Trend Micro™ TippingPoint™

Security Management System (SMS) User Guide

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

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

https://docs.trendmicro.com/en-us/tippingpoint/security-management-system.aspx

Document Part No.: TPEM69835/230927

Release Date: January 2024

Protected by U.S. Patent No.: Pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TippingPoint Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 4: Ports

Chapter 5: Profiles

Chapter 6: Events

Chapter 7: Reports

Chapter 8: Administration

Chapter 9: SMS client dashboard

Chapter 10: Tools

Chapter 11: System preferences

Chapter 12: Responder

Chapter 13: SMS Web Management

Chapter 1

Overview

The Trend Micro™ TippingPoint™ Security Management System (SMS) is the control center for managing large-scale deployments of all TippingPoint products. The main components of the system are the *SMS server*, the *SMS web management console*, and the *SMS client*. The SMS server serves as a management system for multiple devices.

Before you use the SMS server, install and configure the components of the SMS system. You can deploy the SMS as a rack-mountable management server or as a virtual product.

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

SMS interfaces

You can use the SMS client to configure, monitor, and report on all of the TippingPoint devices in your network from a single interface.

The SMS server includes the following interfaces:

- SMS web management console – Web-based interface from which you can install or upgrade SMS client software, monitor the TippingPoint devices installed on your network, access Threat Insights, and examine the operational, security, and performance contexts of your filters so that you can fine-tune your profiles for maximum security effectiveness.

  You can review the SMS system log, exported and archived files, or saved reports. You can also access certain SMS web management console features from your mobile devices and tablets. Learn more: *SMS Web Management on page 13-1*.

- SMS client – Java-based application for Windows, Linux, or Mac workstations. The SMS client consists of a graphical user interface that enables you to manage the TippingPoint system.

- Command Line Interface (CLI) – Text-based interface that enables users with SuperUser rights to log in to and configure the SMS server.

SMS components and services

At the core of the SMS is the ability to create multiple profiles, which can be distributed to specific devices. A *profile* is a collection of filters or rules that enable you to set up security configuration options for TippingPoint solutions.

Using profiles, you can distribute filters to multiple devices, specific devices, physical segments controlled by a specific device, or even virtual segments. The maximum number of devices that one SMS can manage depends on usage, network, and other environmental conditions.

When a profile is distributed, it includes shared settings such as action sets, notification contacts, and services, as well as associated filters and filter setting modifications. The SMS web management console enables you to examine the context of how filters are used in your security profiles. This

interface flags filters according to certain criteria, such as traffic congestion and vulnerabilities to new threats, so that you can make adjustments to your profile for optimal performance. Learn more.

When you organize devices in groups or security zones, you simplify how security profiles are updated and distributed. You can also configure the SMS to regularly update all managed devices with the latest TippingPoint Operating System (TOS) software and Digital Vaccine and malware filter packages.

The SMS interacts with the following services:

- ThreatLinQ – TippingPoint service that works with the TMC to collect and analyze security information.
- Smart Protection Network (SPN) – Repository that collects the global security intelligence from all Trend security products. SPN compiles a list of the top threats and, in conjunction with Digital Vaccine information, refines that list further so users can align their profile strategies to their most relevant threats. The Threat Management Center (TMC) distributes this list of recommended threats.
- Digital Vaccine and ThreatDV– Services that include the latest filter packages for protecting your network against software vulnerabilities and malware.
- Threat Management Center (TMC) – Centralized service center that monitors global threats and distributes up-to-date attack filter packages and software updates.

Chapter 2

API

Trend provides two types of APIs for use with the SMS.

- The *SMS Web API Guide* describes HTTP APIs you can use to access multiple SMS features if you have HTTPS service to the SMS. To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Chapter 3

Devices

The Devices screen provides a dynamic view of your entire system, graphically depicting TippingPoint devices under SMS management, their segments, and the hosts and services on those segments.

When you assume management of a device, you can control networking configuration, virtual segments and segment groups, filters and customizations, and distribution of filters and software. You can also monitor traffic processing, health, and hardware status on each device and its segments.

Note

When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities. See *Authentication and authorization on page 8-15*.

All devices

The All Devices view displays images that represent each TippingPoint device that has been added to the SMS, indicating whether the device is currently managed or unmanaged.

Each image displays the name of the device or component, status indicators, networking information, and other details.

Column	Description
Name	Device name.
IP	IP address used to make a connection to the device.
Model	Device model.
System Health	Health status indicator that provides information about the hardware components of the device.
Performance	Performance status indicator that provides top-level information about the device.
Port Health	Port health monitoring indicator that tracks key port statistics for the device.
TOS	TippingPoint Operating System (TOS) software package version installed on the device.
Digital Vaccine	Active Digital Vaccine version number.

Device details

Device details provide a consolidated view of information and configuration settings for an individual device managed on the SMS. You can adjust how devices are represented in the All Devices area by:

- **Large details** - System health, performance, and port health status indicators appear next to the device icon. The image also includes the device model, IP address, and system name.

- **Large** - System health, performance, and port health status indicators appear next to the device icon. The image also includes the device model, IP address, and system name.
- **Medium** - Device icon displays the same information as the large device icon, but smaller.
- **Small** - System name is displayed to the right of the device icon.

In the Devices view, unread notifications are indicated by a number icon that is displayed in the bottom-left of the icon. If the notification icon is gray with no number, there are no unacknowledged notifications for the device.

To view device details, select **Devices** > **All Devices**, and then double-click a device icon.

Column	Description
Component	Name of the device component, such as model, license, software, and segments.
Type	Type of component, such as chassis or copper port.
System Health	Health status of the device. **Note** For IPS NX-Platform and TPS TX Series and TXE Series devices, system health displays details about the fans and power supplies. If the System Health indicator displays an error or issue, you can review the System Log for information on these health events. See *Events (all devices) on page 3-13*.
Details	Status details or description.

View, edit, or delete device distribution queue

SMS supports queuing of any package distributions to an IPS or TPS device. The types of packages that can be distributed to a device include:

- TOS

- Profile
- Digital Vaccine
- Threat DV
- Digital Vaccine Toolkit

The queuing of distributions to a device allows you to start a distribution of different packages to the same device. Distributions are placed in the device distribution queue and displayed in table format.

Queued distributions are processed when the device is available and in a normal communication state. Each device has one queue and can contain any of the available distribution types. The order in which the distributions are added to the queue is maintained and can be changed.

Procedure

1. Select **Devices** > **All Devices** > **device**, expand the device options, and then select **Distribution Queue**.
2. The Distribution Queue table lists all the packages in the queue and the following information about each queue:
   - **Order** — Number represent the sequential order of the distribution.
   - **Distribution Type** — Type of distribution.
   - **Package** — Name of the package and the version that is being distributed.
   - **Time Entered** — Time distribution was started.
   - **Status** — Waiting in queue or in distribution.
3. To change the order of the entries, select an entry, and click **Move-Up** or **Move-Down**.
4. To delete an entry, select an entry, and then click **Delete**.

Add a new device

A device must be installed and powered on before you can add it on the SMS. After you add a device, it is under the exclusive control of the SMS. If you want to make any local configuration changes using the device CLI, you must unmanage the device first. After you add a device to the SMS, you can unmanage and re-manage the device without having to delete it on the SMS.

You must have SuperUser privileges to use this feature. Learn more: *User roles and capabilities on page 8-39*.

Procedure

1. Select **Devices** > **All Devices** > **New Device**.
2. Select one of the following:
   - **Add Device(s)**, and enter the device IP Address. To add multiple devices, separate each device IP address with a comma.
   - **Add Multiple Devices Using a File**, and click **Browse**. The text file must contain one valid IP address per line, or a comma-delimited list of valid IP addresses.
3. Enter the **Username** and **Password**. If you add multiple devices, every device must use the same authentication credentials.
4. Select a **Device Group**. If you add multiple devices, every device must be in the same device group. SSL devices cannot be added with other devices. See *Create or edit a device group on page 3-9*.
5. Select a **Device Type**.
6. Select the appropriate **Segment Group** entry from the drop down box.
7. Click **Options**, and then select options to:
   - **Synchronize Device Time with the SMS**.
   - **Configure the Device**, which will launch the Device Configuration after the new device is added.
   - **Clone an Existing Device** to copy specific device settings (available settings vary according to device model).

8. Click **OK**.

   When a device is successfully added to the SMS, the device appears under **All Devices**.

Note

When you add a TPS or vTPS device, always distribute an inspection profile to every defined segment on that device to begin protecting network traffic. By default, when you add a vTPS or TPS device, all filter categories are set to Recommended in the default profile.

Clone a device

Clone an existing device configuration to pre-configure a completely new device.

Procedure

1. Add a new device, and select the **Clone an existing Device** option.
2. Select a device from the **Device to clone** drop-down list.
3. Select one of the following:
   - **Select All Settings** to copy all settings from the cloned device.
   - Select **Device Settings**, and then select options for:

     The following device settings cannot be copied from the cloned device: Management Information, Management Network, Management Routes, NAT, and Host IP Filters.

NX-Platform device settings	TPS device settings
Services: • SSH • Telnet • Encrypted alert channel • Port data retrieval services • SNMP version	Services: • SSH • TLS settings
AFC	AFC
Performance protection	Performance protection
NMS	-
-	SNMP
-	Log configuration
-	Data security
Remote syslog	Remote syslog
Servers: • Email	Servers: • Email
Time	Time
TSE: • Connection table • Quarantine • Asymmetric network • HTTP response processing • GZIP decompression • DNS Reputation • IDS mode	TSE: • Connection table • Quarantine • Asymmetric network • HTTP response processing • GZIP decompression • DNS Reputation • HTTP mode • IDS mode

NX-Platform device settings	TPS device settings
Authentication preferences	Authentication preferences
Remote authentication	Remote authentication
Login banner	Login banner
sFlow®	-

4. Click **OK**.

Edit a device

When editing devices, note the following:

- During a multiple-devices edit, FIPS Settings are not available and will not display on the Device Configuration.
- Remote authentication for TPS devices is not supported as part of a multiple-device update.
- During a multiple-devices edit, setting a RADIUS or TACACS+ server as the Remote Authentication or changing one of these servers only updates IPS devices that support those types of remote authentication (for RADIUS authentication, N-Platform or NX-Platform devices running TOS v3.7.0 or later; for TACACS+ authentication, N-Platform or NX-Platform devices running TOS v3.8.0 or later).
- The RADIUS and TACACS+ options and the RADIUS Servers and TACACS + Servers sections are displayed in Authentication Preferences only if at least one of the managed devices supports RADIUS and TACACS+ authentication. Devices that do not support these remote authentication options do not get updated.
- If you replace an IPS device with a TPS device, any configured TACACS servers for the replaced IPS device become a TACACS group in the TPS device.

Procedure

1. Select **Devices** > **All Devices**.
2. Select the devices to edit, and then click **Edit**.
3. Use the Device Configuration to make any device changes. The Devices Being Modified lists every device that is being modified.

Create or edit a device group

Create device groups to organize and manage multiple devices at the same time. Each device group displays its own member summary information. For more information, see *Member summary on page 3-12*.

Procedure

1. Select **Devices** > **All Devices**.
2. To create a device group, do one of the following:
   - Right-click in the **All Devices** area, and select **New Device Group**.
   - Select two or more device icons, right-click and select **New Device Group**.
   - Select **File** > **New** > **Device Group**.
3. Enter a name for the device group.
4. Select a parent group from the **Add to Device Group** list. If you delete a device group, the member devices move to the parent group.
5. Click **OK**.

Manage a device

While a device is being managed, you can control device configuration, software updates, profile distribution, and filters through the SMS client. SMS management overrides any local device use and configuration.

If you want to manage a device, the device must be configured to allow SMS control.

Procedure

1. Select **Devices** > **All Devices**.
2. Right-click on an unmanaged device, and click **Manage Device**.
3. Provide the username and password for the device.
4. Click **Manage**.

Unmanage a device

Unmanaging a device returns control of the device to the device itself.

You cannot unmanage a device while it is receiving or distributing a software or security package.

Note

You must have Administrator access on the SMS to unmanage a device.

Procedure

1. Select **Devices** > **All Devices**, and then select a managed device.
2. Click the **Edit** menu and select **Unmanage Device**.
3. Click **Unmanage**.

   In the navigation pane and in All Devices area, the device icon is overlaid with a red X, which indicates that the device is no longer being managed.

Remanage multiple devices

Remanage multiple devices, device groups, or a combination of both at the same time. If you are remanaging several devices at the same time, the SMS will process them as a single batch of up to five devices.

Procedure

1. Select **Devices** > **All Devices**.
2. Right-click on two or more unmanaged devices, and click **Manage Devices**.
3. Provide the username and password for the device or device group. Every device/device group must use the same authentication credentials.
4. Review the list of devices that are currently managed and devices that will be managed on the Bulk Remanage Summary page, and click **Finish**.

Replace a device

The SMS provides a convenient option that allows you to replace an existing device and have the new device function exactly the same as the old device. If you are replacing the same model with another model and both devices have the same TOS, the one-to-one replacement is straightforward. There are certain limitations based on the device features. For example, If you replace an IPS device that supports DDoS with an IPS device that does not support DDoS, data might be lost.

When you replace a device, the events from the previous device are preserved. However, previous installed TOS versions, rollback versions, and snapshots are reset using the new (replaced) device as a starting point.

Procedure

1. Remove the replacement device from the box and complete the Out of Box Experience (OBE) instructions using the old IPS address for the new one.
2. Select **Devices** > **All Devices**, choose the device to be replaced, and then select **Edit** > **Details** > **Replace Device**.
3. After Devices - Replace Device dialog displays, enter the information for the new IPS device, and then click **OK**.

If all of the supplied information is correct, the models are the same and the TOS versions are the same, a progress dialog appears. When the replacement process is complete, a dialog appears and directs you to redistribute the appropriate versions of the IPS profiles.

Delete a device

Delete a device to permanently remove it and its related managed objects from the SMS. The SMS retains historical data unless you choose to delete it as well.

Procedure

1. Select **Devices**, and click the device you want to remove.
2. Click the **Edit** menu, and select **Delete**.
3. In the Delete Selected Device dialog, click **Delete**.

Member summary

For a top view of configuration settings for all managed devices, expand **All Devices**, and then select **Member Summary**. The Member Summary screen lists managed devices on the SMS including specific configuration information. Tabs on this screen correspond with **Device Configuration**:

- Management Information
- Management Routes
- Services
- High Availability
- Servers
- Remote Syslog Servers
- Time Settings
- TSE Settings

Network summary

The Network Summary page provides a global view of all physical segments, ports, and interfaces for all devices managed on the SMS.

To access the Network Summary information, select **Devices** > **All Devices** > **Member Summary** > **Network Summary**, and then select a tab.

Additional network configuration information is available through the Network Configuration feature for a specific device, see *Network Configuration on page 3-32*.

To edit segment and port properties, select the appropriate tab, select a device, and then click **Edit**. You can also access network configuration options by expanding the entries for a specific device from the left navigation pane and then selecting **Network Configuration** for that device.

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

Events (all devices)

The Events page provides a global view of event information for all devices managed on the SMS. To access and search for global device events, select **Devices** > **All Devices** > **Member Summary** > **Events**, and then select the tab associated with the event you want to view.

For information on viewing events for an individual device, see *Device details on page 3-2*.

View, search for, and flush Blocked and Rate Limited Streams

Blocked Streams display connections blocked by filters. Rate Limited Streams display connections rate limited by filters. Both tabbed screens display the 5-tuple for each stream, including the protocol, source IP address, destination IP address, source port, and destination port.

The Blocked Streams and Rate Limited Streams tabs provide the following information:

Option	Description
Device	Device name.
Protocol	Protocol of the blocked or rate limited stream.
Src/Dest Address	Source IP address, destination IP address.
Port	Port address.
Slot	IO slot from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 5500TX, 8200TX, and 9200TXE devices. IO slot 1 for TPS 1100TX devices.
Segment	IP address of the segment.
Profile	Name of the profile for the filter triggered.
Reason	Reason for the blocked stream.

Procedure

1. Select **Devices** > **All Devices** > **Member Summary** > **Events**, and then select the **Blocked Streams** or **Rate Limited Streams** tab.
2. Search for a stream by selecting:
   - Protocol
   - Source or destination IP address
   - Port number
3. To flush selected streams, select entries, and then click **Flush Selected**. This only removes the blocked streams selected from the list of displayed entries.
4. To flush all Blocked or Rate Limited Streams, click **Flush All**. This removes all blocked streams (including blocked streams not displayed) from the connection table. The effect is as though the blocked streams all timed out at the same time.

View, search for, and flush Trusted Streams

The Trusted Streams table provides the following details:

Entry Title	Description
Device	Device name.
Protocol	Protocol of the blocked or rate limited stream.
Src/Dest Address	Source or Destination IP address. Click the plus symbol (+) in the Src/Dest Address columns to display additional information, including Geography, Region, City, and Named Resource.
Port	Port address.
Src/Dest Address	Source or Destination IP address.
Port	Port address.
Slot	IO slot from 1 to 4 IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 5500TX, 8200TX, and 9200TXE devices. IO slot 1 for TPS 1100TX devices.
Segment	IP address of the segment.
Source Interface	Specific source interface.
Destination Interface	Specific destination interface.
Profile	Name of the profile for the filter triggered.
Reason	Reason for the trusted stream.

Procedure

1. Select **Devices** > **All Devices** > **Member Summary** > **Events**, and then select the **Trusted Streams** tab.
2. Search for a stream by selecting:
    - Protocol

- Source or destination IP address
- Port number

3. To flush selected streams, select entries, and then click **Flush Selected**. This only removes the trusted streams selected from the list of displayed entries.
4. To flush all Trusted Streams, click **Flush All**. This removes all streams (including trusted streams not displayed) from the connection table. The effect is as though the trusted streams all timed out at the same time.

View, search for, and unquarantine Quarantined Hosts

You can unblock IP addresses quarantined by filters. The quarantine option for action sets blocks IP addresses that trigger associated filters. When a filter with a quarantine action triggers, the system places a block on the IP address for a set amount of time unless manually flushed. Depending on the settings of the action set, the user might receive a message or be rerouted to a Web page detailing the reason for the blocked traffic.

The Quarantined tab provides the following information:

Option	Description
Device	Device name.
Host Address	Quarantined IP address.
Slot	I/O slot.
Segment	Segment the IP address is quarantined on.
Profile	Name of the profile for the filter triggered.
Filter	Name of the filter that triggered quarantine.

Procedure

1. Select **Devices** > **All Devices** > **Member Summary** > **Events**, and then select the **Quarantined Hosts** tab.

2. Search for a host IP address.
3. To unquarantine, select entries, and then click **Unquarantine**.
4. To unquarantine all, click **Unquarantine All**.

View AFC filters

View a list of the filters that were most recently affected by adaptive filtering. IPS devices display the ten most recent filters. TPS devices display the twenty-five most recent filters.

The Adaptive Filter List provides the following information:

Option	Description
Device Name	Device name.
Filter Type	Security or Application filter.
Filter Name	The name of the filter being managed by the adaptive filter function. Learn more: *Adaptive filtering on page 5-24*.
Filter State	• Enabled — When selected, this indicates that the filter was once disabled by AFC, cleared by a user, and is now enabled in the engine and will execute the associated action set. Learn more: *Action sets on page 5-3*. • Disabled — If the checkbox is not selected, then this filter has been uninstalled from the engine by the adaptive filter function.

The device automatically takes a traffic capture when a filter enters AFC. After you clear the filter state, it might still appear on the Adaptive Filter List so that you can download the associated packet capture (PCAP) file. Learn more: *Traffic capture on page 3-22*.

Procedure

1. Select **Devices** > **All Devices** > **Member Summary** > **Events**, and then select the **Adaptive Filter** tab.
2. To clear the AFC state on a filter, select the filter(s) and then click **Clear Selected Filters**. This re-enables the selected filter states. This option is

available on IPS devices running any supported TOS, and on TPS devices running TOS version 5.1 and later.

3. To clear the AFC state on all the device filters, click **Clear All**. This re-enables every filter state on the device. This option is available only on TPS devices running TOS version 5.1 and later.
4. To change the AFC setting on a filter, *edit the filter on page 5-50*.

System health (all devices)

The System Health screen provides information on the hardware components of a device including memory, temperature, file system, and license throughput utilization. To access system health, select **Devices** > **All Devices** > **Member Summary** > **System Health**.

Note

For IPS devices only, top-level indicators can be configured. For more information, see *Health thresholds on page 3-45*. You cannot reset health threshold preferences for TPS devices.

Additional system health information is available through the Events feature for a specific device. For more information, see *Events on page 3-42*.

Performance (all devices)

The Performance page provides a global view of the number and status of packets processed by the device since boot time, and the CPU percentage.

To access Performance information, select **Devices** > **All Devices** > **Member Summary** > **Performance**.

Packet statistics

Packet statistics displays the number of packets processed by the device since boot time in the terms displayed in the following table.

Click **Reset** or **Reset All** to reset the counters. Click **Refresh** to display current values.

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

CPU

CPU displays the state and performance value expressed as a percentage. Click **Refresh** to display current CPU values.

Device users (all devices)

The SMS allows superusers to create and edit multiple device users across many devices. In addition to assigning usernames and passwords, superusers can specify whether device users authenticate locally or whether they use a remote server, such as RADIUS or TACACS+, to authenticate.

How a device user authenticates indicates the user's role and reflects the authentication preferences in the device configuration.

To change the password, the **New Password** and **Confirm Password** fields must be changed. To change the role, select the radio button associated with the appropriate role.

To access this feature, navigate to **Devices** > **All Devices** > **Member Summary** > **Device Users**.

The Device User Accounts screen displays a table that lists the user accounts available on managed devices and enables you to create and edit user accounts.

If the **Show All Devices** check box is selected, actions can be performed on all devices. If the check box is not selected, only the user accounts on devices in the current group are displayed.

Table heading	Description
State	Enabled or disabled state of the user account associated with the device.
Name	Unique identifier for the user account on the device.
Role	Access level assigned to the user.
Group	Group assigned to the user.
Password Expiration	Number of days until the password expires.
Auth Type	Indicates whether the user authenticates locally or remotely (through RADIUS or TACACS+).
Family	Displays the family name of the managed device.
Device	Unique name associated with the device.

