo set up.

# Troubleshooting

---

## Recovering from High Availability Failure Events

This section provides guidance on recovering from High Availability (HA) failure events.

The following topics are covered:

## Confirming Scheduled Reports

If a report has been scheduled, and no report appears, use the Job Execution Results page to confirm if the schedule has been completed successfully. To go to the Job Execution Results page, navigate to Administration >> Job Execution Results.

## Failed Report Generation

If you see frequent failed report generation, check to see the number of reports that are being scheduled at the same time. While SecDevice can handle simultaneous report generation, requesting a number of reports simultaneously may result in some failed report generation due to the sudden demand of resources required to handle simultaneous requests.

## Recovering from High Availability Failure Events

This section provides guidance on recovering from High Availability (HA) failure events.

### HA Setup Failure

If a failure occurs during the Distributed Replicated Block Device (DRBD) setup phase, it is recommended that you restore the current SecDevice from an SecDevice backup and restart the process.

### HA Failure Due to Data Corruption

#### Undetected Data Corruption

In cases where an undetected data corruption occurs, attempt recovery from a periodic backup, if one exists.