Device users actions

The Device Users screen provides the following actions:

- **Copy** — Allows the user to select which devices receive a copy of the selected device users. This option is disabled when no users are selected or the user is not authorized to manage user accounts for devices. Use the following authentication guidelines when copying users:
  - Provide and confirm a password for users who require local authentication.
  - When you copy only users who use remote authentication, the New Password and Confirm Password fields are disabled. In addition, these users can only be copied to devices that support RADIUS or TACACS+ authentication. Devices that do not support RADIUS or TACACS+ are disabled in the device selector panel.

- When you copy users who use local authentication mixed with users who authenticate remotely, only users who match the current authentication type configured for the device can be authenticated. For example, if the current authentication type is RADIUS, only RADIUS-authenticated users can be authenticated on the device. All devices are selectable and a password is required. The password is ignored for RADIUS and TACACS+ users that get copied to devices that support remote authentication servers. Attempts to copy RADIUS and TACACS+ users to a device that does not support these servers return a confirmation dialog, prompting you to confirm the action. If you decline, the operation is aborted. If you confirm the operation, the user is copied to the non-RADIUS device as a local user, and the password requirement applies.

- **Enable** — Enables a user account for a specified device. A device user might be in a disabled state due to too many failed login attempts or a failure on the part of the user to perform a required password update.

- **New/Edit** — Create or edit a user account for a specific device. Each device user consists of a User ID, password, the role performed by that device user, and the user's authentication method. When creating a new device user the User ID field must be unique for the device. The User ID cannot be edited. Use the following authentication guidelines when creating or editing users:

  - If RADIUS or TACACS+ is selected as the authentication method for a new user, only devices that support those servers are selectable, and the New Password and Confirm Password fields are disabled. Only users who use local authentication require a password.

  - When editing multiple users across multiple devices, the preselected authentication method matches the authentication method of all the users if they authenticate in the same way.

  - When you edit users with a mix of authentication methods, a No Change authentication is preselected and an automatic password is generated. Changing the password will apply only to local users. Changing authentication from No Change to Local clears the automatic password and requires a new password. Changing

authentication from No Change to RADIUS or TACACS+ impacts only devices that support those servers.

- **Delete** — Delete the specific device users. Multiple device users can be deleted at the same time.
- **Refresh** — Refresh all device user accounts. Refresh the device user accounts after you create or update a device user account.

Traffic capture

Traffic capture allows permitted users to view and manage traffic capture files residing either on the SMS or on a managed device. A traffic capture file contains one or more packets captured by a device on a single segment or all segments.

To access all captures from all devices in a device group, select **Devices** > **All Devices** > **Member Summary** > **Traffic Capture**.

Select the **Show All Devices** check box to see all device groups. Traffic capture files are saved in packet capture (PCAP) file format and support either an internal or external viewer.

Concurrent traffic capture

The SMS allows multiple captures to run concurrently. Traffic capture files are created by the device at the request of a user through SMS. After traffic captures are manually stopped, the traffic capture files move from the device to the SMS if they were created from the SMS or if the user wants to work with the file.

Packet capture summary information and management options can be accessed in the following areas:

- All Devices — **All Devices** > **Member Summary** > **Traffic Capture**
- Device Groups — **All Devices** > **[device group]** > **Member Summary** > **Traffic Capture**
- Device — **All Devices** > **[device]** > **Traffic Capture**

To display traffic captures for all devices, select the **Show All Devices** option on the Traffic Capture summary screen for **All Devices** or **Device Groups**.

Traffic capture expressions (based on TCPDump) are used in traffic captures to refine the types of packets that are captured. The following table outlines the use of traffic capture expressions:

Note

You can use the ampersand (&) operator to concatenate parameters. Do not use the “or” operator.

Create a new traffic capture file

Traffic capture enables permitted users to view and manage traffic capture files residing either on the SMS or on a managed device. A traffic capture file contains one or more packets captured by a device on a single segment or all segments.

Users can see the files for only one device at a time. Traffic capture files are saved in PCAP format and support either an internal or external viewer. Traffic capture files on the SMS are placed in the backup restore area of the SMS drive. Traffic captures placed on an SMS are not sent to the secondary HA system.

Procedure

1. Select **Devices** > **All Devices**, select a device and then select **Traffic Capture**.
2. In the Current Traffic Capture area, click **New** to create a new traffic capture.
3. In the New Traffic Capture dialog, specify the following information:
   - **Name** — Name of the new traffic capture file.
   - **Segment** — Segment on which traffic is captured.

Note

The IPS (NX Series) and TPS (TX Series) device segments indicate slot number and segment number.

- **Maximum Packets** — Maximum number of packets of the capture file (from 1 to 10,000 packets).
- **Maximum File Size** — maximum size of the capture file (from 1 to 10,000,000 bytes).
- **TCPDump Expression** — Expression based on standard TCPDump parameters that refines the types of packets that are captured.

Note

When you want to capture MAC-in-MAC (IEEE 802.1ah) traffic, keep the following points in mind:

- Device support for MAC-in-MAC is limited to the TPS 8200TX and 8400TX devices.
- You can verify the device recognizes MAC-in-MAC traffic by running the `debug np stats show npParseStatsInst` CLI command on the device or by taking a packet capture. When you configure the packet capture, specify a TCPDump expression that identifies the Backbone MAC address (B-MAC) or Backbone VLAN identifier (B-VID) of the traffic you want, or capture all packets for particular segment.

4. Click **OK**.
5. (Optional) Click **Stop** to stop all current traffic capture on the devices. A confirmation message is displayed.
6. (Optional) Click **Refresh Statistics** to refresh the current traffic capture statistics.

Existing captures

Existing Captures provides a listing of existing captures.

Column	Description	Type
Name	Name of the new traffic capture file.	Current, Existing
Date	Date of the traffic capture.	Current, Existing
Slot	I/O slot (from 1 to 4 for NX and 8400TX devices; from 1 to 2 for 5500TX, 8200TX, and 9200TXE devices; 1 for 1100TX devices)	Current, Existing
Segment	Segment on which traffic is captured.	Current, Existing
File Size	Size of file from 1 to 10,000,000 bytes.	Current, Existing
Packets	Number of packets from 1 to 10,000 packets. For TPS devices, this value will always be N/A.	Current
Device	Name of the device.	Current, Existing
On Device	File status on the device. A check mark indicates the traffic capture file is present on the device.	Existing

Export a traffic capture file

Export a traffic capture from the SMS. Traffic capture files on the SMS are placed in the backup restore area of the SMS drive. Traffic captures placed on an SMS are not sent to the secondary HA system.

Procedure

1. Select **Devices** > **All Devices**, select a device and then select **Traffic Capture**.
2. In the **Existing Captures** table, select a listing, and then click **Export**.
3. In the **Save File** dialog box, navigate to the desired location, specify a name for the file, and then click **Save**.

Transfer traffic capture files to the SMS

Transfer traffic captures to the SMS.

Procedure

1. Select **Devices** > **All Devices**, select a device and then select **Traffic Capture**.
2. In the **Existing Captures** table, select a listing that has a capture file on the IPS device (indicated with a check mark in the **On Device** column).
3. Click **Transfer to SMS**.

Traffic capture expressions

Traffic capture expressions are used to narrow down the types of traffic that are captured. This feature supports true tcpdump expressions. For more information about expression usage, refer to external tcpdump and libpcap documentation.

To capture only TCP traffic enter the following expression in the **Expression** field:

```
tcp
```

The following example captures IPv4 HTTP packets that are transmitting to and from port 80 and only includes packets that contain data. SYN, FIN, and ACK packets are excluded.

```
tcp port 80 and (((ip[2:2] - ((ip[0]&&0xf)<<2)) -
((tcp[12]&&0xf0)>>2)) != 0)
```

Parameter	Description
ip	IPv4 traffic. By default, only IPv4 traffic is captured.
ipv6	IPv6 traffic.
proto	Designates the protocol of captured traffic. Can be an explicit number or **tcp**, **udp**, or **icmp**.

Parameter	Description
src	Specifies the source of the traffic. This parameter can be applied to both host and port.
dst	Specifies the destination of the traffic. This parameter can be applied to both host and port.
host	Designates a host IP address. IPv4 and IPv6 addresses are supported, as is CIDR format.
port	Designates the port; you must also specify a port number.
Examples:	
`host 172.31.255.254`	Captures all traffic to and from 172.31.255.254.
`src 172.31.255.254`	Captures all traffic from 172.31.255.254.
`dst 172.31.255.254`	Captures all traffic to 172.31.255.254.
`src 172.31.255.254 & dst 10.10.10.10`	Captures all traffic from 172.31.255.254 to 10.10.10.10.
`ip proto tcp`	Captures only TCP traffic.
`ip proto tcp & src port 63`	Captures only TCP traffic on port 63.

Inspection bypass

Through the Events screen for IPS (N-Platform or NX-Platform) and TPS devices, you can create and manage Inspection bypass rules that are a set of criteria used to determine if a given packet should be routed through the device without further inspection.

Inspection bypass is available for TippingPoint IPS (2500N, 5100N, 6100N, and NX-Platform) and TPS devices. vTPS devices are not supported. Because TPS devices perform inspection bypass only at the BCM (switch) level, some inspection bypass rules that you might have previously employed on NX-platform devices (which can also apply bypass rules at the FPGA level) will not work on TPS devices. Contact your support representative for information on how to determine whether other solutions, such as traffic

management rules, can serve as a workaround. For example, one workaround is to use the custom Ethernet type 8847 and 8848 for MPLS traffic.

The maximum number of bypass rules is 8 for IPS devices and 32 for TPS devices.

Entry Title	Description
ID	Reference ID of the rule in the listing.
Enabled	Enable/disabled status.
Name	Name of the bypass rule. Inspection bypass rule names should be unique. The name is an SMS-only feature and does not appear on the managed device.
Ethernet Type	Type of Packets that are exempt from traffic based on the Rules criteria: • IP — Type of IP packets that are exempt. • Not IP — All non-IP packets that are exempt from inspection. • Protocol — Packets from a specified protocol that are exempt.
IP Protocol	Transport layer protocol of packets to exempt from inspection.
Statistics	Number of packets that match a bypass rule.
Src IP	Source IP address of packets to exempt from inspection.
Src Port	Source port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the **IP Protocol** field.
Dst IP	Destination IP address of packets to exempt from inspection.
Dst Port	Destination port of packets to exempt from inspection. This field is valid only if TCP or UDP is specified in the **IP Protocol** field.

Entry Title	Description
Action	Action that the rule applies to the traffic. (TPS devices only) • Bypass (default) – Bypasses the traffic. • Block – Blocks the traffic. • Redirect – Redirects the traffic. A **Target Port** field (required) is displayed for you to specify which segment port the traffic gets redirected to. This option is unselectable if no target port is available. • Ingress mirror – Mirrors (copies) traffic entering the port to another segment port before the traffic gets inspected. A **Target Port** field (required) is displayed for you to specify which segment port the traffic gets mirrored to. Four mirror-to-port (MTP) configurations are supported. This option is unselectable if no target port is available. • Egress mirror – Mirrors (copies) inspected traffic exiting the port to another segment port. A **Target Port** field (required) is displayed for you to specify which segment port the inspected traffic gets mirrored to. Four MTP configurations are supported. The port-assigned Virtual LAN (VLAN) is recorded inside the captured packet. This option is unselectable if no target port is available.

Configuring Inspection Bypass Rules includes the following areas:

- **Name** — Descriptive name and enabled state option.
- **Action** — Action that the rule applies to the traffic.
- **Protocol** — Ethernet frames that match these settings and the settings specified for VLAN are delivered directly to the other side of the IPS segment. They are not routed for inspection.
- **VLAN** — Configure the VLAN tag. Ethernet frames that match these settings and the settings specified for Protocol are delivered directly to the other side of the Device segment. They are not routed to an iLink for inspection.
- **Segments** — Segments with traffic that are subject to the Inspection Bypass Rule.

Create or edit an inspection bypass rule

Before you configure an inspection bypass rule, you must distribute a profile to the segment.

Procedure

1. Select **Devices** > **All Devices**, select a device that supports inspection bypass, and then select **Inspection Bypass**.
2. Click **New** to create a new rule, or select an existing rule and click **Edit**.
3. In the Inspection Bypass Rule wizard, select **Name** from the left navigational menu.
4. Specify a **Name** for the exception rule and then indicate the desired **Enabled** status for the rule.
5. (TPS devices) Click **Next** or select **Action** from the wizard navigation pane to specify the **Action** to be performed on the traffic.

   For a description of the available actions, see *Inspection bypass on page 3-27*.
6. Click **Next** or select **Protocol** from the wizard navigation pane.
   - Select the Ethernet Type.
   - For IP Protocol, specify the Source/Destination ports and addresses.
7. Click **Next** or select **VLAN** from the wizard navigation pane. By default VLAN tag, MPLS label, or tunneling checks are NOT performed.
   - To match all frames, do not select the **VLAN** check boxes.
   - (N-Platform and NX-Platform devices only) To exempt frames from inspection, select the **VLAN** or **MPLS** option and define the value or range of frames.

     If you select **None** for VLAN and MPLS, the device only matches traffic that has both.
   - (N-Platform and NX-Platform devices only) To exempt tunneling frames from inspections, select the appropriate options (**GRE, MIPv4, IPv6in4**) and select an option (**Any, Present, Absent**).

8. Click **Next** or select **Segments** from the wizard navigation pane and then select the segments where the inspection bypass rule should be applied.

Note

For NX series and TX Series devices, the segments are listed by slot numbers.

9. Click **Finish**.

I/O module replacement – TPS (TX Series/TXE Series)

On a TPS TX Series or TXE Series device, *hot swapping* allows you to add, remove, or replace an I/O module without shutting down the device. When the device is turned on, you can hot swap an I/O module without interruption to the TPS device.

Note

Hot-swapping I/O modules during system initialization is not supported.

When you hot swap an I/O module, keep the following points in mind:

- The module port configuration is always reset.
- The module segment configuration, including Link Down Synchronization, Intrinsic HA, and inspection bypass, is always preserved.
- The second slot of the 5500TX device supports only the first four segments of a 6-segment I/O module.

When the device is turned off, *cold swapping* allows you to add, remove, or replace an I/O module as you would when you hot swap. However, when you cold swap an I/O module, if the replacement module type is the same, the module port configuration is preserved.

When the device is managed by the SMS, a delay of up to 1 minute can occur before the SMS recognizes the changed I/O module.

Note

When you insert a bypass I/O module, the bypass I/O module always starts up in bypass mode. A bypass I/O module remains in bypass mode until you remove it from bypass mode. To change the module from bypass mode to normal mode using the SMS, click the device and select **Device Configuration -> HA (High Availability) -> Zero Power HA**. To configure this using the device CLI, refer to the respective documentation. Rebooting the TPS does not change the bypass mode of the bypass I/O module.

Network Configuration

Through the SMS, you can view information about the segments on all of the IPS devices you are managing.

You can view and configure the networking and traffic processing of those segments through the Device (Network Configuration) screen.

To access this information, you expand a device entry, and select **Network Configuration**.

Segments

Segments are the portions of your network that you protect as discrete units. Traffic for one segment flows in and out of one port pair. By default, a filter applies to all segments that you are protecting

Physical segments

Physical segments set up a partition for traffic between two physical ports. This allows you to identify streams of traffic that flow between two defined physical ports.

Physical segments can be grouped together to form segment groups. You can apply a security profile (policy) to a physical segments and segment groups.

- **Name** — Segment name.
- **No.** — Segment number.
- **Direction** — Traffic direction for the segment.
- **Intrinsic Network HA** — Level of action for Intrinsic Network HA: Block All or Permit All.
- **Link-Down** — Mode, such as Hub, Breaker or Wire.
- **Port A, Port B** — Associated port for the segment.
- **Segment Group** — Membership in a segment group.
- **Profile Name** — Associated profile for the segment.

Virtual Segment Assignments

Virtual segments define traffic using an endpoint pair, a VLAN ID, or both that are assigned to one or more physical segments.

- **Name** — Segment name.
- **Direction** — Traffic direction for the virtual segment.
- **VLAN(s)** — Virtual LAN.
- **Side A, Side B** — User-defined labels that are used to monitor traffic flow.
- **Physical Ports** — Associated physical ports for the virtual segment.
- **Segment Group** — Membership in a segment group.
- **Profile Name** — Associated profile for the virtual segment.

Link-Down Synchronization

When editing a segment, you have the option to enable Link-Down Synchronization. Also called Sympathetic HA, this feature allows you to configure the device to force both ports down on a segment when the device detects a link state of down on one of the ports. When Link-Down Synchronization is enabled, the device monitors the link state for both ports on a segment. If the link goes down on either port, both ports on the

segment are disabled. This functionality propagates the link state across the device.

In the case of Router A and Router B, if the link to router A goes down, then both ports on the segment are disabled, resulting in the link to Router B going down, which Router B detects. With Link-Down Synchronization, ports respond according to the configured setting.

The settings include the following:

- **Hub** — When a port goes down, the system ensures the partner port remains up.
- **Breaker** — When a port goes down, the system disables the partner port until both ports are manually restarted. The breaker option requires manually restarting both ports.
- **Wire** — When a port goes down, the system disables the partner port, automatically restarting both ports when the link is re-established.

In addition to the ability to enable Link-Down Synchronization for each segment, you can change the amount of time after detecting a link is down before forcing both ports down on a segment. The default is one second. You can configure the setting to any number of seconds in the range of zero to 240.

After you enable Link-Down Synchronization for a segment, monitoring of that segment begins only after link up is detected on both ports. When Link-Down Synchronization disables the ports on a segment, two audit log messages are generated. The first message in the audit log corresponds to the port with the link down. The second message corresponds to the segment partner. Additionally, an error message is added to the system log indicating which port was detected with the link down, activating Link-Down Synchronization for that segment.

Import a profile

When you import a profile, the SMS migrates the filters into their new categories. The SMS assigns an action set of **Recommended** for all filters without customizations. If the filters have customized settings for action set, those settings are retained.

Procedure

1. From the navigation menu, expand the **All Devices** listing and select an IPS device by the device name. Open the tree of options for that device, and then select **Network Configuration**.
2. Select segment from the **IPS Segments** table, and then click **Import IPS Profile**.
3. The SMS imports the filters from the device into the SMS. The SMS names the profile using the segment name.
4. Click **OK**. Distribute the profile before you can monitor events or run a report.

Edit device segment details

Edit TPS or IPS segment details

Procedure

1. Select **Devices** > **All Devices** > **[device]** > **Network Configuration**.
2. Select the **Modules & Segments** tab.
3. In the **Physical Segments** table, select an entry, and then click **Edit**.
4. Modify the **Segment Name**.

   Follow these restrictions when you name or rename a segment:

   - Restrict characters to letters A–Z and a–z, digits 0–9, single spaces, periods (.), underscores (_), and hyphens (-).
   - Include at least one alphabetical character.
   - Do not begin or end the name with spaces.
   - Do not extend a name beyond 32 characters.
5. Modify the **Description** using up to 2048 characters.
6. For **Segment Group**, select the appropriate group entry from the drop down box.

7. For **Intrinsic Network HA**, select a fallback action:
   - **Block All** - All traffic is blocked while in fallback.
   - **Permit All** - All traffic is permitted while in fallback.
8. For **Link Down Synchronization**, select a mode, and then enter a value in seconds for the **Wait Time** (0-240).
   - **Hub** (port goes down, partner port remains up).
   - **Breaker** (port goes down, partner taken down, both require manual restart).
   - **Wire** (port does down, partner taken down, automatically restart when link reestablished). When selected, if one interface is down for an amount of time exceeding the time-out period, both interfaces are managed according to the selected option.

Edit a virtual segment

Edit a virtual segment to specify the traffic of interest.

Procedure

1. Select **Devices** > **Virtual Segments**.
2. Select a virtual segment, and then click **Edit** .
3. Edit the virtual segment.
4. Click **OK**.

Ports

The Ports tab displays the following information:

- **Type** — Type of port, such as Management Port or Data Port.
- **Slot** — IO slot is numbered from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. For TPS 5500TX, 8200TX and 9200TXE devices, the IO slot is numbered from 1 to 2. For TPS 1100TX devices, the slot is 1.

- **Port** — Port designation.
- **Segment** — Segment associated with the port.
- **Enabled** — enabled/disabled status.
- **Auto Negotiation**— check mark indicates the port auto-negotiates for line speed.
- **Configured** — Speed and duplex configuration.
- **XCVR** — Presence of a transceiver.
  - Grayed out: Port does not accept a transceiver.
  - Unchecked: No transceiver in the port.
  - Checked: Transceiver is present.
- **XCVR Info** — Information on transceiver (TPS TX Series and TXE Series devices, and IPS NX-Platform devices only) as applicable, such as transceiver connector type, compliance, and technology. If you see a red marker at the cell's upper-right corner, click the marker to expand the row for additional undisplayed information. Alternatively, toggle the visibility of information in expandable rows using the controls in the table's far left column.
- **Negotiated** — Negotiated setting.
- **State** — Health status of the port.
- **Media** — Type of media for the port, such as copper or fiber.

Edit ports

Edit Port A and Port B.

Fiber ports can only be set to 1000 Mbps line speed and full duplex. Although the port might negotiate different settings, you cannot arbitrarily downgrade line speed on a fiber Gigabit Ethernet port.

Procedure

1. Select **Devices All Devices [device name] Network Configuration Ports**.

2. Check the **IPS Segments** table to determine which port number is associated with Port A and which port number is associated with Port B.
3. From the **Ports** table, select the entry that corresponds to the Port entry in the **IPS Segments** table, and then click **Edit**. The Port Details - Edit dialog displays.
4. For **Hardware**, modify the **On** check box if the hardware is physically on or off.
5. For **Auto-Negotiation**, modify the **Enabled** check box if the port allows auto-negotiation for line speed.

Note

If you use a copper-fiber translator (such as Netgear), you should leave Auto-Negotiation disabled.

6. If you are not using Auto Negotiation, modify the following settings:
   - **Line Speed**.
   - **Duplex** setting: **Full** or **Half**.
7. Click **OK**.
8. Repeat steps for Port B.

Resolve out-of-service mode

If the SMS has errors and refuses to locate the device, check the connections on the device. If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver will attempt to re-initialize the port several times before timing out and placing the port in an out-of-service mode.
Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the device.

Procedure

1. From the Ports table on the Network configuration screen, select the entry that corresponds to the Port A entry in the **IPS Segments** table, and then click **Edit**.
2. For **Auto-Negotiation**, clear the **Enabled** check box. This disables the option.
3. Click **OK**.
4. Repeat steps 1 through 4 for port B. Leave auto-negotiation disabled. The port should reset.

VLAN translation

Some TippingPoint security devices can translate VLAN IDs per segment. The translation occurs after the inspection so incoming VLANs are used for virtual segments. For VLAN Translation, STP is not supported on the links attached to the IPS.

The **VLAN Translation** tab displays the following information:

- **Slot** — IO slot is numbered from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. For TPS 5500TX, 8200TX, and 9200TXE devices, the IO slot is numbered from 1 to 2. For TPS 1100TX devices, the slot is 1.
- **Incoming Port** — port number of incoming traffic.
- **Incoming VLAN ID** — VLAN ID for incoming traffic.
- **Outgoing VLAN ID** — VLAN ID for outgoing traffic.
- **Auto reverse** — reverse mapping setting.

Create or edit VLAN translation

This feature is available on IPS devices (N-Platform and NX-Platform) and TPS devices (TX Series and TXE Series). VLAN translation is not available on vTPS devices.

Procedure

1. Select **Devices** > **All Devices** > **device** > **Network Configuration**.
2. Click the **VLAN Translation** tab.
3. Perform one of the following tasks:
   - To edit a VLAN Translation, select an entry from the table, and then click **Edit**.
   - To create a new VLAN Translation, click **New**.
4. Enter the **Incoming VLAN ID** and **Outgoing VLAN ID** numbers from 1 to 4094.
5. In the Port Selection area select the appropriate settings for each segment (1 to 11).

Note

For NX-Platform, TX Series, and TXE Series devices, the segments are grouped by slots. The segment lists the slot number and the segment number.

   - **No mapping** — Do not use mapping for selected segment.
   - **A > B** — For traffic arriving on side A with the specified **Incoming VLAN ID**, the VLAN ID is set to the specified **Outgoing VLAN ID** prior to leaving side B.
   - **A < B** — For traffic arriving on side B with the specified **Incoming VLAN ID**, the VLAN ID is set to the specified **Outgoing VLAN ID** prior to leaving side A.
   - **Reverse mapping** — Automatically creates an inverse mapping. Changes the VLAN ID for traffic in the reverse direction from the Outgoing value to the Incoming value.
6. Click **OK**.

Modules and Segments

The Modules & Segments tab displays the following information about IPS NX-Platform, TPS TX Series and TXE Series devices:

- Modules
  - **Slot** — IO slot from 1 to 4 for IPS NX-Platform and TPS 8400TX devices. IO slot from 1 to 2 for TPS 5500TX, 8200TX, and 9200TXE devices. IO Slot 1 for TPS 1100TX devices.

Note

The second slot of the 5500TX device supports only the first four segments of a 6-segment I/O module.

  - **Module** — Information about the module
  - **Serial No.** — Serial number of the module
  - **Status** — Active status of the module
- Physical Segments
  - **Name** — Segment name
  - **No.** — Segment number
  - **Direction** — Traffic direction for the segment
  - **Intrinsic Network HA** — Level of action for INHA: Block All or Permit All
  - **Link-Down** — Mode, such as Hub, Breaker or Wire
  - **Port A, Port B** — Associated port for the segment
  - **Segment Group** — Membership in a segment group
  - **Profile Name** — Associated profile for the segment
  - **sFlow®** — Sampled traffic on segment for analysis
- Virtual Segment Assignments

- **Name** — Segment name
- **Order** — Sequential order
- **VLAN(s)** — Virtual LAN
- **Src Addr/Dst Addr** — Source/destination IP address
- **Segment Group** — Membership in a segment group
- **Profile Name** — Associated profile for the virtual segment

Events

Through the Events screen for an individual device, you can monitor system-specific information. The default displays data from the past 24 hours. (When first adding a device to the SMS, all of the graphs might not have 24-hours of data). Realtime data is available for most monitoring parameters. The data in the graphs can be printed or exported. To format, right-click on the graph.

Note

When you use the drop-down menu to change the graph view to view larger date ranges (either the **Last 7 Days** or **Last Month**), the SMS client will request additional data from the SMS server. These larger ranges can delay the response time of the SMS client, causing it to appear unresponsive until the data is populated.

For additional information on monitoring your IPS device, see *Events (all devices) on page 3-13*.

System Health (Health Stats)

Health Stats track key health areas for devices, and provides information in textual and graphical formats. Monitored statistics include temperature (measured in Celsius), memory, HA state, and license utilization of the selected managed device. The `High Water Mark %` license utilization value, which gets polled every five minutes, is the highest percentage usage on the

device since the last time the value was cleared. To display current values, click **Refresh**.

Column	Description
Name	Displays the components of the device. Available items depend on the device and TOS, and may include the following: • CPU • Disk/ramLog, Disk/ramRO, Disk/ramTmp • Disk/system • Disk/user • Fans • Voltage • Memory • Temperature
State	Displays the current state including critical (red), normal (green), or major (yellow).
Current Value	Displays the percentage amount of the component used.
Details	Displays details for the health stat, for example, the amount used of the total available megabytes (MB).

Click **Settings** to set health threshold preferences for storage, memory, and temperature.

Device health event entries

Issues with the health of a device list as event entries in the system log. These health events detail information about the status of your device depending on triggered filters. These events provide information about the issues of a device or group of devices.

The following events might occur on a device, component, resource, or host:

Event	Origin	Component	Definition
Add Device	SMS	device name	**Component** has been discovered and configured.
Alert Status	SMS	device name	The alerts status of **component** has changed to **status.**
Block Status	SMS	device name	The block status of **component** has changed to **status.**
Cold Start	device	device name	**Component** has been rebooted.
Config Sync	SMS	device name	SMS management data has been synchronized with **component**.
Connection Down	SMS	device name	**Component** has stopped communicating with the SMS.
Connection Up	SMS	device name	**Component** is now communicating with the SMS.
Device Availability	device	device name	**Component** entered Fall Back state at **time** or **Component** was available for service (not in the Fall Back state) at **time**
Delete Device	SMS	device IP	**Component** has been deleted from the SMS.
Delete Host	SMS	device component	**Component** has had a host removed from the SMS.
Fall Back Status	SMS	device-name	**Component** is in Fall Back state or **Component** is available for service (not in the Fall Back state)
Hardware Health	device	device component type	**Component** is **status**.
Hardware Status	SMS	device component	The health status of **component** has changed to **status.**
Manage Device	SMS	device name	The SMS is now managing **component.**
Managed From Device	device	device name	**Component** is now managed by the SMS.

Event	Origin	Component	Definition
New Host	SMS	device component	**Component** has a new host found by the SMS
Resource Health	device	resource name	**Resource-name** has changed from **pre-status** to **post-status.**
Resource Status	SMS	device component	The resource status of **component** has changed to **status.**
Unmanage Device	SMS	device name	The SMS is no longer managing **component.**
Unmanaged From Device	device	device name	**Component** is no longer managed by the SMS.
Warm Start	device	device name	**Component** has been restarted.

Health thresholds

Health thresholds determine whether a current setting for disk, memory or temperatures shows a major or critical status. A major threshold must be lower than critical.

In the SMS, configure system health thresholds for IPS security devices. You cannot change the system health thresholds for TPS devices. The following table lists the default health threshold settings for the IPS.

Factor	Major Parameters	Critical Parameters
Memory	> = 90%	> = 95%
Temperature (IPS)	> = 73° C	> = 75° C
Temperature (IPS N-Platform or NX-Platform)	> = 46° C	> = 51° C
File System space	> = 90%	> = 95%
License utilization	> = 70%	> = 90%

Procedure

1. On the Devices screen, expand the **All Devices** in the navigation pane.
2. Select a device and expand the options.
3. Expand the **Events** entry, and then select **System Health**.
4. In the Health Stats section, click **Settings**.
5. In the Devices - Health Thresholds dialog,
   - For **Storage**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
   - For **Memory**, enter a **Major** and **Critical** amount. The amount should be between 60% to 100%.
   - For **Temperature**, enter a **Major** and **Critical** amount. The amount should be between 40 to 80 Celsius.

Performance

Performance monitoring tracks key performance areas for managed devices and provides information in textual and graphical format. Monitored statistics include performance protection, packet status, and CPU for the selected managed device.

Entry Title	Description
Device	Name of the device.
Total Packets	The total number of packets for the device.
Blocked	The number of blocked packets.
Hit Permit Action	The number of permitted packets.
Rate Limited (availability depends on device and TOS version)	Number of rate-limited packets.
Trusted (availability depends on device and TOS version)	Number of trusted packets.

Entry Title	Description
Dropped	The number of dropped packets.

The Performance graphs area displays graphs for the following items:

- **Performance Protection** — Performance Protection activated on the device.
- **Packet Statistics** — Status of packets inspected by the device.
- **CPU for XLR A** — How much of the CPU capacity is in use.
- **Deep Packet Inspection (S-Series)** — The counts of packets that undergo greater inspection.
- **Tiers (Ratio to next tier)** — Represented in percent over time as a ratio to next tier.
- **Tier 1 Transmit and Receive Rates** — Represented as Mbps over time.
- **Tier 4 Reason** — Represented as percent over time.
- **Tier 1 Balance** — Represented as percent over time.
- **Tier 1 Bypass** — Represented as Mbps over time.

To display current values, click **Refresh**. To view Realtime data, click **Realtime**.

Tier statistics

Tier statistics provides information on packets and speed by tier. This area also displays Ratios and Utilization for A-side and B side traffic.

For more information about tier statistics for IPS NX-Platform, TPS TX Series, and TPS TXE Series devices, see *Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices on page 3-47*.

Tier statistics for the vTPS, TPS, and IPS (NX-Platform) devices

Displays throughput and efficiency across the different inspection tiers of this device. Use this information to diagnose certain performance-related issues. On a stack device, the device's stacking statistics are displayed.

Inspection Tier	Description
Stack : Segment Ports	For IPS (NX-Platform), TPS 8200TX/8400TX, and TPS TXE Series devices, the following information is displayed when stacking is enabled: • `Segment Rx Mbps` displays the aggregate received traffic from all network segments on this device. • `Segment Tx Mbps` displays the aggregate traffic transmitted from all network segments on this device. • `Stack Balance` displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. Note this will include devices that are in Intrinsic HA L2FB which would be zero in the load balance calculation. This statistic is analogous to the XLR load balance percent in Tier 1. • `<host n> Rx Mbps` displays the traffic balanced from this device's network segments to the other devices in the stack. • `Segment ratio to tier 1` displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic.
Stack : Stack Ports	For IPS (NX-Platform), TPS 8200TX/8400TX, and TPS TXE Series devices, the following information is displayed when stacking is enabled: • `Stack Rx Mbps` displays the aggregate received traffic from both stacking ports. • `Stack Tx Mbps` displays the aggregate traffic that is transmitted from both stacking ports. • `Stack Rx > Stack Tx` displays the total amount of transit or through traffic on the stacking ports; for example, traffic received on one Stack port that is forwarded by the switch to the other stack port. • `Stack Rx > Seg Tx` displays the amount of return traffic coming in on a stacking port en route to a network segment. • `Stack ratio to tier 1` displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.

Inspection Tier	Description
Tier 1	Inspection bypass and Intrinsic HA L2FB are handled here, preventing traffic from going to the next tier. It also handles the rate limiter, inspection bypass rules, jumbo packet shunting, and hardware watchdog timer. • `Rx Mbps` and `Rx packet/sec` indicate how much traffic is entering the device from all the segments. `Tx Mbps` and `Tx packet/sec` indicate how much traffic is egressing the device. A value in parentheses () represents the high-level watermark and a value in brackets `[]` represents the low-level watermark since the IPS was powered on or the tier statistics were reset.  **Note** Use the `clear np tier-stats` CLI command to clear out these statistics. • `Bypass Mbps` displays the current and max throughput matching an Inspection Bypass rule. Traffic matching an Inspection Bypass rule does not count towards the IPS inspection limits. • `A/B/C Balance` displays how well the flows are being balanced between the XLRs. 100% indicates even balance 33/33/33 split, which is ideal. 0% means that all traffic is going to a single XLR. Note that the number of packets going thru the each XLR is flow based, so it is not uncommon to see a slight difference between them. • `Utilization` displays the percentage of rated system throughput and of traffic to next tier. • Inspection bypass rules reduce the value of both `Utilization` and `Ratio to next tier`.
Tier 2	Load balances flows through the KS threads and handles traffic management trusts and block filters will prevent traffic from proceeding to the next tier. `Ratio to next tier` accounts for Traffic Management Trust and Block rules and Traffic normalization filters. TCP ACKs are trusted by default, and reduces Tier 2 ratio to next tier.

Inspection Tier	Description
Tier 3	This tier is designed to search for suspicious traffic that needs to undergo deep inspection. This section handles IPv6 + GRE and Mobile IPv4 tunnels. IP reassembly, maintaining connection table, and TCP state tracking is handled here. If triggers are found it determines what filters need to be checked against the packet or flow then it turns on soft-reroute for the flow, and, if necessary, sends it for deep packet inspection. This section displays how much traffic KS threads and IP reassembly will inspect. Ratio to next tier shows what percentage of traffic needs TCP reassembly or is suspicious (matched a trigger).

Inspection Tier	Description

Tier 4	This tier performs TCP reassembly and threat verification which includes header-based checks, protocol decoders, content search, and regular expression matching. Also, action handling occurs here whether the packet is dropped, rate limited, or rate limited in the connection table.
	• `Rx due to` indicates why traffic is going deep:
	  • `Trigger match`. Displays the percentage of traffic that matched a trigger.
	  • `Rx due to Reroute`. When a packet matches a trigger the following packets which belong to the same flow are required for threat verification.
	  • `TCP sequence`. If traffic cannot be reordered by K threads using loopy packet, it must go to Tier 4 for reordering.
	• `Ratio to next tier`. Displays the percentage of traffic that matched a filter, regardless of the Action Set.
	Tuning is required if congestion is occurring or if an IPS is being operated close to its maximum rated throughput. The deeper a flow is inspected the more processing is required, so the most performance gains can be attained by optimizing the KS threads at this level (Tiers 3 and 4). The three most process intensive operations are:
	1. IP reassembly
	2. Threat verification
	3. TCP packet reordering
	For supported TPS devices with a TOS v5.3 or later, the following information is displayed when SSL inspection is enabled:
	• `Rx Mbps and Tx Mbps` indicate how much encrypted traffic is entering the inspection engine from all the segments. The numbers in the brackets represent the high-level water mark since the IPS was powered on or `tier stats` was reset.
	Note
	Use the `clear np tier-stats` CLI command to clear out these statistics.

Inspection Tier	Description
	• `Utilization` displays the percentage of rated system throughput and of traffic to next tier.
Tier 5	For supported TPS devices with a TOS earlier than v5.3, the following information is displayed when SSL inspection is enabled: • `Rx Mbps and Tx Mbps` indicate how much encrypted traffic is entering the inspection engine from all the segments. The numbers in the brackets represent the high-level water mark since the IPS was powered on or `tier stats` was reset.  **Note** Use the `clear np tier-stats` CLI command to clear out these statistics. • `Utilization` displays the percentage of rated system throughput and of traffic to next tier.

Port health

Port health monitoring tracks key port statistics for managed devices and provides information in textual and graphical formats. For IPS NX-Platform, TPS 8200TX/8400TX, and TPS TXE Series devices, the SMS displays the slot number in addition to the other port information.

You can edit port information directly from the graph area of the Events - Port Health screen. To edit port details, click **Edit** associated with the graph that displays the port information. See *Import a profile on page 3-34*.

To display current values, click **Refresh**. To view Realtime data, click **Realtime**.

Port statistics

The textual display provides data by segment and includes the following information:

- Total In/Out Byte
- Total In/Out Discards

- Total In/Out Errors

The graphical display tracks Input/Output by port and provides information about the following items:

- Media
- Line Speed
- Link Status
- Duplex Status

Historical graphs

Historical graphs track Input/Output by port and provides information about the following items:

- Media
- Line Speed
- Link Status
- Duplex Status

Traffic

Traffic tracks and compiles information on all traffic managed by the device. Traffic graphic include the following:

- **Frame Size** — Traffic profile by frame size, by specified byte ranges. This graph currently returns no statistics for vTPS devices.
- **Frame Type** — The frame types of the packets flowing through the IPS.
- **Protocol** — Displays attack traffic categorized by protocol. Includes the number of filtered packets for each protocol and the percentage of total traffic the number represents. Protocols include: ICMP, UDP, TCP, and IP-Other.
- **Severity** — Displays the number of attacks categorized as Low, Minor, Major, and Critical. Also shows the percentage of total traffic for each

severity level. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.

System log

The system log contains information about the software processes that control TippingPoint devices including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with your TippingPoint device.

The system log also includes event information regarding device health. If the status indicator for the device displays an error or issue, you can view the log to locate information on the health events. See *System health (all devices) on page 3-18*.

The following table details the system log details:

Heading	Description
ID	The ID of the alert in the log.
Message	The description of the alert.
Entry Time	The time of the alert added to the log.
Severity Level	The severity level of the alert in the log.
Component	The component affected by the alert or event, such as report, policy, and OAM.

Audit log

The audit log keeps track of device user activity that might have security implications. This activity includes user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change device configuration
- Gain access to controlled areas (including the audit log)

- Update system software and attack protection filter packages
- Change filter settings

Note

For TPS devices, users must have at least Administrator access level to view, reset, and download the audit log. For IPS devices, SuperUser access level is required.

Heading	Description
ID	The ID of the alert in the log.
Time	The time of the alert added to the log.
Access Level	The access level of user causing the alert. Can include SMS for the system, SuperUser, and so on.
Interface	The interface used that generated the alert or event: WEB or SYS.
IP Address	The IP address of the system that generated the alert or event.
Component	The component affected by the alert or event, such as report, policy, and OAM.
Result	The result of the event, such as PASS for successful.
User	The user account causing the alert.
Message	The description of the alert.

When you view the log, the user listed for the logged events might include SMS and CLI. These entries are entered by those applications into the audit log, as a SuperUser level of access.

Device configuration

Update management information

Depending on the device, you can:

- Update the host name of your device and add descriptions for the device location and contact information.
- Review the device model and serial number.
- View or configure the management port settings.
- View the Network Mask and Default Gateway and enter settings for fast ethernet port located on the management processor module. The IP address for this port is the IP address through which you access the device. This port must be contained within your local network, but must not be contained within any of the subnets that pass traffic through the Multi-Port Defense Module of the device.
- Review the currently installed TOS, Digital Vaccine, and Threat DV.
- Reboot or shutdown the device.
- Reset IPS filters to their recommended state. Use this option to reset filters due to issues or settings. The recommended settings for a filter might differ by state (enabled/disabled), notification contacts, exceptions, and action sets.
- Go to the associated device. Click the **SSH Terminal** to access the device from the SMS.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Management Information** and update the following:

Field	Description	Valid Input
Hostname	The hostname of the device. It should be the same host name as the one listed for the device IP address in your network DNS lookup.	A valid hostname on your network segment. A valid hostname consists only of alpha-numeric characters and hyphens, and cannot exceed 63 characters or have a hyphen at the beginning or end.
Location	A description of the location of the device.	
Contact	A contact name for the device. **Note** This feature is only available on TPS devices.	A maximum of 32 characters describing the device contact.
Model	The number of the device model.	—
Serial Number	The serial number of the device.	—
Mgmt IP Address	The IP address used to make a network connection to the device.	A valid IP address on the network segment the device is attached to in dotted decimal IP address (255.255.255.255) notation.
Network Mask	The network mask in effect on the subnet that your device is attached to.	A valid network mask for the network segment on which your device resides in dotted decimal IP address (255.255.255.255) notation.
Default Gateway	The gateway through which the device communicates with external network entities, and through which external network entities communicate with your device. You can enter a number of gateways for Gateway and Routing.	A network device that contains routing tables that list your device and external network entities as well.

Field	Description	Valid Input
Edit Management Port Settings	Informational dialog that provides Port Details. Enable or disable auto negotiation. **Note** This feature is only available on select IPS devices.	Enable/disable auto negotiation
View Management Port Settings	Click **View Mgmt Port Settings** to view management port settings and current state details.	
TOS	TippingPoint Operating System (TOS).	
DV	Digital Vaccine version numbers.	
Auxiliary DV	Enables you to update to the latest malware filter package if you subscribe to Threat DV. For subscription information, contact your TippingPoint representative.	—

3. Click **OK**.

Reset IPS filters

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Management Information**.
3. Click **Reset IPS Filters**. A message prompts you to confirm that you want to reset all filters back to their recommended state.
4. Click **OK**.

   After resetting the IPS filters on an IPS, a message notifies you that the reset is complete; the reset process might take several minutes. Any

profile distributions attempted before the reset has completed will fail, as the device is still busy resetting the filters.

Management network

From this screen you can configure the management network settings for your device. These settings only affect the device's management port and its ability to communicate with the SMS. They do not modify filters or otherwise change the way traffic is inspected.

IPv6 is an Internet protocol that uses 128-bit addresses, which increases the number of possible addresses and adds increased security. Expressed in a series of four-digit hexadecimal numbers that are separated by colon (:) notation, IPv6 addresses allow the Internet to grow in terms of connected hosts and data traffic.

Note

Incorrect settings for the default gateway or management port prevent management communication with the device.

From this screen you can:

- Enable IPv6.
- Automatically assign IPv6 addresses to the management port.
- Configure the default gateway.
- Choose one of the following ways to manage the device.
  - Specified IPv6 address to the management port interface.
  - Link-Local IPv6 address — the device and the SMS MUST be on the same physical network.
  - Auto IPv6 address — Global unicast address assigned during network initialization.
- Enable the configured IPv6 IP address to manage the device.

Note

If you do not select **Use IPv6 address to manage this device**, the IPv4 address or **Public IP Address** on the **Management Information** page is used to manage the device.

Configure management network (TPS and NX-Platform)

Note

The management network configuration only impacts the device management port and its ability to communicate with the SMS. These settings do NOT modify filters or change the way traffic is inspected.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Management Network**.
3. To set the protocol for managing the device, go to the Communication area and select one of the following protocol options:
   - **Use IPv4** to manage device to manage the device using its IPv4 address.
   - **Use IPv6** to manage device to manage the device using its IPv6 address.

   Note

   If you are editing the Network Management configuration and want to disable IPv4, use IPv6 to manage the network BEFORE you disable IPv4. If you are editing the Network Management configuration and want to disable IPv6, use IPv4 to manage the network BEFORE you disable IPv6.
4. For IPv4 Configuration:

- **Enable IPv4** — Select this check box to configure the device management port with an IPv4 address.

Important

If this check box is not selected, the IPv4 stack is disabled.

- **IP Address** — Specify the IP (IPv4) address to assign to the device management port interface.
- **Network Mask** — Specify the subnet mask to assign to the device management port interface.
- **Default Gateway** — Specify the IP address of the route to use to send packets addressed to other networks.
- **Default Gateway Enabled** —Select this check box to assign the specified IPv4 default gateway to the device management port interface. Deselect this check box to disable gateway configuration.

Important

If this check box is not selected, the device and the SMS MUST be on the same subnet.

5. For IPv6 Configuration:

- **Enable IPv6** — Select this check box to configure the device management port with an IPv6 address.

Note

If this check box is not selected, the IPv6 stack is disabled.

- **Automatically configure network interface** — Select this check box use IPv6 stateless address auto configuration to assign IPv6 addresses to the management port.
- **Management Address** — Choose one of the following ways to manage the device:

- **IP Address** — user-specified IPv6 address to the management port interface.
- **Link-Local** — local IPV6 address assigned during network initialization. The SMS and the device MUST be on the same physical network.
- **Auto** — local unicast address assigned during network initialization.

- **Default Gateway** — Specify the IP address of the route to use to send packets addressed to other networks.
- **Default Gateway Enabled** —Select this check box to assign the specified IPv6 default gateway to the device management port interface. Deselect this check box to disable gateway configuration.

Important

If this check box is not selected, the device and the SMS MUST be on the same subnet.

Note

If you do not select **Use IPv6 address to manage this device**, the IPv4 address or **Public IP Address** on the Management Information page is used to manage the device.

6. Click **OK**.

Management routes

Routing options enable the device to communicate with network subnets other than the subnet on which the Management Port is located. If you will manage your TippingPoint device from a different subnet, you will need to define a route between the subnet to which your workstation is connected and the subnet to which your TippingPoint Host Management Port is connected.

Host IP filters

IP filters prioritize traffic and implement security policy. When you specify filter settings, you control system access by services that use the management port. Filter rules set to Deny affects the SMS management of the appliance.

Configure NAT

Use NAT to minimize the number of internal IP addresses that are exposed to the Internet. NAT technology converts private IP addresses on an internal private network to one or more public IP addresses for the Internet.

The NAT IP address is only saved on the SMS and is used when communicating with the device.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **NAT**.
3. To enable NAT, select **Enable**.
4. Enter the Public IP Address for the device.
5. Click **Apply**.
6. Click **OK**.

Services

On the Device Configuration (Services) screen, you can configure settings for system services. For Services, you can enable one or more remote services for secure connections. These services provide connections for the Command Line Interface (CLI) and Web (HTTPS). You should use secure communications (SSH and HTTPS) to operate the CLI and the Web interfaces.

Note

HTTPS service is an integral service for the SMS, always enabled and available. SSH and telnet require SuperUser access.

If you disable SSH, you cannot run or access the CLI.

For devices using V 2.1 or higher TOS, the system can use an encrypted channel for sending messages between the device and SMS. The encrypted channel polls the device according to the polling interval for the mode.

The Encrypted Alert Channel Settings option provides three modes:

- **Enabled Normal Mode** — Disables the SNMP traps and enables an SSL connection between the SMS and the device to transfer Alert messages reliably and securely by polling the device approximately every five seconds. This option is the default.
- **Enabled Batch Mode** — Disables the SNMP traps and enables an SSL connection between the SMS and the device to transfer Alert messages reliably and securely by polling the device according to a configured amount of minutes, which reduces network traffic slightly but increases the average time for the SMS to become aware of device Alerts.
- **Disabled (Use SNMP)** — Uses the existing SNMP trap mechanism.

Option	Description
SSH	Secure connection for using the CLI. Requires a user with SuperUser capabilities.
HTTPS	Secure network communication for Web pages. Enabling HTTPS enables Web services for the SMS. See the *SMS Web API Guide*.

Option	Description
HTTP	Unsecure network communication connection for Web pages. Enabling HTTP enables Web services for the SMS. See the *SMS Web API Guide*. **Note** See *TSE Settings on page 3-85* for HTTP mode on TPS devices.
Encrypted Alert Channel Settings	Compiles and sends alerts. Encrypted for security. You can disable this service to use SNMP. • **Enable Normal Mode** —Sends alerts as they are received • **Enable Batch Mode** — Compiles alerts according to a configured **Wait Time Interval** (minutes ranging from 1 to 60). Enter an amount of minutes if selecting this option. • **Disabled (Use SNMP)** — Alerts are sent using SNMP, disabling this service. **Note** You must enable Encrypted Alert Channel if your profile's Capture Additional Event Information setting includes HTTP. SNMP does not support HTTP context. Encrypted Alert Channel settings are not supported on TPS devices.
Data Retrieval Service	Enables the SMS to retrieve and display traffic stats by port per device. Data Retrieval Services only apply to IPS devices.
SNMP	Alerts are sent using SNMP. If your devices support both SNMP v2 and SNMP v3, you can configure the device to use one or both versions. To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

Option	Description
TLS Settings	Enable or disable the TLS versions (v1.0, v1.1, v1.2, and v1.3) for a managed device. TLS Settings are only supported on TPS devices running TOS v4.1 or later. The TLS versions enabled on a TPS device must be compatible with the TLS versions enabled in this section. By default, only TLS v1.2 is supported.

Device settings

Configure appliance-specific global settings, such as IDS and quarantine settings, timeout settings, asymmetric routing (DDoS filters cannot work if this feature is enabled), adaptive filter properties, and auto-reboot enablement.

You can configure the global settings for the following items:

- **Adaptive Filtering** — Set Adaptive Filtering Configuration (AFC) options that automatically manage your appliance under extreme load conditions and protect against the potential adverse effects of a defective filter. On rare occurrences, the system can experience extreme load conditions due to filter failure and traffic congestion, causing a device to enter High Availability (HA) mode. Adaptive filtering disables the filters that are likely causing traffic congestion.
- **Connection Table** — The value for the global connection table timeout. This value is 30-1800 seconds. This value applies to all blocked streams in the connection table, and determines the amount of time that elapses before that connection is cleared from the connection table. Before that period of time elapses, any incoming packets for that stream are blocked at the box. After the connection is cleared, the incoming connection is allowed (if its action set has changed) or re-added to the blocked list. Separate settings are available for TCP and non-TCP traffic.
- **Asymmetric Network** — The dynamic sharing and use of bandwidth for increased network traffic performance. If you configure the appliance through the TSE configuration for an asymmetric network, the SYN flood detection, or DDoS filters, will be disabled. In effect, the TSE will not see both sides of a TCP connection. SSL inspection cannot occur in

asymmetric mode. Consult your device documentation for a list of additional filters that cannot be run in asymmetric mode.

- **Quarantine** — Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses can be automatically released, if that option is selected.

Note

If you unmanage an appliance and then remanage the appliance, the quarantine settings are reset to the default value.

- **IDS Mode** —When enabled, automatically configures the device to operate in a manner similar to an Intrusion Detection System (IDS).
  - Performance protection is disabled. As a best practice, enable this option and set it to **Always**.
  - Adaptive Filtering mode is set to Manual.
  - Filters currently set to Block are not switched to Permit, and Block filters can still be set.

Note

Using an IPS/TPS device in a mixed configuration is not supported. When an IPS/TPS device is used in an IDS configuration, then it is an IDS device. Use the IPS/TPS as *either* an IDS device or an IPS device, but not both. Attempting to run your device in mixed mode will lead to performance issues.

Reboot your system for settings to take effect.

- **Auto Reboot** —Specifies whether automatic reboots can be determined by the appliance.

Configure a device for adaptive filtering

The Adaptive Filter Configuration (AFC) state enables the Threat Suppression Engine to automatically manage a device. This feature protects against the potential adverse effects of a filter that interacts poorly with the network environment.

At the filter level, you have the option to disable adaptive filtering so that a filter is never impacted by the adaptive filter settings on a device. Learn more: *Adaptive filtering on page 5-24*.

You can also view the filters most recently affected by adaptive filtering in the **Adaptive Filter List,** and re-enable the filter state. Learn more: *View AFC filters on page 3-17*.

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **AFC Settings**.
3. Select the AFC setting:
   - **Auto** — This setting enables the device to automatically disable the defective filter and generate a system message.
   - **Manual** — This setting enables the device to generate a system message regarding the filter. However, the filter is not disabled.
4. Select the severity of the system log message that is automatically generated when a filter triggers the AFC setting configured on a filter.
5. Click **OK**.

Device High Availability

You can configure settings for Intrinsic, Transparent, and Zero Power High Availability (HA).

Intrinsic HA

Intrinsic HA determines how the device manages traffic on each segment in the event of a system failure. When the system fails, the device goes into fallback mode and either permits or blocks all traffic on each segment, depending on the fallback action setting for the segment.

- *Normal mode* configures the device to inspect traffic according to the Threat Suppression Engine (TSE) settings.
- *Fallback mode* either permits or blocks all traffic on each segment, depending on the Intrinsic HA fallback action setting for the segment. Any permitted traffic is not inspected.

A lack of reported errors or congestion through the TSE does not guarantee that the components receive correct and error-free traffic. Intrinsic HA monitors for several points of failure and applies failure detection logic against the system.

The device performs the following checks to detect a failed condition and trigger intrinsic HA:

- Handle non-atomic nature of the data path — Packet pass through each component at different times and rates. The status of each component is determined independently of each other. Intrinsic HA uses sampling to determine health.
- Check and transmit the inbound receive counters — Each component has receive counters incremented by packets received from the previous component. The component transmits these counters incremented as packets to the next component. These counters are the most accurate and most complicated way of detecting health.
- Dropped packets exceeds threshold — If too many packets awaiting deep inspection are queued up, packets are dropped. The system checks every five seconds to see if the device drops 90 percent or more of the traffic that goes to Tier 3. If so, the system enters fallback mode. However, this condition is difficult to create because the TSE only sends a fraction of incoming traffic to Tier 3.
- Low memory — Whether available system memory is too low for proper operations.

Intrinsic HA monitors the device to detect hardware operating system failures and to automatically switch to the fallback mode when a server outage or system failure is detected.

Use the **fallback** mode to permit or block all traffic according to the fallback settings for each device segment.

Transparent HA

Deploy Transparent HA in a redundant network configuration so that a partner device takes over in the event of system failure. Transparent HA partner devices constantly update each other with their managed streams information (blocked streams, trusted streams, and quarantined hosts). If a system failure occurs, interruptions to network protection are minimized because the partner device does not have to rebuild all of the current managed streams information.

Important

When Transparent HA is enabled, a hijacked partner device or a rogue device that impersonates the IP address of a Transparent HA partner device can communicate with the partner device.

When you configure TPS devices for Transparent HA, keep the following points in mind:

- With the exception of 8200TX, 8400TX, and 9200TXE devices, TPS devices in an Transparent HA configuration can only be connected—through the HA port—to an identical model device (for example, you can only connect a 2200T device with another 2200T device). The 8200TX and 8400TX devices are the only two TPS devices that can be mixed in a Transparent HA configuration. Connect these two devices using the management (MGMT) ports. TRHA for TXE Series devices require that you pair each device with an identical model with identical management ports.
- Transparent HA requires the same TOS version on each Transparent HA device.
- Transparent HA partners must be able to communicate with each other on TCP port 9591.
- On a TippingPoint Virtual Threat Protection System (vTPS) security device, Transparent HA is not supported.

After you configure Transparent HA, keep this point in mind:

- If you plan to change the global timeout interval on the connection table, be sure to update both partner devices. Transparent HA does not synchronize changes to the global timeout interval.

Zero Power HA

Zero Power HA (ZPHA) ensures a constant, uninterrupted flow of traffic. During a system outage, ZPHA bypasses the device and provides continuous network traffic.

Note

Be aware that ZPHA technology is not "hitless"; when relays are switched over, you might lose traffic.

Configure ZPHA to determine its state:

- *Bypass mode* bypasses the TSE and maintains high availability on any network segments that have ZPHA support. When the device loses power, any network segments that do not have ZPHA support are disconnected.
- *Normal mode* inspects traffic according to the TSE settings.

Bypass is available for the IPS as an external modular device or as optional bypass I/O modules on NX-Platform, TX Series, and TXE Series devices.

TPS device support for ZPHA varies by device:

- On TippingPoint TX Series and TXE Series devices, optional bypass I/O modules provide high availability for copper and fiber segments.

  Note

  When you insert a bypass I/O module, by default the I/O module starts up in bypass mode.

- On a TippingPoint 2200T device, ZPHA support is built-in for copper segments. An external ZPHA module is required to enable ZPHA on SFP and SFP+ segments.

- ZPHA is built-in for all copper segments for a 440T device.
- ZPHA is not supported for vTPS.

Configure network HA

Procedure

1. Select **Devices** > **All Devices** > **<device>**, and then click **Device Configuration**.
2. Select **HA (High Availability)**.
3. To configure **Intrinsic HA**, do one of the following:
   - Select **Normal** to override all Intrinsic HA settings and configure the device to inspect traffic according to the TSE settings.
   - Select **Fallback** to permit or block all traffic according to the fallback settings.
   - Click **Apply**.
4. To configure **Transparent HA**, do the following:
   - Select the **Enable** check box to configure the device to constantly be updated with TCP flow information.
   - Select a **Partner Device** to configure Transparent HA.
   - Select the **Encrypt Traffic** check box to protect network traffic between the devices, and enter and confirm the **Passphrase**.
5. To configure **Zero Power HA**, do the following:

   Note

   If the TPS device or IPS NX-Platform device does not have an installed bypass module, this option is not available.

   - Select **Normal** to configure the device to inspect traffic according to the TSE settings.

- Select **Bypass IPS** to pass all network traffic regardless of the fallback configuration on each segment.
- Click **Apply**.

6. Click **OK**.

Performance Protection

Configure settings for alerts. You can enable or disable alerting of permitted and blocked packets or set the Logging Mode to **Always** or **Disable if congested**.

If you set the Logging Mode to **Disable if congested**, you can set the following logging options:

- **Congestion Percentage** — percentage of congestion that must be met in order for logging to be disabled.
- **Disable Time** —amount of time in seconds (between 60 and 3600 seconds) that logging will be disabled after the congestion percentage is met.

Configure NMS settings for SNMP v2

Protocol for monitoring a device by a restricted network management protocol (NMS).

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **NMS Settings**.
3. Enter or edit a **Community String** (1-31 characters).
4. Click **New**, or select an existing NMS, and click **Edit**.
5. Enter the **IP Address** and the **Port** (162 is the default port).

6. Click **OK**.

Configure NMS for SNMP v3

This feature is available for N-Platform or NX-Platform IPS devices running TOS v3.1 or later. To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **NMS Settings**.
3. Enter or edit a **Community String** (1-31 characters).
4. Click **New**, or select an existing NMS, and click **Edit**.
5. Enter the **IP Address** and the **Port** (162 is the default port).
6. For the trap destination, select **SNMP v3**.
7. Enter the **Engine ID**, **User Name**, **Password**, and then **Verify Password**.
8. Select a **Privacy Protocol**.
9. Click **OK**.

SNMP settings

Configure your device for Simple Network Management Protocol (SNMP) support. When SNMP is not enabled, an SSL connection between the SMS and the device transfers Alert messages reliably and securely. Alerts sent using SNMP can be encrypted if DES or AES is selected in the SNMP User Privacy settings.

Specify the properties for SNMP traps, users, and communities.

Note

To use SNMP v3 for NMS traps, you must configure Services for SNMP v3 or Both.

You can create multiple SNMPv2c communities to support NMS, IPs, or subnets. Each community can have multiple rules; however, the source IP address must be different. For example, you can create a rule for a Community named Public with a source IP address of 1.1.1.1. You can have a second rule for Public with a source IP address of 2.2.2.2.

After you enable SNMP, it might take a couple of seconds to start the SNMP daemon. In the unlikely case of a collision with another device, you can change the Engine ID to a different value; however, the new value must be unique. Note that changing the Engine ID regenerates each read-only user, which affects connectivity.

Note

For NX-Platforms, you must reboot the device for the SNMP settings to take effect.

Log Configuration

Use the Log Configuration screen to configure user encryption policy, specify your master key, and set the notification contact properties and threshold severities of audit, system, VPN and quarantine logs.

Data Security – vTPS and TPS

For vTPS 5.0 (and later) and TPS devices, use the Data Security screen to secure the system keystore with a new master key and to secure the external user disk (CFast or SSD).

(Best Practice) To avoid keystore issues with a TOS rollback, set the master key to a passphrase that you specify. If the keystore in the rollback image is secured with a different master key than the master key that is set on the device, you can set the master key to the correct passphrase.

By default, the external user disk is not encrypted which enables you to easily access the contents of the external user disk from a different device. The external user disk (CFast or SSD) stores all traffic logs, snapshots, ThreatDV URL Reputation Feed, User-defined URL Entries database, and packet capture data.

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

- To reset the master key using the SMS, you must have superuser capabilities.
- You cannot change the encryption status of external user disk on the vTPS.
- When you change the encryption status of the external user disk, the device automatically formats the disk and all data is erased. On large, external CFast disks (32 GB or more), it can take 40 seconds or more to complete disk format and encryption operations.
- The system master key encrypts and decrypts the external user disk. To access the contents of an

  encrypted external user disk from a different device, for example to restore a snapshot, the same master

  key must also be set on the device.

Remote syslog

A remote syslog server is another channel that you can use to report filter events. Remote syslog sends filter alerts to a syslog server on your network. You can have one or more remote syslog servers.

Note

Designating a remote system log server does not automatically send attack notifications to that server. You must select the Remote System Log contact for action sets. After you apply these changes, active filters associated with the modified action set will send remote messages to the designated server.

Security devices that run TOS 3.6 or later can collect a client's true IP address before it is overwritten by a forwarding proxy IP address. X-Forwarded-For and True-Client-IP technologies identify a request's source IP address without administrators having to refer to proxy logs or Web server logs. When the **Additional Event Information** options are turned on, additional fields in the event logs display the True-Client-IP address and any HTTP URI information associated with the event. This visibility lets security teams set a more accurate network-based user policy.

If you intend to use Action Sets that include the Notify Remote Syslog option, you must create an entry for the devices to use. The system uses collectors for the settings. Collectors are specified by the required settings for the IP address and port, including options for a delimiter and facility numbers for alert messages, block messages, and misuse/abuse messages. The settings for the facilities are optional. Valid delimiters include horizontal tab, comma (,), semicolon (;), and pipe (|).

The log format for the remote syslog includes changes detailed below. The following is an example of packet data sent to a collector. Make note that collectors might display the header portion of the stream differently.

```
<13>Jan 13 12:55:01 192.168.65.22 ALT,v4,20050113T125501+0360,"i
robot"/192.168.65.22,1017,Alert,1,1,
00000002-0002-0002-0002-000000000164,"0164:
ICMP: EchoRequest (Ping)","0164: ICMP: Echo Request
(Ping)",icmp,216.136.107.233:0,216.136.107.91:0,20

050113T125205+0360,199," ",1,3:1
```

In this example, the header follows the standard syslog format. Using the previous log entry as the example, the message is as follows:

```
ALT,v4,20050113T125501+0360,"i
robot"/192.168.65.22,1017,Permit,1,Low,
00000002-0002-0002-0002-000000000164,"0164:
ICMP: EchoRequest (Ping)","0164: ICMP: Echo
Request(Ping)",icmp,216.136.107.233:0,216.136.107.91:
```

```
0,20050113T125205+0360,199,"
",1,3:1
```

The character located between each field is the configured delimiter. In this case, the delimiter is a comma. The following table details the fields and their descriptions.

Field	Description
1	Log-type; ALT = alert, BLK = block, P2P = misuse and abuse
2	Version of this message format
3	ISO 8601 Date-Time-TZ when this alert was generated
4	Hostname/IP address that generated the alert; note that the quotes are required for this release because of a bug in the hostname validation (note the space in the name)
5	Sequence ID
6	(reserved)
7	Action performed (Block or Permit)
8	Severity (Low, Minor, Major, or Critical)
9	Policy UUID
10	Policy Name
11	Signature Name
12	Protocol name (icmp, udp, tcp, or unknown)
13	Source address and port, colon delimited
14	Destination address and port, colon delimited
15	ISO 8601 Date-Time-TZ when the aggregation period started
16	Number of events since start of aggregation period
17	Traffic Threshold message parameters

Field	Description
18	Packet capture available on device (available = 1; none = 0)
19	Slot and segment of event

Configure a remote syslog server

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Remote Syslog**.
3. Click **New**, or select an existing listing, and then click **Edit**.
4. Specify an **IP Address** and **Port** (514 is the default port).
5. Select an **Alert Facility**: none or select from a range of 0 to 31.
6. Select a **Block Facility**: none or select from a range of 0 to 31.
7. Select a **Delimiter** for the generated logs: **Horizontal Tab**, **Comma**, **Semi-colon**, or **Pipe**.
8. Click **OK**.

   The SMS restarts the segment, updating the hardware settings for the device and restarts the auto-negotiation process. If an error occurs, the copper cable translator might not support auto-negotiation.

Email server

Configure settings for DNS and email servers. Domain Name Service (DNS) supplies the address or addresses which should be consulted for host name to IP address resolution. Email server supplies the default email settings for email alerts.

Note

You must be sure that the device can reach the SMTP server that will be handling the email notifications. You might have to add a management route so that the device can communicate with the SMTP server.

Specify the following information:

- **IP Address**
- **Domain Name**
- **From Email** address. This is the sender address when the SMS sends alerts to notification contacts.
- **Threshold**, which is the maximum emails per minute (1 - 35).

Configure time settings (TPS devices)

View the current device time and configure the settings for how the system tracks time. A device comes with pre-defined time zone entries. Although system logs are kept in Universal Time (UTC), the SMS translates UTC time values into local time values for viewing purposes.

Note

We recommend that you use the SMS as your primary SNTP or NTP server. The SMS IP address is displayed at the bottom of the timekeeping panel.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Time Settings**.
3. In the **Clock Source** section, select one of the following:
   - **Manual/Internal Device Time** — Sets the internal CMOS clock. You can set this manually.

- **NTP Server** (one server required when selected) — Establishes an NTP server to record accurate log file timestamp information. Adjust the polling period as necessary, optionally set an authorization key, and specify the hostname or IP address of the NTP server. NTP settings for a device remain even after the device is unmanaged and then remanaged.

4. If you select **NTP Server (one server required when selected)**, do the following:
   a. Adjust the polling period as necessary (32 seconds is the default).
   b. You can optionally add authentication keys. Select **Auth Keys** > **New** in the Authentication Keys window.

      A Key ID can be a number between 1 and 655535 that corresponds to a Key ID on a server. The Authentication Key value corresponds to an authentication key on an NTP server.
   c. To set up NTP Servers on the device, click **New** on the Time Settings page.
   d. Specify the hostname or IP address, version (1–3 for IPS devices), authentication preferences (optional), and whether the configured NTP server is the preferred NTP server.
5. From the **Time Zone** section, select a location and city.
6. Click **OK.**

Configure time settings (N-Platform and NX-Platform)

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **Time Settings**.
3. In the **Clock Source** section, select one of the following:
   - **Manual/Internal Device Time** — Sets the IPS to use its internal CMOS clock.

- **NTP Server (one server required when selected)** — Sets the IPS to use an NTP server.
- **Remote SNTP Server** — Sets the IPS to use an Simple Network Time Protocol (SNTP) server. You must define the **Primary SNTP Server Address**. Optionally, you can define a second server.

4. If you select **NTP Server (one server required when selected)**, do the following:
   a. Adjust the polling period as necessary. The default is 16 seconds.
   b. You can optionally add authentication keys. Select **Auth Keys** > **New** in the Authentication Keys window.

      A Key ID can be a number between 1 and 655535 that corresponds to a Key ID on a server. The Authentication Key value corresponds to an authentication key on an NTP server.
   c. To set up NTP Servers on the device, click **New** on the Time Settings page.
   d. Specify the hostname or IP address, version (1–3 for IPS devices), authentication preferences (optional), and whether the configured NTP server is the preferred NTP server.
   e. Click **OK**.
5. If you select **Remote SNTP Server**, do the following:
   a. To **Use the SMS as the Primary SNTP Server**, select the check box.
   b. Enter the **Primary SNTP Server Address**.
   c. Enter the **Secondary SNTP Server Address**.
   d. Enter a **Duration** amount in minutes.
   e. Enter an **Offset** amount in seconds.
   f. Enter a **Port**.
   g. Enter a **Timeout** amount in seconds.
   h. Enter the amount of **Retries**.

6. To enable daylight saving time, select the **Automatically adjust clock for daylight saving changes** check box.

7. From the **Time Zone** drop-down menu, you can choose from the following time zones:

Abbreviation	Offset from UTC (hours)	Daylight savings time	Time zone name
ACST	+9.5	OFF	AU Central Standard Time
AEST	+10	OFF	AU Eastern Standard/Summer Time
AKST	-9	OFF	Alaska Standard Time
AST	-4	OFF	Atlantic Standard Time
AWST	+8	OFF	AU Western Standard Time
CET	+1	OFF	Central Europe Time
CST	-6	OFF	Central Standard Time
EET	+2	OFF	Eastern Europe Time
EST	-5	OFF	Eastern Standard Time
GMT	0	OFF	Greenwich Mean Time
HST	-10	OFF	Hawaiian Standard Time
JST	+9	OFF	Japan Standard Time
KST	+9	OFF	Korea Standard Time
MSK	+3	OFF	Moscow Time
MST	-7	OFF	Mountain Standard Time
NST	-3.5	ON	Newfoundland Standard Time
NZST	+12	ON	New Zealand Standard Time
PST	-8	OFF	Pacific Standard Time
WET	0	OFF	Western Europe Time

Abbreviation	Offset from UTC (hours)	Daylight savings time	Time zone name
GMT-12	-12	OFF	Time zone GMT-12
GMT-11	-11	OFF	Time zone GMT-11
GMT-10	-10	OFF	Time zone GMT-10
GMT-9	-9	OFF	Time zone GMT-9
GMT-8	-8	OFF	Time zone GMT-8
GMT-7	-7	OFF	Time zone GMT-7
GMT-6	-6	OFF	Time zone GMT-6
GMT-5	-5	OFF	Time zone GMT-5
GMT-4	-4	OFF	Time zone GMT-4
GMT-3	-3	OFF	Time zone GMT-3
GMT-2	-2	OFF	Time zone GMT-2
GMT-1	-1	OFF	Time zone GMT-1
GMT+1	+1	OFF	Time zone GMT+1
GMT+2	+2	OFF	Time zone GMT+2
GMT+3	+3	OFF	Time zone GMT+3
GMT+4	+4	OFF	Time zone GMT+4
GMT+5	+5	OFF	Time zone GMT+5
GMT+6	+6	OFF	Time zone GMT+6
GMT+7	+7	OFF	Time zone GMT+7
GMT+8	+8	OFF	Time zone GMT+8
GMT+9	+9	OFF	Time zone GMT+9
GMT+10	+10	OFF	Time zone GMT+10

Abbreviation	Offset from UTC (hours)	Daylight savings time	Time zone name
GMT+11	+11	OFF	Time zone GMT+11
GMT+12	+12	OFF	Time zone GMT+12

Note

The device keeps internal time information in Coordinated Universal Time (UTC) format. Log messages and other timestamp information is translated from UTC to the local time zone that you configure using timekeeping options.

8. Click **OK.**

TSE settings

Configure the global settings for the Threat Suppression Engine (TSE).

You can configure the global settings for the Threat Suppression Engine (TSE). These options include the following:

- **Connection Table Timeout** — The value for the global connection table timeout. This value is 30-1800 seconds. This value applies to all blocked streams in the connection table, and determines the amount of time that elapses before that connection is cleared from the connection table. Before that period of time elapses, any incoming packets for that stream are blocked at the box. After the connection is cleared, the incoming connection is allowed (if its action set has changed) or re-added to the blocked list. Separate settings are available for TCP and non-TCP traffic.
- **Trusted Streams** — Specifies the global timeout interval for the trust table. This value determines the time interval that elapses before the trusted connection is cleared from the trust table.
- **Asymmetric Network** — The dynamic sharing and use of bandwidth for increased network traffic performance. If you configure the device through the TSE configuration for an asymmetric network, the SYN flood detection, or DDoS filters, will be disabled. In effect, the TSE will

not see both sides of a TCP connection. SSL inspection cannot occur in asymmetric mode. Consult your device documentation for a list of additional filters that cannot be run in asymmetric mode.

- **Quarantine**— Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses can be automatically released, if that option is selected.

Note

If you unmanage and then remanage a device, the quarantine settings are reset to the default values.

- **GZIP Decompression**— When enabled, permits decompression of GZIP HTTP responses.
- **IDS Mode**—When enabled, automatically configures the device to operate in a manner similar to an Intrusion Detection System (IDS).
  - Performance protection is disabled. As a best practice, enable this option and set it to **Always**.
  - Adaptive Filtering mode is set to Manual.
  - Filters currently set to Block are not switched to Permit, and Block filters can still be set.

Note

Using an IPS/TPS device in a mixed configuration is not supported. When an IPS/TPS device is used in an IDS configuration, then it is an IDS device. Use the IPS/TPS as *either* an IDS device or an IPS device, but not both. Attempting to run your device in mixed mode will lead to performance issues.

Note

You must reboot the device for any changes to take effect.

- **HTTP Response Processing**—Specifies inspection of encoded HTTP responses.
  - **Accelerated inspection of responses**: Hardware acceleration is used to detect and decode encoded HTTP responses.
  - **Inspection of responses**: Enables strict detection and decoding of encoded HTTP responses.
  - **Ignore responses**: The device does not detect or decode encoded HTTP responses.

Note

Some of these options are only available on TPS devices and IPS devices running specific TOS 3.2.x versions.

- **DNS Reputation**

Note

Some of these options are only available on TPS devices and IPS devices running specific TOS 3.2.x versions.

Create sFlow® collector

TPS devices running TOS v5.*x.x* and later, and NX-Platform devices support export of flow data statistics for visualization and analysis based on the sFlow technology standard.

Statistics and flow data summaries can be viewed and analyzed by the SMS. The information can be used with external visualization and Network Behavior Anomaly Detection (NBAD) solutions to help identify compromised hosts and other suspicious and malicious network traffic.

When sFlow is enabled, it samples the packets on a segment and sends the data as a UDP packet to one or more servers. Port 6343 is the default sFlow

collector port. You can send sFlow monitoring data from a device to one or more sFlow servers, including the SMS Collector. To start receiving sFlow data at a server, sFlow must also be enabled on one or more physical segments. The sampling rate is also set on each individual segment.

The SMS has the ability to auto-configure the sampling rate on the devices to maintain optimal SMS performance. When sFlow data is first collected, the SMS establishes a resource performance threshold by measuring the amount of disk space used by incoming sFlow data to be processed. If the threshold is exceeded and then increases again with a subsequent measurement, the sFlow sample rate gets cut in half on all segments. If another higher threshold is exceeded, the SMS automatically turns off the sFlow Collector. When performance stabilizes below the initial threshold, the sFlow Collector automatically turns back on. If necessary, the SMS Collector can be manually disabled and enabled using the **`service sflowd stop`** and **`service sflowd start`** commands, respectively.

Note

The option to use sFlow is available only when editing the configuration for an NX-Platform IPS system that is running TOS v3.6 or later and a TPS system running TOS v5.*x.x*. vTPS devices do not support sFlow sampling. If there are no devices configured for sFlow sampling, the following warning message is displayed at the bottom of the Reports panel:

```
Currently there are no devices configured with the SMS as an sFlow® Collector.
There may still be historical results.
```

Procedure

1. Complete a successful profile distribution to all the devices that the sFlow reports will be run against.

   This creates a policy association, which the Vertica database requires in order to generate a report.

2. Select **Devices** > **All Devices** > **[device name]**, and then click **Device Configuration**.

3. Select **sFlow**.

4. Select **Enabled** to allow an sFlow data report to be sent to a collector, and specify up to two sFlow collector servers for report analysis. You must enable sFlow on at least one physical segment before sFlow data can be received at a collector. The SMS prompts you if an sFlow report is attempted without a configured collector server.
5. If the SMS only has a single IP address configured for sFlow, select from the following:
   - **Use SMS Collector** — Select this option to automatically populate the IP address of the SMS and the default collector port (6343). The generated sFlow reports are displayed on the Dashboard.

     Note

     The SMS Collector server automatically adjusts the device sampling rate as required to maintain optimal SMS performance.

   - **Use a Remote Collector** — Specify the IP address and the port (default is 6343). Use this option if you require visualization and Network Behavior Anomaly Detection (NBAD), which is useful in identifying compromised hosts and suspicious network traffic.
   - (Optional) Enter the IP address and port for the second sFlow collector.
6. If the SMS uses both IPv4 and IPv6 for sFlow, select from the following:
   - **Use SMS as Collector with IPv4 Address** — Select this option to automatically populate the IPv4 address of the SMS and the default collector port (6343).
   - **Use SMS as Collector with IPv6 Address** — Select this option to automatically populate the IPv6 address of the SMS and the default collector port (6343).
   - **Use a Remote Collector** — Specify the IP address and the port (default is 6343). Use this option if you require visualization and Network Behavior Anomaly Detection (NBAD), which is useful in identifying compromised hosts and suspicious network traffic.

- (Optional) Enter the IP address and port for the second sFlow collector.

7. Click **OK**.

Enable FIPS on an IPS device

Before you begin

Before you can enable FIPS on a managed IPS device, you must make sure that FIPS mode is disabled on the SMS. If the SMS does have FIPS mode enabled, enable FIPS on the IPS device using the IPS CLI. Refer to the product document for your IPS device.

Note

You must reboot the device to completely enable or disable this service.

The following table describes the FIPS settings available for IPS devices.

Setting	Description
None	No FIPS compliance actions or restrictions are activated on the device.
Crypto	The device uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. You must reboot the device for the system to operate in FIPS Cryptography mode.
Full	The SMS displays the Changing FIPS Mode wizard. Complete this wizard to enable full FIPS mode on the device. The SMS will delete all existing users on the device and will replace it with the user defined in the wizard. The SMS will also rekey the device with a FIPS compliant key.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **FIPS Settings**.

3. For **FIPS Mode**, select the **Full** radio button, and then click **OK**.
4. Click **Next** when the Changing FIPS Mode wizard is displayed.
5. Enter a username, enter and confirm your password, and then click **Next**.
6. Review your choices and click **Finish**.
   - If the SMS can communicate with the TMC, it will download and install the FIPS key package.
   - If the SMS cannot communicate with the TMC, the following error message instructs you to manually rekey the device:
7. Close the message and download the FIPS key package from the TMC to your computer.
8. After the device completes rebooting, navigate to **System** > **Update** > **Install Package** on the device LSM.
9. In **Step 4** of the Install Package page, browse to your FIPS key package and click **Install Package**.

   If you receive the following error message, click OK, manually reboot the device, and repeat the previous two steps. The IPS should accept this second attempt to install the FIPS key package.

What to do next

Verify that the device is in Full FIPS mode by doing any of the following:

- Enter `sh fips` on the CLI.
- From the SMS, select the Device Configuration for your device and view the **FIPS Mode** status under **Management Services**.

If you see a `Socket Closed` SMS error message when trying to add an IPS in FIPS mode, run the `fips restore-ssl` command from the IPS CLI.

After running this command, navigate to the **System** > **Update** > **Install Package** on the device LSM to reinstall the FIPS key package. This ensures that the IPS will use keys that meet FIPS strength requirements.

Enable FIPS on a TPS device

If your device supports FIPS mode, you can allow management services for the device to be installed into a Federal Information Processing Standard (FIPS) Security Level 2 tamper-resistant hardware security module. When enabling FIPS mode on a supported device, review all the warning messages that display on the SMS.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Device Configuration**.
2. Select **FIPS Settings**.
3. Select one of the following settings.
4. On the Device Configuration page, select **FIPS Settings**.

Setting	Description
None	No FIPS compliance actions or restrictions are activated on the device.
FIPS Enabled	The device uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. You must factory reset the TPS device before you enable FIPS mode. To disable FIPS mode, you must factory reset the device. The following authentication settings are not supported on the TPS device: • RADIUS • TACACS+ SNMP settings do not support MD5 and DES protocols when the TPS device is in FIPS mode. The SMS must have a 2K key installed to communicate with the TPS device in FIPS mode.

5. Click **OK**.

Packet trace

Packet trace is a useful tool that captures all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.

Packet trace options are available for devices that support the packet trace feature. Devices, such as the Core Controller and the SSL do not support packet trace. See *Save all packet trace information for a device on page 3-93*.

Save all packet trace information for a device

Opens a file chooser dialog where you can provide a location on the client system for saving all the packet trace information for the selected device. Packet trace files are merged into one PCAP file.

Procedure

1. On the Devices (All Devices) screen, right-click a device in the graphics pane or right-click a device listing the table.
2. Select **Packet Traces (all)** and then the **Save** option to save all the packet trace information for the selected device.
3. Browse to the area where you want to save the packet trace information, and then click **Save**.

Download all packet trace files for a device to the SMS

Download all the packet trace information for the selected device into the Exports and Archives section of the SMS client.

Procedure

1. On the Devices (All Devices) screen, right-click a device in the graphics pane or right-click a device listing the table.
2. Select **Packet Traces (all)** and then the **Download to the SMS** option to download all the packet trace information for the selected device.

When the download is complete, a popup message displays the location where the PCAP file was downloaded and provides an active HTML link to the files.

Import or export device configuration

The SMS provides export and import functions of the settings that you can use to configure device settings that are common across multiple devices. The first step is to configure a device with the settings that you want to use across multiple devices. The settings can be exported to a device settings file. The device settings in the file can then be imported into multiple devices.

This option is useful when deploying multiple devices that have the same or similar configuration requirements. For devices with similar configurations requirements, you can set up base settings that can then be tuned on each device after the settings file is imported.

Note

Depending on the managed device, some device configuration settings do not support import/export. For example, you cannot import or export FIPS Settings.

Import device configuration

Import device configuration settings.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Import Configuration**.
2. Specify the name and location of the file to be imported or click **Browse** to find and select the file.

   To review the settings in the import file, click **View Details**.
3. Select **Device Configuration Settings** from the left navigational menu or click **Next**.

4. Do one of the following:
   - To import all of the device settings, select the check box labeled **Select All Options**.
   - To import specific device settings, select the check boxes associated with the desired settings.

Note

When you import settings from a device that authenticates using RADIUS or TACACS+, select the **Remote Authentication** checkbox to include those settings in the import.

5. Select **Device Targets** from the left navigational menu or click **Next**.
6. Select the device or devices that are the targets for the imported settings. If a device is grayed out or lists an error, the device might not be compatible with the device settings, be unmanaged, or have another issue.
7. To view the status details of a listed device, click the device listing. The status summary displays in the table below the **Target** table.
8. Click **Finish** to import the selected setting from the import file to the selected target devices.

Export device configuration

Export device configuration settings.

Procedure

1. Select **Devices** > **All Devices** > **device**, and then click **Export Configuration**.
2. Specify the location for the exported file.
3. Do one of the following:
   - To export all of the device settings, select **Select All Options**.

- To export selected specific device settings, select the settings you want to export.

Note

When you export settings from a device that authenticates using RADIUS or TACACS+, select the **Remote Authentication Settings** checkbox to include those settings in the export.

4. Click **OK.**

Remote Authentication

Select **Devices** > **All Devices** > **Device** > **Authentication** to configure remote authentication groups, servers, and administrative login privileges. Click **Edit** to specify the source that the managed device uses to authenticate users.

- **Local** — The SMS stores a hashed password for the user account and authenticates against a user database stored locally on the device.
- **SMS as Authentication Source** — The SMS is responsible for user authentication. If you choose to use SMS as the authentication source, specify the **Time Out Interval** (in number of seconds) and make sure that SMS port 443 is open and accessible by the device.
- **RADIUS as Authentication Source** — Authentication is performed on the RADIUS server; user role and access rights are maintained on the SMS server. You can specify up to three RADIUS servers. Note that user management remains on the device.
- **TACACS+ as Authentication Source** — Authentication is performed on the TACACS+ server; user role and access rights are maintained on the SMS server. You can specify up to three TACACS+ servers. Note that user management remains on the device.

Note

RADIUS authentication is supported on N-Platform and NX-platform devices running TOS v3.7.0 or later and all TPS and vTPS devices. If the device does not support RADIUS authentication, the RADIUS options are disabled. TACACS+ authentication is supported only on N-Platform and NX-platform devices running TOS v3.8.0 or later. If the device does not support TACACS+ authentication, this option is disabled.

Authentication preferences

For managed TPS devices and IPS devices running TOS v.3.3 and later, the SMS supports user authentication for individual devices.

Note

In order for TPS devices to use the SMS as an authentication source, SMS port 443 must be open and accessible by the device.

From the Device Configuration screen for a managed device, you can set the following user authentication preferences:

- **Security Level** — None (level 0), Low (level 1), Medium (level 2), or High (level 3).
- **Maximum Login Attempts** — Login attempts from 1 to 10.
- **Failed Login Action** — Disable account and/or lockout IP address, lockout account and/or IP address account (default setting), or audit event.
- **Lockout Time** — Lockout time from 1 to 1440 minutes.

Local Authentication Only

The SMS stores a hashed password for the user account and authenticates against a user database stored locally on the TPS device.

Note

This option only appears on TPS devices.

The following password expiration options apply to accounts that are configured for local authentication only:

- **Password Expiration** — The minimum expiration period is 10 days, and the maximum expiration period is one year.
- **Password Expiration Action** — Force user to change password; notify user of expiration; or deny login, SuperUser must reset password.

Note

You cannot disable the password expiration for a Threat Protection System (TPS) device; therefore, **Disabled** is not available as an option.

Import an X509 certificate

Procedure

1. On the RADIUS tab, click **Import** to the right of the Primary RADIUS Certificate panel.
2. Select the X509 certificate file from your local drive or storage media, and click **Import**.

   To clear the current certificate, click **Reset**.

   Important

   A certificate import or reset does not get saved until the entire device configuration is saved by clicking **OK** on the Device Configuration wizard.

Specify one or more RADIUS servers for IPS

Procedure

1. On the Device Configuration Authentication Preferences screen, select the **RADIUS as Authentication Source** option in the Remote Authentication section.
2. In the RADIUS Servers section, click **Edit** next to the Primary, Secondary, or Tertiary Server IP.
3. In the RADIUS Server Configuration dialog, configure the RADIUS server options described in the following table.

Setting	Description
IP Address	IP address of the RADIUS server.
Port	Port on the RADIUS server that listens for authentication requests; the default is port 1812.
Authentication Protocol	Authentication method used on the RADIUS server: • PAP (default) • MD5 • PEAP/EAP-MSCHAPv2 To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server. You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see *View certificates on page 8-56*.
Secret/Confirm Secret	String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.
Timeout	Timeout, in seconds, for communication with the RADIUS server. Default is 3.

Setting	Description
Attempts	Number of times communication with the RADIUS server is attempted. The default is 1 (no retries after first unsuccessful attempt to contact RADIUS server).

Note

An IPS device that is managed by the SMS cannot have more than one RADIUS server configured with duplicate IP address, port, and authentication protocol settings.

4. Test the RADIUS configuration by entering a valid User Name and Password for the server (and confirming), and then clicking **Test**.
5. Click **OK** to save the server configuration as an authentication preference.

Note

To save the server configuration to the SMS and to the device, you must click **OK** on the Device Configuration wizard.

An X509 certificate is required for validating PEAP/EAP-MSCHAPv2 authentication responses. The certificate is generated on the RADIUS server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.

Note

Invalid certificates, including expired and revoked certificates, can still be used according to the administrator's discretion.

Specify one or more TACACS+ servers for IPS

Procedure

1. On the Device Configuration Authentication Preferences screen, select the **TACACS+ as Authentication Source** option in the Remote Authentication section.
2. In the TACACS+ Servers section, click **Edit** next to the Primary, Secondary, or Tertiary Server IP to configure a TACACS+ server.
3. In the TACACS+ Server Configuration dialog, configure the TACACS+ server options described in the following table.

Setting	Description
IP Address / Hostname	IP address or hostname of the TACACS+ server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can contain an unqualified hostname or a fully qualified hostname (hostname+domain name).
Port	Port, between 1 and 65535, on the TACACS+ server that listens for authentication requests; the default is port 49.
Authentication Protocol	Authentication method used on the TACACS+ server: • ASCII • PAP (default) • CHAP • MSCHAP
Secret/Confirm Secret	Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 63 characters.
Timeout	Timeout, between 1 and 15 seconds, for communication with the TACACS+ server. Default is 15.
Attempts	Number of times, between 1 and 10, communication with the TACACS + server is attempted. Default is 3 attempts.

Note

An IPS device that is managed by the SMS cannot have more than one TACACS+ server configured with duplicate IP address, port, and authentication protocol settings.

4. Test the TACACS+ configuration by entering a valid User Name and Password for the server, and then clicking **Test**.
5. Click **OK**. This saves the server configuration changes to the Device Configuration dialog only.

Important

To save any of the device configuration changes you just made, you must click **OK** on the Device Configuration wizard.

TippingPoint Operating System

When TippingPoint identifies new attacks or improves methods of detecting existing attacks, the TMC makes the updates available to customers in the form of software packages. Software packages are upgrades to your IPS operating system. DV filter packages contain newly developed attack, peer-to-peer, and anomaly filters along with improvements to existing filters.

Through the Devices screen, you can check for update notifications for the TOS. The SMS client allows you to download and store the TOS files on the system. The packages display on their own screens providing quick review of which devices have received the updates. You can also distribute the updates from each page. The TMC notifies you that new packages are available on the Dashboard.

The following table defines the TOS Inventory details. The Distribution Progress table provides information on distribution status of the TippingPoint OS. *Learn more on page 5-61*.

Column	Description
Version	Version number of the TOS.
Product	Models that the selected TOS package supports.
Released	Date and time of the released version of the TOS.
Downloaded	Date and time of the download to the SMS.
Devices	The number of devices defined on the SMS that are running this release.

Import TOS

The TOS software updates the operating system software for devices. The Devices (TippingPoint OS) screen allows you to download and import many versions of the software to give you more control over your device software. You can import and download updated versions of the TippingPoint operating system (TOS) for distribution to your TippingPoint system.

When you add a new device on the SMS, the TOS version list is updated the next time the SMS contacts the TMC. You can refresh the TOS inventory list. (Select **Download from TMC** > **Refresh**).

Procedure

1. In a Web browser, open https://tmc.tippingpoint.com.

   If you have not already done so, create a TMC account using your Customer ID and Serial Number.

2. From the top menu bar on the TMC home page, click **Releases** > **Software** > **[model_type]** > **[model_number]**.

3. Locate the package you want to download and follow the download instructions for your specific browser. To avoid unexpected behavior on the SMS, do not change the name of this file.

4. Select **Devices** > **TippingPoint OS** > **Import**.

5. Browse to and select the TippingPoint OS software package file.

Download TOS software

Procedure

1. Select **Devices** > **TippingPoint OS**.
2. Click **Download from TMC** under TOS Inventory.
3. Verify that the Available Device Software selection is correct, and click **Download**.

Distribute the TOS

After you have downloaded and imported TippingPoint OS software packages into the SMS, you can distribute the updates to devices.

You can also review the details and manage the available TOS entries in the TOS Inventory section. You can keep multiple versions of the TOS software. You can distribute the software updates to all devices or a particular device group.

Procedure

1. Select **Devices** > **TippingPoint OS** > **TOS Inventory**, and select a TippingPoint OS software package file.
2. Click **Distribute**. You cannot cancel a TOS update when it is in-progress.

Delete a previous TOS version

Procedure

1. Select **Devices** > **All Devices** > **device** > **Device Configuration**.
2. Select **System Update**.

3. From the Previous TOS Versions table, select a software version entry, and click **Delete**.

Rollback to a previous version

A rollback operation reverts the currently running software on your device to a previous working version that you select.

Before you begin

Before you roll back to a software version, make sure to review the release notes for any specific notations and warnings regarding the functionality for that version. After you install the 2K key, you will lose device management functionality on the SMS, if you roll back to TPS devices running TOS v4.0. Learn more: *SMS certificate key on page 8-9*.

Important

(TPS and vTPS only) After you roll back, always make sure the master key on the device is the same as the master key that was used to secure the keystore in the rollback TOS image.

A TPS device stores a maximum of three previous TOS versions that you can roll back to. If all three rollback slots are full, the oldest version gets overwritten when you perform your next TOS upgrade. To preserve the oldest TOS version from being overwritten, specify and delete another TOS version before you upgrade your TOS. *Learn more on page 3-104*.

Procedure

1. Select **Devices** > **All Devices** > **device** > **Device Configuration**.
2. Select **System Update**.
3. From the Previous TOS Versions table, select a software version entry, and click **Previous Version Rollback**.

What to do next

(TPS and vTPS only) When the rollback completes, verify the master key on the device is the same as the master key that was used to secure the keystore in the rollback TOS image. From the CLI, edit and save the configuration. If a "Device keystore is locked" message is displayed, the master key does not match. To resolve this issue, complete the following steps:

- If you know the master key that was set in the TOS rollback image, set the master key to that passphrase. Use the `master-key set` CLI command to set the master key.
- If you do not know the master key:
  1. (TOS 4.x.x images only) Clear the master key and reset the keystore by using the `master-key clear reset-keystore` CLI command.
  2. (TOS 5.x.x and later images only) Reset the keystore by using the `master-key reset-keystore` CLI command.
  3. Reset the master key by using the `master-key set` CLI command.
  4. If the keystore persisted sensitive information, such as private keys for SSL inspection, import the private keys into the keystore and assign the new keys to the appropriate SSL servers.
  5. If the external user disk is encrypted, synchronize the ThreatDV URL Reputation Feed and User-defined URL Entries database to the device.

Note

If you change the master key while the external user disk is encrypted, the contents of the external user disk, which include the ThreatDV URL Reputation Feed and User-defined URL Entries database, are erased.

Snapshots

Create a new system snapshot on the device

The snapshot procedure might take time. Allow sufficient time for the procedure to complete.

Procedure

1. Select a device, expand the device entry in the left navigational menu, and then expand the **Device Configuration** entry.
2. Select the **System Update** entry. The Device Configuration (System Update) screen displays.
3. From the System Snapshots area, click **New**.
4. A new snapshot image is created of the device and the entry displays in the table.

Import a system snapshot from a file

Import a snapshot to the SMS.

Procedure

1. Select a device, expand the device entry in the left navigational menu and expand the **Device Configuration** entry.
2. Select the **System Update** entry. The Device Configuration (System Update) screen displays.
3. From the System Snapshots area, click **Import**.
4. Browse to and select the local file, and then click **OK**.

Archive a system snapshot to the SMS

Archive a snapshot to the SMS.

Procedure

1. Select a device and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
3. In the System Snapshots table, select a snapshot to archive.
4. Click **Archive to SMS.**

Export a system snapshot to a file

Export a system snapshot from the SMS.

Procedure

1. Select a device and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
3. In the System Snapshots table, select a snapshot to export.
4. Click **Export**.
5. Select a location for the file export.

Restore from a system snapshot

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

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

When you restore a snapshot, keep in mind the following points:

- The contents of the system keystore are not included in the snapshot. When you restore a snapshot to a different device, you should plan to also import any private key information from the device where the snapshot was taken.

- When you want to restore a snapshot to a different device, and URL Reputation Filtering is enabled, a full synchronization of the Reputation database is required after you restore the snapshot. The snapshot does not include the ThreatDV URL Reputation Feed and User-defined URL Entries database. For more information, see the *SMS User Guide*.
- The snapshot includes the license package. The license package provides license information for each of your TippingPoint devices. If the license package that was included in the snapshot is outdated, restore the snapshot and then download and install an updated license package from the TMC.
- (TX Series/TXE Series) The port configuration for each slot is preserved after you restore a snapshot when the same I/O module is installed in the same slot. Otherwise, the port configuration resets to the default.
- If an external ZPHA was configured on the original device, be sure to add an external ZPHA to the target device or update the device configuration to remove ZPHA.

Procedure

1. Select a device and expand the **Device Configuration** entry.
2. Select the **System Update** entry.
3. In the System Snapshots table, select a snapshot to rollback to and click **Restore**. When you rollback, the snapshot overwrites all settings for a profile to the device with the snapshot settings.

Delete a system snapshot

This action deletes the system snapshot from the device and, if present, the snapshot on the SMS.

Procedure

1. Select a device and then expand **Device Configuration**.
2. Select the **System Update** entry.

3. In the System Snapshots table, select a snapshot to delete.
4. Click **Delete**.
5. If a confirmation message displays, select the appropriate option to delete the snapshot.

Virtual segments

Virtual segments can be set up to define traffic using a VLAN ID, an endpoint pair (source and destination IP addresses of a packet), or both. One or more physical segments are then assigned to the virtual segment. Virtual segments are members of a segment group and the assigned devices are not exposed in segment group membership. You define the priority order for virtual segment so that any overlapping definitions are resolved. Attempting to define an overlapping virtual segment on a device which does not allow it will produce an error.

Virtual segments can be used as:

- A target for distribution
- Search criteria in events and reports

The Virtual Segment table is an inventory listing of the currently defined virtual segments and lists the following information:

- **Order** — Priority order that allows resolution for overlapping definitions. Keep in mind the following points:
  - You cannot have a virtual segment with an overlapping VLAN ID on the same physical segment.
  - A user-defined virtual segment with a specified VLAN ID takes precedence over a physical segment (any VLAN).
  - A packet can only be assigned to a single segment and will only be inspected against a single profile.
- **Name** — User-defined name of the virtual segment.
- **VLAN** — VLAN associated with the virtual segment.

- **Src/Dest Addr** — Source/Destination address of a layer 2 virtual segment.
- **Segments Assigned** — User-assigned physical segments associated with the virtual segment.
- **Segment Group** — User-created segment group associated with the virtual segment.
- **Profile Name** — Name of profile associated with the virtual segment.

Virtual segment considerations

When you configure virtual segments, keep in mind the following points:

- The IPS (N-Platform or NX-Platform) provides a system-defined virtual segment named **ANY-ANY** to which the default security profile is assigned. The **ANY-ANY** segment protects any traffic that does not match another inspection profile on the device. The **ANY-ANY** segment is not configurable (and is not displayed in the virtual segment table), but you can distribute your own inspection profile to the virtual segment. The priority order for virtual segments on the IPS is:
  1. User-defined virtual segments with a specified VLAN-ID and source/destination IP address.
  2. Physical segments (any VLAN)
  3. **ANY-ANY** virtual segment
- Unlike the IPS, the TPS does not provide a system-defined **ANY-ANY** virtual segment. However, you can create a “catch all” virtual segment to distribute your own inspection profile and protect network traffic that does not match another inspection profile on the device. When you create a “catch all” virtual segment, be sure to assign all physical segments and to order the virtual segment lowest in priority. The priority order for virtual segments on the TPS is:
  1. User-defined virtual segments with a specified VLAN-ID and source/destination IP address (layer 2).
  2. Physical segments (any VLAN)

- Virtual segments appear only if the user has access to the segment group for the virtual segment.
- Virtual segments can be created that do not initially contain any physical segments.
- Physical segments tied to a TOS version 2.2 or earlier device which does not support virtual segments are disabled but displayed in the physical segment lists.
- Physical segments tied to a TOS version 3.0 or earlier device are disabled if the virtual segment is CIDR based.
- IPS devices with virtual segments that were configured locally on an IPS device and then added to the SMS are merged to the global virtual segment listing.
- In a virtual segment definition, you must specify at least one VLAN ID, Source IP, or Destination IP traffic definition besides ANY.

Create a virtual segment

For better management, create a unique segment group before you create a new virtual segment.

Procedure

1. Select **Devices** > **Virtual Segments**, and then click **New**.
2. Enter the following:
   - **Name** — Must be unique among all existing virtual segments.
   - **Description** — A brief explanation about the virtual segment.
3. Complete any of the following criteria you want to use to define the traffic for the virtual segment:
   - **VLAN**— Can be one or more comma-separated VLAN IDs or a Named Resource.
   - **Source IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Range-based Named Resources is not supported.

- **Destination IP Address** — Can be one or more comma-separated CIDRs or a Named Resource. Ranged-based Named Resources is not supported.

Note

For IPS NX-Platform, TPS TX Series, and TPS TXE Series devices, the slot number is represented.

4. When the Segment Group Membership dialog box displays, select a group for this virtual segment.
5. If no custom segment groups have been created, the virtual segment is automatically assigned to the default segment group. To create a new segment group or change group membership, see *Create a segment group on page 3-115* and *Edit segment group membership on page 3-116*.
6. From the left navigational menu, select **Physical Segments**.
   - Select one or more physical segments from the **Physical Segments** list that you want to assign to the virtual segment.
   - To add a physical segment to the list, select **Add**. From the Select Physical Segment screen, select the segment or segments to add.

   When you create a virtual segment on a stack of IPS devices, the available physical segments consist of network segments on slots 1–3.

Note

For IPS NX-Platform, TPS TX Series, and TPS TXE Series devices, the segments are listed by slot numbers.

7. Click **OK** .
8. To validate the virtual segment setup, select **Validation Report**. The Validation Report screen provides information about the severity and summary of error status. To view additional information, click **Details**.
9. Click **OK**.

Delete a virtual segment

Delete a virtual segment.

Procedure

1. Select **Devices** > **Virtual Segments**.
2. Select a virtual segment, and click **Delete**.

Traffic Flow Analyzer

The traffic flow analyzer allows you to check which virtual segments match the supplied criteria for the traffic. If no matches are found of any virtual segment, the device physical segment is used.

Procedure

1. Select **Devices** > **Virtual Segments** > **Traffic Flow Analyzer**.
2. Select one or more of the following options and enter the required information:
   - Source Address
   - Destination Address
   - Device Segment
   - VLAN ID
3. Click **Find**.

Segment groups

Segment groups help you maintain settings and file distribution according to grouping of device segments. These groups provide greater management and distribution of profiles and updates for Digital Vaccine and Threat DV packages, device TOS software, and SMS software.

Depending on your network setting and architecture, you might need to have differing types and versions of filters and action sets running on particular

segments. By creating segment groups, you can associate a particular profile of filters to the group.

The Segment Groups lists the segment groups with the following information.

Column	Description
Group Name	Name of the segment group.
Members	Total number of segment members.
Profile	Name of the associated profile of filters.

Create a segment group

Segment groups are an organizational tool on the SMS. Segment groups are stored on the SMS only and are not distributed to the device.

A segment can only be a member of one group and have only one distributed profile at any given time. You cannot add a segment to multiple groups. However, you can have many profiles point to the same segment. When you distribute a profile, the segment replaces the currently used profile.

Procedure

1. Select **Devices** > **Segment Groups**.
2. Click **New**.
3. Enter a **Group Name**.
4. Enter a **Description** of up to 2048 characters.

Note

You cannot edit the Description of the default segment group.

5. Select an **Organize By** option (device or segment group).
6. Select one or more devices from the list.

- When creating a segment group for a stack of devices, choose from the physical segments on the segment reference device.
- For IPS (NX-Platform) and TPS (TX Series) devices, the Segment Group table lists the slot number associated with the segment group.

7. Click the **right arrow** to move the selected device to the Group Members list.
8. Click the **left arrow** to remove the selected device from the Group Members list and back to the Non Members list.
9. Click **OK**.

Edit segment group membership

Procedure

1. On the Devices (Segment Groups) screen, select an entry from the Members table, and do one of the following:
   - Click **Edit Membership**.
   - Right-click and select **Edit Membership**.
   - Go to the top menu bar and select **Edit** > **Edit Membership**.
2. If desired, modify the **Group Name** and **Description**.
3. In the **Non Members** pane, select how you want to organize the list: by **Device** or by **Segment Group**.
4. Select one or more devices from the list. You can select multiple devices by clicking and dragging your cursor over the names and using the **SHIFT** and **CTRL** keys.
5. Click the right arrow button to move the selected device to the right members pane.
6. If you want to remove a device or devices from the segment group, select a device or multiple devices from the Group Members area, and then click the left arrow button to move the device or devices.

Note

For IPS NX-Platform, TPS TX Series, and TPS TXE Series devices, the Segment Group table lists the slot number associated with the segment group.

7. Click **OK**.

Edit the name and descriptions for a segment group member

Procedure

1. On the Devices (Segment Groups) screen, select an entry from the Members table, and do one of the following:
   - Click **Edit**.
   - Right-click and select **Edit**.
2. Make desired modifications to the **Name** and **Description**.

   Learn more on page 3-35 about restrictions on how to name segments.
3. Click **OK**.

Edit permissions for a segment group member

Procedure

1. On the Devices (Segment Groups) screen, select an entry from the Members table.
2. Go to the top menu bar and select **Edit > Permissions**.

   The Segment Group - Permissions dialog displays.
3. By default, permissions are granted to SuperUsers. If you want to grant permissions to other roles, select the appropriate check box in the Permissions area.

4. Click **OK**.

Advanced DDoS tasks

This section includes the following topics:

Advanced DDoS supported models

The SMS supports DDoS for the following devices:

- 5200NX/7100NX (TOS 3.5 and later)
- 2600NX/7500NX (TOS 3.6 and later)
- 440T/2200T (TOS 4.0 and later)
- 1100TX/5500TX (TOS 5.2 and later)
- 8200TX/8400TX (TOS 5.0 and later)
- 9200TXE (TOS 6.0 and later)

Go to Profiles to enable the SYN Proxy filter. The SYN Proxy Threshold setting and Advanced DDoS configuration options for these devices are configured when you edit Profile filters. See *Advanced DDoS on page 5-49*.

Advanced DDoS filter configuration

To view supported advanced DDoS filter configuration settings for devices, see *Advanced DDoS on page 5-49*.

To configure an Advanced DDoS report template, see *Advanced DDoS templates on page 7-8*.

Chapter 4

Ports

The SMS includes the following ports:

Proxy server port information

A proxy server can be used for TMC access if required in your network. To update the TMC proxy connection, select **Admin** > **Server Properties** > **Network** > **TMC Proxy**.

If your security policy requires you to restrict access by hostname, contact your TippingPoint product representative for a current list of required hosts.

Required ports

The SMS requires certain ports to be available including:

- *Ports required to use the SMS client on page 4-2*
- *Ports required for the SMS to manage devices on page 4-3*
- *Ports required for software and security updates on page 4-3*
- *Network ports required for the SMS to perform WhoIs lookups on page 4-4*

Ports required to use the SMS client

The following ports are required to use the SMS client.

Note

For TPS devices to use the SMS as an authentication source, SMS port 443 must remain open.

Port	Service	From	To	Description
22/TCP	SSH	SMS client	SMS server	CLI management of the SMS.
9033/TCP	SMS	SMS client	SMS server	Required for the SMS client to connect to the SMS server.
10042/TCP	SMS	SMS client	SMS server	Required for the SMS client to connect to the SMS server.

Port	Service	From	To	Description
443/TCP	HTTPS	SMS client browser	SMS server	File downloads, such as client installation, exported reports, or web services, if configured.
943/TCP	HTTPS	SMS server	SMS client	SMS restore.

Ports required for the SMS to manage devices

The following ports are required for the SMS to manage devices.

Port	Service	From	To	Description
161/UDP	SNMP agent	SMS server	IPS	SMS management.
443/TCP	HTTPS	SMS server	TPS, IPS, DD Analyzer	SMS management.
8162/UDP	SNMP trap	IPS/TPS	SMS server	SNMP traps from device to SMS.
8163/UDP	SNMP trap	IPS/TPS	SMS server	SNMP traps from device to SMS.
8443/UDP		Identity Agent	SMS server	SMS management.

Ports required for software and security updates

Network ports are not required when you configure the Proxy Server Port to access the TMC for software and security updates. You can also manually download packages from the TMC.

Port	Service	From	To	Description
443/TCP	HTTPS	SMS server	Outbound msd.tippingpoint.com	Digital Vaccine updates from TMC

Port	Service	From	To	Description
443/TCP	HTTPS	SMS server	TMC ws.tippingpoint.com	Updates from TMC For new SMS installations, this port is the **NEW** default for communication with the TMC

Network ports required for the SMS to perform WhoIs lookups

The following ports are required for the SMS to perform WhoIs lookups.

Port	Service	From	To	Description
43/TCP	WhoIs	SMS server	whois.arin.net whois.apnic.net whois.ripe.net whois.lacnic.net	Perform WhoIs lookups

Optional ports

The SMS includes other ports available for optional tasks including:

- *Device ports on page 4-4*
- *SMS server ports on page 4-5*
- *SNMP ports on page 4-6*

Device ports

The following device ports are optional.

Port	Service	From	To	Description
123/UDP	NTP	IPS	SMS server	Required only if IPS uses SMS for NTP time synchronization.
6343/UDP	sFlow®	IPS	sFlow server	Send sFlow data from TPS devices running TOS v5.*x.x* and NX-platform IPS devices to one or more sFlow servers.
10043/TCP	SMS provision	IPS	SMS server	Remote authentication for NX devices only.
443/TCP	URL Threat Analysis	SMS server	DD Analyzer	Send URL data from the SMS to the DD Analyzer.

SMS server ports

The following SMS server ports are optional.

Port	Service	From	To	Description
389/TCP/UDP	LDAP non-SSL	SMS server	AD server	SMS AD LDAP authentication
636/TCP/UDP	LDAP over SSL	SMS server	AD server	SMS AD LDAP over SSL authentication
3306/TCP	Database	SMS server	Any	External database access
			External server	External replication
53/TCP/UDP	DNS	SMS server	Name server	Name resolution
135/TCP/UDP	IP correlation	SMS server	AD server	SMS server and AD communication for IP correlation
239/UDP	IP2ID	SMS server	IPS (A10)	IDsentrie
111/TCP/UDP	NFS	SMS server	File server	Report export, database backup

Port	Service	From	To	Description
369/TCP/UDP				
2039/TCP/UDP				
123/UDP	NTP	SMS server	NTP server (time source)	Time synchronization from external NTP server
1812/UDP	RADIUS	SMS server	RADIUS server	SMS user authentication
49/TCP	TACACS+	SMS server	TACACS+ server	SMS user authentication
137/TCP/UDP	Samba	SMS server	File server	Report export, database backup
138/TCP/UDP				
139/TCP/UDP				
1512/TCP/UDP				
25/TCP	SMTP	SMS server	Mail server	Email notifications such IPS events, Responder
514/UDP	Syslog	SMS server	Syslog server	SMS audit and syslog
943/TCP		SMS server	External system	SMS backup/restore

SNMP ports

The following SNMP ports are optional.

Port	Service	From	To	Description
80/TCP	HTTP	SMS client browser	SMS server	File downloads, such as client installation, exported reports, web services.
161/UDP	SNMP	SNMP client	SMS server	Query SMS SNMP MIBs.

High Availability (HA) ports

Required High Availability ports that you must make available. In addition to these HA ports, required ports must be open for both primary and secondary SMS servers.

The SMS provides command options that allow you to disable or re-enable HA ports. By default all SMS devices are set to **yes** or **enabled**.

SMS to SMS HA ports

Port	Service	From	To	Description
22/TCP	SSH	SMS primary	SMS secondary	Secure remote command execution and file replication.
		SMS secondary	SMS primary	
1098/TCP	RMI	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration.
		SMS secondary	SMS primary	
1099/TCP	RMI registry	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration.
		SMS secondary	SMS primary	
10042/TCP	SMS	SMS primary	SMS secondary	CLI command replication.
		SMS secondary	SMS primary	
3306/TCP	MySQL	SMS primary	SMS secondary	Database replication.
		SMS secondary	SMS primary	
4444/TCP	RMI	SMS primary	SMS secondary	JAVA RMI for HA configuration and remote peer administration.
		SMS secondary	SMS primary	
9033/TCP	JMS	SMS primary	SMS secondary	JAVA Messaging Service for the SMS client to connect to the SMS server and for HA configuration.
		SMS secondary	SMS primary	

IPS/TPS to IPS/TPS Transparent High Availability (TRHA) ports

Port	Service	From	To	Description
9591/TCP	SSL	IPS/TPS primary	IPS/TPS secondary	TRHA messaging via SSL. Each HA ping (heartbeat) message is sent at 60 second intervals.
		IPS/TPS secondary	IPS/TPS primary	

Responder ports

You might need to open additional ports, if they are defined in your Active Response action script.

Port	Service	From	To	Description
25/TCP	SMTP	SMS server	Mail server	Active response email action
80/TCP	HTTP	SMS server	Remote host	Active response web action
162/UDP	SNMP	SMS server	Remote host	Active response SNMP action
162/UDP	SNMP	SMS server	Remote host	Active response NMS action
514/UDP	Syslog	SMS server	Syslog server	Active response syslog action
1812/UDP	RADIUS	SMS server	External switch	RADIUS proxy (required for active response switch disconnect action)

Responder triggers for port availability

Port	Service	From	To	Description
80/TCP	HTTP	SMS server	External host	Trigger active response/ via URL, IP correlation lookup, IP or MAC lookup.

Port	Service	From	To	Description
162/UDP	SNMP	SMS server	NMS server	SNMP traps from an SNMP client or NMS server, such as 3Com Network Directory (3ND) to active response.
443/TCP	HTTPS	SMS server	External host	Trigger active response via URL, IP correlation lookup, IP or MAC lookup.

SMS encryption protocols, algorithms, and cipher support

When the SMS is in FIPS mode, it does not support SSLv2 formatted hello, SSLv3, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ciphers.
The SMS does not support SSLv2 protocol at any time.

Port	Protocol	Ciphers/Algorithms	Description
443	TLSv1.0 TLSv1.1 TLSv1.2 SSLv2Hello	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	HTTPS service: • SSL provided by SunJSSE. • Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS).

Port	Protocol	Ciphers/Algorithms	Description
10042, 9033	TLSv1.0 TLSv1.1 TLSv1.2	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Client-server communication: • SSL provided by SunJSSE. • Encryption algorithms provided by SunJCE (Non-FIPS) and NSS (FIPS).
10043	TLSv1.0 TLSv1.1 TLSv1.2	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 (only supported with TLSv1.2) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Device provision manager (device remote authorization).
22	SSH-2	aes128-gcm aes256-gcm aes128-ctr aes192-ctr aes256-ctr	SSH service: • SSH provided by OpenSSH. • Encryption algorithms provided by OpenSSL.

Chapter 5

Profiles

Profiles are a collection of filters or rules that provide a method for setting up security configuration options for TippingPoint products. The SMS ships with a default inspection profile along with a standard Digital Vaccine filter package that addresses known security issues.

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

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

Profiles provide three different levels of security protection:

- **Enterprise-wide** - These settings affect all devices and segments on your network. Examples of enterprise-wide security include shared settings and security filter exceptions or restrictions. Digital Vaccine, Threat DV, and Digital Vaccine Toolkit packages also fall under this type of protection, as you can distribute these packages to all of your devices.
- **Device-wide** - These settings affect all of the segments on a particular device. Digital Vaccine, Threat DV, and Digital Vaccine Toolkit packages also fall under this type of protection, as you can distribute these packages to individual devices.
- **Segmental** - These settings affect only a particular segment or segment group.

Shared settings

Shared settings include common configuration objects that are shared enterprise-wide by all profiles on the SMS. Shared settings include:

- *Action sets on page 5-3* — Determine system policy when traffic matches a filter.
- *Notification contacts on page 5-8* — Create collections of email, syslog, or SNMP contacts that are used for notification when a policy event occurs.
- *Services on page 5-11* — Configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic.
- *SSL on page 5-11* — Add SSL server and client proxies, including the certificates, protocols, cipher suites, and the SSL service that is accepted on the SSL detection port. Refer to the *SSL User Guide* to learn more about configuring SSL inspection.

Action sets

Action sets determine what the device does when a packet matches a filter. An action set can contain more than one action, and more than one type of action. When you modify or add an action set, the settings change enterprise-wide for all filters using the action set. The types of action that determine where a packet is sent after it is inspected include the following:

- A **permit** action enables a packet to reach its intended destination.
- A **block** action discards a packet. A block action can also be configured to quarantine the host and/or perform a TCP reset.
- A **quarantine** action enables you to manage internal and external threats by quarantining network connections. This option provides the ability to automate sophisticated responses to security events.

  When an IP address (address group)/system is quarantined, select **Responder** > **Response History** to review the list and manage the status of these systems.

- A **rate limit** action enables you to define the maximum bandwidth available for the traffic stream. Incoming traffic exceeding this bandwidth is dropped.

  If two or more filters use the same Rate Limit action set, then all packets matching those filters share the bandwidth. For example, filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps pipe instead of each filter getting a dedicated 10Mbps pipe.

  Supported rates are subject to restrictions according to device model. Any of the predefined rates can be used as long as it does not exceed 25 percent of the total bandwidth of the product.

- A **trust** action enables the designated traffic to bypass all inspection; the traffic is transmitted immediately. Trust has lower latency than Permit, and using it can reduce load on the CPU and processors.

Action Name	Description
Recommended	The default action set, as determined by the filter's category settings. When you assign this action set to a filter, the filter uses the recommended action setting for the default category settings. The recommended action set can enable different configurations for filters within the same category. Under a recommended category setting, some filters are disabled while others are enabled; some might have permit actions assigned while others are set to block.
Block (+TCP Reset)	Blocks a packet from being transferred to the network. You can use the TCP Reset option for resetting blocked TCP flows.

Action Name	Description
Block + Notify (+ TCP Reset)	Blocks a packet from being transferred and notifies the SMS management console in the form of an event listing. Blocks a packet from being transferred. Notifies all selected contacts of the blocked packet. You can use the TCP Reset option for resetting blocked TCP flows. When you create an action set with Block + Notify + TCP Reset Destination, when a Reputation filter is hit, the TCP Reset to the Destination IP does not work properly. To resolve this problem, do not use the 'tcp reset' feature or only use 'tcp reset both' when the trigger reason is Reputation.
Block + Notify + Trace (+TCP Reset)	Blocks a packet from being transferred, notifies the SMS management console in the form of an event listing, and logs all information about the packet according to the packet trace settings. Blocks a packet from being transferred. Notifies all selected contacts of the blocked packet. Logs all information about the packet according to the packet trace settings. You can use the TCP Reset option for resetting blocked TCP flows.
Permit + Notify	Permits a packet and notifies the SMS management console in the form of an event listing and all selected contacts of the packet.
Permit + Notify + Trace	Permits a packet, notifies the SMS management console in the form of an event listing, and logs all information about the packet according to the packet trace settings.
Trust	Allows the traffic stream to continue without comparing it with any other filter rules.

Create or edit an action set

The SMS provides default action sets that can be customized for your security policy.

Procedure

1. Select **Profiles** > **Shared Settings** > **Action Sets**.

2. Click **New** to create a new action set, or **Edit** to change an existing one.
3. Under the Flow Control tab:
   a. Enter the name of the action set.
   b. Select the action from the **Flow Control** options.
   c. Select whether the option to reset a TCP connection is enabled. With **TCP Reset** enabled, the system resets the TCP connection for the source or destination IP when the Block action executes. You can configure this option on Block action sets.
4. Under the Notifications tab, configure notification contacts (either human or machine) that get sent messages in response to a traffic-related event. You can configure any of the following notification contacts to be notified when the action is triggered:
   - **Management Console** – Sends messages to the SMS, and generates an event when a filter hits. This default contact is available in all action sets. If you select this contact, messages are sent to the Alert or IPS Block Log, depending on whether a permit or block action has executed.
   - **Remote Syslog** – Send filter alerts, which must be configured for every device using that contact, to a syslog server on your network.
   - SMS Response – Associate a Responder policy when a filter hits. The Responder policy must have **Enable Policy** selected.
5. Under the Packet Trace tab, select whether to capture all or part of a suspicious packet for analysis. This should be set only for specific filters to avoid a performance issue with the device.
   - **Level** determines how much verbosity of a suspicious packet is logged for analysis. Full verbosity records the whole packet. Partial verbosity enables you to choose how many bytes of the packet (from 64 to 25,618 bytes) the packet trace log records.
   - **Priority** sets the relative importance of the information captured. Low priority items are discarded before medium priority items if there is a resource shortage.

6. Under the Quarantine Settings tab, assign a quarantine action set to a filter. You can select the following quarantine options for the action set:

   - Configure the **Hit Count** (1-10,000) and threshold **Period** in minutes (1-60). You can determine whether to Permit or Block traffic before the threshold period is reached. If you select Permit as the action, you can select **TCP Reset** to enable the device to reset TCP flows (Source IP, the Destination IP, or both), which ends the session.
   - Select **Web Requests** to manage all HTTP traffic from the quarantined addresses. You can configure the SMS to:
     - Block the requests entirely.
     - Redirect the client to another Web server that you specify.
     - Display the quarantined Web page according to options you select.

       Do not use `<frameset>` or `<form>` HTML tags for the message.
   - Select other traffic to configure the response (Block or Permit) to other non-HTTP traffic from hosts listed in the Response History queue. Select **Responder** > **Response History** to review the list.

7. Under the Quarantine Exceptions tab, you can select the following quarantine exceptions for the action set if you enabled the **Quarantine hosts that trigger this action** option in the preceding step:

   - Restrictions – A list of IP address groups that are not permitted. This option limits the quarantine action to specific IP addresses within the address groups.
   - Exceptions – A list of excluded IP address groups that will be permitted. When a filter hits, the specific IP addresses within the address groups are not quarantined.
   - Quarantined Access – A list of IP address groups that hosts can still access regardless of being quarantined. For example, when a host is detected as malicious and is quarantined, you might need to allow access to a specific website to remedy the situation.

   To create an unnamed IP address group:

- Click **New** to create a new unnamed IP address group, or **Edit** to change an existing one.
- (Optional) Enter the name of the IP address group.
- Enter the IP address in the **Source** field for a restriction or exception.
- Enter the IP address in the **Destination** field for the quarantined host.

To create a named IP address group:

- Click **New** to create a new named IP address group, or **Edit** to change an existing one.
- Click the **Right arrow** next to the **Source** field for a restriction or exception.
- Click the **Right arrow** next to the **Destination** field for the quarantined host.
- From here, you can search for, select, or create a new IP address group. For more information, see *Create or edit named resource groups on page 8-126*. After you create the action set, select **Admin** > **Named Resources** > **IP Address Groups** to view this IP address group.

8. Click **Finish**. To distribute the action set, distribute the profile.

Notification contacts

Configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the device. The traffic-related event can be the result of triggering a filter configured with an action set that specifies a notification contact. A notification contact can be any of the following:

- **Remote System Log** — Sends messages to a syslog server on your network. The syslog server uses the numbers you specify for the Alert Facility and the Block Facility to identify the message source.

After you configure this contact, verify that your device can reach the remote system log server on your network. If the remote system log server is on a different subnet than the management port, you might need to configure the routing. This is a default contact available in all action sets.

Note

To maintain backwards compatibility with the capabilities of existing remote syslog servers, the remote syslog sends clear text log messages using the UDP protocol with no additional security protections. Use remote syslog only on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

- **Management Console** — Sends messages to the SMS. This default contact is available in all action sets. If you select this contact, messages are sent to the Alert or IPS Block Log, depending on whether a permit or block action has executed. This notification contact does not require any configuration, although you can change the default name and aggregation period.
- **Email or SNMP** — Sends messages to the email address or specified SNMP. All email or SNMP contacts must be added from the Notification Contacts page.

  To use email contacts, you must complete the Mail Server panel of the Configuration window for each device. If the default email server is not configured on the device, you are prompted to configure it before adding a contact. After you configure this option, verify that the email server is reachable from the device, that mail relaying is enabled, and that you use an acceptable account/domain.

Note

SNMP notification contacts require SNMPv2, and do not work when SNMPv2 is disabled. Before creating an Email or notification contact, you must configure Email and SMTP server settings on the device from the **System** > **Email** page.

The SMS limits the number of email alerts sent in a minute. By default, the SMS sends 10 email alerts per minute. On the first email alert, a one minute timer starts, counting the number of email alerts to send according to the configured limit. Email alerts beyond the limit in a minute are blocked. After one minute, the system resumes sending email alerts. If any email alerts were blocked during that minute, the system logs a message to the system log.

After configuring notification contacts, you can select them for events when you create or edit the action set assigned to the filter. You cannot delete the default Remote System Log and Management Console contacts. You cannot delete a Notification Contact if it is currently configured in another action set.

Alert aggregation and the aggregation period

The SMS uses alert aggregation to prevent system performance problems resulting from an excessive number of notification requests. Because a single packet can trigger an alert, attacks with large numbers of packets could potentially flood the alert mechanism used to send out notifications.

Use alert aggregation to receive alert notifications at intervals to prevent this flooding. For example, if you set the aggregation interval to 5 minutes, the system sends an alert at the first filter trigger, collects subsequent alerts, and sends them out every five minutes.

The *aggregation period* that you configure when you create a notification contact controls alert aggregation. All notification contacts require this setting.

CAUTION!

Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems. Consistent aggregation alerts can be an indication of over configuration. Performance tuning may be needed.

In addition to the user-configured aggregation period, the system also provides alert aggregation services to protect the system from over-active filters that can lower performance.

For email contacts, the aggregation period works in conjunction with the email threshold setting configured for the email server.

Services

Configure additional ports associated with specific services and protocols using the Services page. The additional ports expand the range of traffic scanned by the device.

During the inspection process, the device first scans traffic against the standard ports for listed services, and then scans traffic against the list of additional ports you configure.

You can configure up to 16 additional ports for each service other than HTTP. For HTTP, you can configure only eight additional ports.

SSL

Configure your SSL server and client proxies before you create an SSL inspection policy. An SSL Server Proxy enables you to decrypt incoming SSL traffic for inspection. An SSL Client Proxy enables you to decrypt outgoing SSL traffic for inspection. SSL inspection relies on the private keys associated with the configured certificates, and decryption applies only to traffic directed to servers that match the SSL inspection configuration.

Note

SSL inspection cannot occur in asymmetric mode.

Refer to the *SSL User Guide* to learn more about configuring SSL inspection.

Default inspection profile

The SMS ships with a default inspection profile that can be used out-of-the-box to start protecting your network. This profile includes the default set of filters on the SMS.

Deployment modes

When you create a new profile, you can use the **Default** deployment mode or choose from a list of available deployment modes, and the device will use the recommended filter configuration for that deployment.

Depending on your network, it might be necessary to tune the selected deployment mode by overriding specific filters or categories. Digital Vaccines contain deployment settings for filters that address specific types of deployments.

Deployment mode	Description
Default	Provides a balance between high quality security and appliance performance and is suitable for most deployments.
Security-optimized	Favors additional security over network performance or application adherence to protocol standards and is a subset of the Hyper-Aggressive deployment mode. Enables more Zero Day Initiative (ZDI) protection than other deployment modes.
Performance-optimized	Emphasizes network performance over security and is not recommended for use in a production environment. This deployment mode is intended for testing purposes only.
Core [Deprecated] (1)	Offers improved performance for devices that are deployed on the interior of a network, with the expectation that perimeter-facing devices block most malicious Internet traffic.
Edge [Deprecated] (1)	Ideal for Web farms and DMZs that typically expose services to the Internet.

(1) Deprecated deployment modes include new filters added to the Digital Vaccine, but the new filters in the deprecated deployment modes have the same characteristics as the Default deployment mode.

Deployment mode	Description
Perimeter [Deprecated] (1)	Offers optimal security for devices deployed on the perimeter of a network and protects the network from Internet traffic.

Capture additional event information

The device can collect a client's true IP address before a forwarding proxy IP address overwrites it. X-Forwarded-For and TrueClient-IP technologies identify a request's source IP address without having to refer to proxy logs or Web server logs. When possible, the device will detect this and provide the original Client IP address in the Inspection Events.

You can also configure the device to display HTTP context information, including the requester's URI, method, and hostname. When possible, the devices will detect this and provide the HTTP hostname, URI, and method in the Inspection event.

Inheritance

When you create a new profile, you can target a specific deployment or leverage an existing profile using inheritance. Profiles with inherited settings **cannot** be edited if the main profile is locked. For each profile in the hierarchy, the following items can be inherited from the profile in the next level up:

- Security filter exceptions and restrictions
- Application filter restrictions
- Reputation exceptions
- Category settings
- Digital Vaccine, Threat DV, and Digital Vaccine Toolkit package filters
- Advanced DDoS filters
- Reputation filters
- Traffic Management filters

Create a new profile

The SMS builds the profile based on the currently activated Digital Vaccine settings.

Procedure

1. Select **Profiles** > **Inspection Profiles** > **New**.
2. Enter a name for the profile.
3. Select a deployment mode.
4. Select whether to capture additional event information:
   - Select **Client IP (X-Forwarded-For & True-Client-IP)** if you want the profile to identify whether packets associated with an inspection event were forwarded for another IP address.
   - Select the **HTTP Context (Hostname, URI, Method)** check box if you want the profile to identify information associated with any HTTP URI. Select this to view Suspicious Objects on the Threat Insights.
5. Select whether to choose an existing profile for inherited settings. If a filter has inherited settings and the base filter is locked, the filter with inherited settings cannot be edited.
6. (Optional) Enter a description for the profile.
7. Click **OK**.

Profile Tasks

Copy a profile

Save an existing profile using a different name. When you create a copy of a profile, you create a complete duplicate of the original profile.

Procedure

1. Select **Profiles** > **Inspection Profiles**.
2. Select a profile from the Inventory pane, and then click **Save As**.
3. Complete the rest of the profile information as you would when you create a new profile.

Compare profiles

You can select up to three profiles to compare the differences between profiles such as category settings and filters.

Note

The compare process skips over any SSL client objects.

Procedure

1. Select **Profiles** > **Inspection Profiles**.
2. Select up to three profiles to compare.

   The Profile Compare screen displays tabs for the following areas of comparison: category settings, filters, traffic management filters, advanced DDoS filters, reputation filters, SSL inspection policy, and profile settings.
3. Select the **Filter** tab, and then select the **Show Differences Only** check box to only view the differences in the selected profiles. A yellow triangle in the **Diff** column indicates that one or more entries in that row are different.
4. To make changes to the profiles, click **Edit** in each tabbed area.

Export profiles

You can export an existing profile to a local file, the SMS http server, or an external SMB or NFS server.

Procedure

1. Select **Profiles** > **Inspection Profiles**.
2. Select a profile, and click **Export**.
   - If you export to local SMS exports and archives, the exported file can be viewed and accessed from the Exports and Archive section of the SMS Web interface. See *Exports and archives on page 8-128*.
   - If you export to an external source and select NFS Server, the SMS must have write-permission for the anonymous user on the directory exported by the specified NFS server.
   - If you are exporting the profile to one or more SMS servers, you have the option to create a new profile or merge the profile with the existing profile.

Note

The merge process skips over any SSL client objects.

Delete profiles

When you delete a profile, you delete all data relating to that profile including profile snapshots. However, events that have been generated by the profile will remain accessible.

1. Select **Profiles** > **Inspection Profiles**.
2. Select one or more profiles, and click **Delete**.

Import profiles

Import a new profile or replace an existing profile with the option to add new settings or change existing settings. You can import an existing profile from a local file, from a device segment, or from another SMS.

Profile import filter behaviors

When you import a profile, you can choose to create a new profile, replace an existing profile, or combine the imported profile with an existing profile.

When you combine profiles, the following behaviors occur, depending on the filter type.

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

Named IP address groups

When you import a profile that contains a named IP address group (for a filter exception, a quarantine exception, an Advanced DDoS filter, an SSL inspection policy, or a Traffic Management filter), the SMS verifies whether the named IP address group already exists.

- The SMS assigns one IP address group for each imported IP address group.
- If the named IP address group exists and the values are an exact match, then the SMS keeps that existing named IP address group for the profile.
- If the named IP address group exists but the values are not an exact match, then the SMS adds each named IP address group, and each named IP address group is identified with an underscore and a number (for example `NamedIPAddress_1`, `NamedIPAddress_2`, `NamedIPAddress_3`, and so on).
- If the named IP address group does not exist on the SMS, the SMS adds it as an unnamed resource. See *Named resources on page 8-123*.

Import a profile

Procedure

1. Select **Profiles** > **Inspection Profiles**.
2. Click **Import**.
3. Follow the steps on the Profile Import wizard.

View profile details and versions

You can view profile details and edit the Deployment Mode. For every inspection profile you create, the SMS tracks information about the profile when you distribute the profile to a device.

Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Details** or **Versions** to access this information. Alternatively, you can double-click a profile in the navigation pane to access the individual tabs.

Details

The **Details** tab provides the most current profile information including details about the profile, the profile distribution schedule, and the profile distribution details.

Profile details

Important profile details to note:

- **Inheritance** - Profile name or series of profile names that indicate the hierarchy for the inherited settings.
- **Deployment Mode** - Deployment settings for DV filters that address specific types of deployments.
- **Capture Additional Event Information** - Configuration for identifying a request's source IP address before it is overwritten by a forwarding proxy IP address, and for identifying the true source of an HTTP request.

Profile distribution schedule

From here, you can create a **New Schedule** for the profile.

Profile distribution details

The profile distribution details area displays information on the distribution of the selected profile to your devices. Profile distribution details include the following:

- **Distribution Target** - Segment or segment group that received the profile distribution.
- **Distributed** - Date and time of the last profile distribution.
- **Version** - Version of the profile that was distributed.
- **Changed** - **Yes** indicates there is a changed version of the profile that has not been distributed.

Versions

For every inspection profile you create, the **Versions** tab provides information about all versions of the selected profile, including whether the profile is active, its version number, when it was last distributed to your devices, and any comments.

As you modify or make changes to a profile, the version for that profile displays as a point release. For example, three changes to a profile moves the version from 1.0 to 1.3. When you distribute or create a snapshot of this profile, the version is committed and is displayed on the screen as 1.3. Subsequent changes to that profile move the version number up a major level to 2.0. Any changes made prior to the next distribution of the profile are indicated as a minor or point release number. Changes made after the distribution of a profile begin with a major number allowing you to keep track of distributed profile versions.

Edit profile details

To edit the profile details, select the **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Details** tab, and then click **Edit Details**.

Create a snapshot of a profile version

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Details**.
2. Click **Snapshot**. A snapshot of the current version of the profile is created.

Note

If you delete a profile, you will lose all snapshots associated with the profile. Profile snapshots are saved as part of the profile data and will be deleted along with the other data.

When you click on the **Versions** tab, the new entry displays in the All Versions table.

Activate a profile version

To activate a profile, select the **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Versions** tab, select a profile version, and then click **Activate**. The selected profile activates as the current profile and replaces all filter changes with changes from the snapshot.

Named IP address groups

When you activate a profile that contains a named IP address group (for a filter exception, a quarantine exception, an Advanced DDoS filter, an SSL inspection policy, or a Traffic Management filter), the SMS verifies whether the named IP address group already exists. This ensures that the enforcement of policies, including exceptions, are restored when you activate a previous profile snapshot.

- The SMS assigns one IP address group for each imported IP address group.
- If the named IP address group exists and the values are an exact match (IP address group contains the same IP addresses), then the SMS keeps that existing named IP address group for the profile.

- If the named IP address group exists but the values are not an exact match, then the SMS adds each named IP address group, and each named IP address group is identified with an underscore and a number (for example `NamedIPAddress_1`, `NamedIPAddress_2`, `NamedIPAddress_3`, and so on).
- If the named IP address group does not exist on the SMS, the SMS adds it as an unnamed resource. See *Named resources on page 8-123*.

SSL Inspection policies

You can add an SSL Server Inspection policy to specify inbound SSL traffic that you want to protect for particular segments on a managed device, and an SSL Client Inspection policy to specify outbound SSL traffic that you want to protect for particular segments on a managed device.

SSL Inspection profiles include a set of SSL policies, each of which uses an SSL proxy containing the information needed to determine what servers need to be decrypted. Assign the SSL inspection policy to the inspection profile that carries the traffic of interest.

You must first define an SSL server proxy before you configure an SSL server policy.

You must first define an SSL client proxy before you configure an SSL client policy.

Note

SSL inspection cannot occur in asymmetric mode.

Refer to the *SSL User Guide* to learn more about configuring SSL inspection.

Working with filters

Profiles provide a management facility for packaging and distributing filters to your devices. Filters provide information and instructions for the devices protecting your network against malicious attacks. These filters enable your devices to monitor and respond to network traffic according to a particular pillar, or type. These pillars separate filters into types that apply to different

attacks and sections of your network. You can create, modify, and manage these filters to block and protect against malicious attacks and piracy of your bandwidth and network services. Each filter consists of customizable options and settings that detail how the system should monitor, investigate, process, and block traffic.

If the SMS identifies traffic that matches a filter, it responds to that traffic based on the instructions defined in the action set for the filter. All action sets require a flow control action—the SMS can block, permit, or react in a combination of ways to the traffic. As an added measure of safety and information dissemination, you can configure alerts to inform interested parties about detection and responses to malicious attacks and usage by notifying the SMS or by sending emails to specified email addresses. You can also log information about matching traffic to a packet trace log or a remote syslog server for review and reporting.

All filters are assigned to protect a segment on your system. When you change the settings of these filters, only the target distribution segments receives the changes. You can also create Segment Groups. *Learn more on page 3-114*.

Note

When a device is added on the SMS, any unused virtual ports (those that are not in a virtual segment in a profile) are deleted on the SMS. To keep any unused virtual ports, put them into a virtual segment as SMS valid combinations before adding your device. *Learn more on page 3-110*.

Filter components

Filters have the following components, which determine the filter type, global and customized settings, and how the system responds when the TSE finds traffic matching the filter:

- **Category** — Defines the type of network protection that the filter provides. This category also enables you to locate the filter and control the global filter settings using the Category Setting configuration.

- **Action set** — Defines what occurs when the system detects traffic that matches the filter.
- **Adaptive Filter Configuration State** — Enables you to override the global Adaptive Filter configuration settings so that adaptive filtering does not affect the filter.
- **State** — Indicates if the filter is enabled or disabled.

Category settings

Use category settings to configure global settings for all filters within a specified category group. Digital Vaccine filters are organized into groups based on the type of protection provided:

- Application Protection filters — Defend against exploits targeting applications and operating systems. These filters include a variety of security filters and application filters.
- Infrastructure Protection filters — Protect network bandwidth and network infrastructure elements.
- Performance Protection filters — Allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of high congestion. Types of filters in this group include Peer-to-Peer, Instant Messaging, and Streaming Media.

Use category settings to assign global configuration settings to filters in a subcategory. For example, if you decide not to use any filters to monitor P2P traffic, you can change the category settings for the Performance Protection P2P filter group to disable these filters. Category settings consist of the following global parameters:

- **State** — Determines whether filters within the subcategory are enabled or disabled. If you disable a category, you disable all filters in the category.
- **Action set** — Determines what occurs when traffic matches a filter. If you configure the `Recommended` action set, filters within the category are configured with the settings that the Digital Vaccine team recommends.

If required, you can override the category setting on individual filters by editing the filter to define custom settings.

Adaptive filtering

Adaptive filtering (AFC) avoids device congestion by automatically disabling filters that trigger excessively. You can configure AFC on individual filters or on all filters (at the device level). Learn more: *Configure a device for adaptive filtering on page 3-68*.

Edit the filter and clear the **Use Adaptive Configuration Settings** checkbox if you choose not to submit filters to adaptive filtering.

You can view which disabled filters have been most recently affected by AFC in the **Adaptive Filter List**. Learn more: *View AFC filters on page 3-17*.

Security filter exceptions and restrictions

Security filter settings do the following:

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

The SMS enforces the maximum number of filter exceptions for a device based on device capacity. The SMS groups devices into three categories (low-end, medium-end, and high-end) with an assigned maximum to each category for enforcement purposes. Filter exception limits include:

- Medium-end devices (NX-Platform, 440T, 1100TX, and vTPS devices) limit: 8,000 filters.
- High-end devices (2200T, 5500TX, 8200TX, 8400TX, and 9200TXE devices) limit: 12,000 filters.

Create or edit a security filter restriction or exception

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Security Filters**.
2. Click the **Restrictions** or **Exceptions** tab, and then click either **Add** or **Edit**.
3. Enter the appropriate information in the **Create/Edit Address Pair** dialog.

   Keep the following information in mind:

   - Select **Any IP** to apply the restriction to all traffic sources/destinations.
   - Select **IP Address**, and provide or select an IP address to apply the restriction to that specific source/destination.
4. Click **OK**.

Create or edit application filter restrictions

You can create restrictions for all application filters to function for the listed IP addresses. When you add or modify an application filter restriction, the settings apply global changes to the following filter categories:

- *Instant Messaging on page 5-35*
- *Streaming Media on page 5-35*
- *Peer-to-Peer on page 5-35*

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Application Filters**.
2. Click the **Restrictions** tab, and then click either **Add** or **Edit**.
3. Enter the appropriate information in the **Create/Edit Address Pair** dialog.

Keep the following information in mind:

- Select **Any IP** to apply the restriction to all traffic sources/ destinations.
- Select **IP Address**, and provide or select an IP address to apply the restriction to that specific source/destination.

4. Click **OK**.

Search

The SMS provides several methods to search profiles for filters:

Type	Description	Access
Global Search	Searches all listed profiles for filters that match search criteria.	**Profiles** > **Inspection Profiles** > **Global Search**
Search	Searches within a selected profile for filters that match search criteria. You can search by extended criteria, across all filter categories within a listed profile. **Note** This function is not supported for client SSL inspection profiles.	**Profiles** > **Inspection Profiles** > **[profile name]** > **Search**
Find	Searches on the displayed page and highlights the next filter that contains the keywords. This option only searches on the displayed page.	**Find** button located at the bottom of the Search Results

Find a filter in search results

Procedure

1. Do one of the following:

- To find a filter across all listed profiles, select **Profiles** > **Inspection Profiles** > **Global Search** > **Find**.
- To find a filter within a selected profile, select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Search** > **Find**.

2. Enter the name of the filter or keyword, and click **Find**.

   The next entry that matches the criteria is highlighted in the filter list.

Search profile filters

Search enables you to search by extended criteria, across all filter categories, and includes options for user settings, severity, protocol, platform, modified or added filters, and vulnerability criteria.

Procedure

1. Select **Global Search** to search across all listed profiles or select **Search** within a profile to search that particular profile.
2. Select **Filter Criteria** to search for:

SELECT THIS CRITERIA:	TO SEARCH FOR ...
Filter Type	• *Security filters on page 5-30* • *Application filters on page 5-30*
Suspicious URL Metadata	• **Include** - Filters that include suspicious URL metadata. • **Exclude** - Filters that do not include suspicious URL metadata. **Note** The correct Digital Vaccine is required to enable the Suspicious URL Metadata field. Activate the Digital Vaccine after you upgrade the SMS.

SELECT THIS CRITERIA:	TO SEARCH FOR ...
User Defined Filters	• *Advanced DDoS filters on page 5-49* • *Reputation filters on page 5-40* • *Traffic Management filters on page 5-47* • SSL inspection policies (SSL server inspection policies only) • SSL servers
Control	• **Category** - All filters distributed by the TMC are initially tagged *Category*. • **Filter** - If a filter has been edited to use specific settings, select this check box.
State	**Type Specific** - Depending on device model, the same filter may have different states (for example, a filter may be enabled on a device but disabled on a different device).
Filter Category	Specific *filter categories on page 5-30*.

3. Select **Source Criteria** to search for:

SELECT THIS CRITERIA:	TO SEARCH FOR ...
Filter Released and **Filter Last Modified**	When filters where released and when filters where last modified. **Note** After upgrading, activate a new Digital Vaccine before you can search for filters by released dates.
Filter Source	• Digital Vaccine • ThreatDV (Auxiliary DV), and select **Malware** • DV Toolkit, and select **Any** or a specific version

4. Select **Additional Criteria** to search for.
5. Select **Filter Taxonomy Criteria** to search for.

6. Click **Vulnerability Criteria** to search for:

SELECT THIS CRITERIA:	TO SEARCH FOR...
CVE ID	Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE)
Bugtraq ID	Unique tracking number used to identify a Bugtraq ID
Vulnerability Scan Database	Vulnerability scans that have been imported for use on the SMS. *Learn more on page 5-111*. • **Asset Addr(s)** - One or more IP addresses for an asset. An asset is the network IP address of the host vulnerable to the CVE identified in the vulnerability scan. • **Flagged** - All CVEs that are flagged for follow-up. • **Not Flagged** - All CVEs that are not flagged.

7. Click **Search**.

View filter search results

The Search Results display information for each filter, like the State, Name, Action Set, and other filter descriptions.

More information on the Search Results.

COLUMN	DESCRIPTION
Control	All filters distributed by the TMC are initially tagged *Category*. If you edit the filter to use specific settings, *Filter* displays.
Source	Source of the filter and can be one of the following: • *Digital Vaccine on page 5-53* • *ThreatDV on page 5-54* • *DV Toolkit on page 5-64*
AFC	Individual filters contain *Adaptive Configuration Settings on page 5-24* that can be enabled or disabled. *Learn more on page 5-24*.

Column	Description
Filter Disclosed	Date the filter was publicly disclosed, if available. **Note** You must activate a new Digital Vaccine before you view the filter disclosed date.

Filter categories

Filters are a part of Inspection profiles and can be customized for your network security needs. Filters are policies with settings and rules for managing and blocking traffic on a network.

Each filter includes an action set that contains instructions for managing data and a category setting. As security threats are recognized, filter updates are released to protect potentially vulnerable systems.

Specific devices may not support certain types of filters.

Security filters

Security filters defend against exploits that target applications and operating systems of workstations and servers on a network. Malicious attacks may probe your network for vulnerabilities, available ports and hosts, and network accessible applications. Security filters defend your network by providing a device with threat assessment, detection, and management instructions.

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

To view the security filter categories on the SMS, select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Security Filters**.

Application filters

Application filters allow key applications to have prioritized access to bandwidth. These filters ensure mission critical applications have adequate

performance during times of high congestion. Application filters allow you to manage the policy around non-productive or potentially illegal applications. Initially, this includes Peer-to-Peer management, where the user may apply block or shape actions across the category or on an individual basis.

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

To view the application filter categories on the SMS, select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Application Filters**.

Exploits

Exploits are attacks against a network using weaknesses in software such as operating systems and applications. These attacks usually take the form of intrusion attempts and attempts to destroy or capture data. These filters seek to protect software from malicious attacks across a network by detecting and blocking the request.

The two most common methods for exploiting software include email and Web browsing. All Web browsers and many email clients have powerful capabilities that access applications and operating systems. Attackers can create attachments that scan for and exploit this software.

Identity theft

Identity theft involves various methods of obtaining key pieces of data related to personal or financial information and using that information to gain goods and services.

Reconnaissance filters

Reconnaissance filters protect your system against malicious traffic that scans your network for vulnerabilities. These filters constantly monitor incoming traffic, looking for any sign of network reconnaissance. These attacks probe your system, seeking any weakness that can be exploited by attacks. In effect, the attacks attempt to perform reconnaissance of your network to report its strengths and weaknesses for further attacks.

By default, Reconnaissance filters are either disabled or set to Block/Notify.

Scan and sweep filters

Scan and sweep filters constantly analyze traffic across several sessions and packets against potential scan and sweep attacks against a network. As a result, the Block action setting functions differently for these filters. If the Block action is configured with TCP Reset functions, the TCP Reset does not occur as the network traffic is not tied to a single network flow.

In addition, a Block action will cause the source address to be blocked in future network flows.

Scan and sweep filters are not affected by restrictions and exceptions in the shared settings for Application Protection filters. When you create exceptions and apply-only settings in the shared settings, they only affect Vulnerability Probing filters.

Attackers may try to scan a network for available ports or try to infiltrate a host system through its ports and software. These attacks provide entry points for introducing malicious code to further enact attacks through your host and ports. Scan and sweep attacks can consist of multiple probe attacks in large amounts, sending numerous requests for access and information at once. Scans and sweeps filters protect against scan attacks and possible exceeded threshold limits against your ports and hosts.

Security policy filters

Security policy filters act as attack and policy filters. As attack filters, these filters compare packet contents with recognizable header or data content in the attack along with the protocol, service, and the operating system or software the attack affects. These attack filters require deployment knowledge and/or operational policy.

These filters detect traffic that may or may not be malicious that may meet one of the following criteria:

- Different in its format or content from standard business practice.
- Aimed at specific software or operating systems.

- Contrary to your company security policies.

By default, Security Policy filters are disabled. Configuring security policy filters requires knowledge of the installation network configuration. When enabled, these filters may generate false attack alerts depending on your network or application environment. For example, false alerts could be caused by the following:

- Custom or legacy software that uses standard protocols in non-standard ways.
- Attacks on applications or operating systems that you do not have installed.
- Activities that could be benign or malicious depending on where they originate.

Note

Scan your network hosts before disabling or creating exceptions to specific attack protection filters. Some operating systems install default services which may be vulnerable to attack. If you disable or add an exception to a filter that protects a service that you do not know about, you may increase your network vulnerability.

Spyware

Spyware is a type of software that transmits information without the user's knowledge or permission. Spyware may be the result of a virus infection or may be installed along with other applications. Spyware often consumes vast resources and can slow systems and, in some cases, cause systems to become unstable or unusable.

Virus

A virus is an application or piece of malicious code that can infect other programs. Viruses can embed a copy of itself in programs making them Trojan Horses. When you run these infected programs, the embedded virus also runs and propagates the infection.

If you use ThreatDV, it is not recommended that you enable this category to Block as a group due to the quantity of filters enabled.

Vulnerabilities

Attackers generally look for vulnerabilities in a network. They try to find the weak points in a network security system to bypass filters and reach data and services. These attackers seek to use intrusion methods against areas such as software back-doors and poorly protected hosts and ports. Vulnerability scanning checks for all potential methods that an attacker could use to infiltrate a network and system.

Vulnerability filters protect these possible points of entry in a network, detecting and blocking attempted intrusions. The filters constantly scan for possible intrusion points, giving a warning when a vulnerability is found or when malicious attacks occur.

Network equipment

Network attacks can broadly or specifically seek access to corrupt data on a network. Networked hardware receives requests from operating systems and services on a network.

These filters detect and block the malicious attacks that target equipment accessible through a network, such as printers, modems, routers and integrated phone systems.

Traffic normalization

Traffic Normalization filters block network traffic when the traffic is considered improper or malformed.

These filters allow you to set alerts to trigger when the system recognizes this traffic. Traffic pattern anomaly filters alert when network traffic varies from normal. Traffic normalization filters enforce valid packet processing within the Threat Suppression Engine. They protect the engine by detecting invalid or abnormal packets.

Because they inspect traffic for malformed packets, Traffic Normalization filters are set to Block by default. We do not recommend using a Permit

action because it could introduce vulnerabilities with malformed packets. If you select the Block action set, the SMS does not log the traffic that matches this filter. Use caution when selecting this action as it might cause a network outage, if not correctly defined.

As these filters manage traffic, you may notice that not all filters result in blocked streams. The following filters do not hold blocked data streams:

- 7102: IP fragment invalid. The packet is dropped.
- 7103: IP fragment out of range. The packet is dropped.
- 7104: IP duplicate fragment. The packet is dropped.
- 7105: IP length invalid. The packet is dropped.
- 7121: TCP header length invalid. The packet is dropped.

Traffic Normalization filter names must be unique within a profile. The SMS gives each filter a unique ID, which it uses as a reference in the system.

Instant messaging

Performance Protection filters allow you to shield traffic associated with instant messaging.

Peer-to-Peer (P2P)

Peer-to-peer protocols essentially turn a personal computer into a file server, which makes its resources as well as those of its host network available to the peer-to-peer community.

Performance Protection filters allow you to shield traffic associated with these kinds of file-sharing protocols. All peer-to-peer filters are user-activated and must be enabled to block peer-to-peer traffic.

Streaming media

Streaming media protocols include:

- **Unicast** — Sends a separate copy of the media stream from the client to each client.

- **Multicast** — Sends a single copy of the media stream over any given network connection and must be implemented in network routers and servers.

Reputation feed

The reputation feed enables you to monitor and block inbound and outbound communications with known malicious and undesirable hosts. It is a robust security intelligence feed powered by advanced analytics and a global reputation database of IPv4 and IPv6 addresses, DNS names, and URLs. You can then define your security policy based on the categories and reputation scores from the reputation feed. The reputation feed is updated multiple times a day to stay ahead of emerging threats.

Reputation scores

Each reputation entry has an associated reputation score that represents potential risk level. Reputation scores range from 1 to 100, with a score of 100 representing a definite threat. Reputation scores are categorized into the following five ranges:

- **80-100**: These entries are blocked by default when you use ThreatDV and have created a reputation filter for your profile.
- **60-79**: These entries are known to be somewhat malicious, but may not have enough corroborating information.
- **40-59**: These entries are likely to be malicious, but not enough information is available to assign them a score of 60.
- **23-39**: These entries are mostly non-malicious in nature, but may have generated undesirable traffic.
- **0-19**: These entries generally do not represent any threat, but may have generated slightly suspicious traffic.

You can use reputation scores to assess and reassign risk for reputation filters that are active on a device. If suspicious activity continues, you can assign a higher score to the reputation entry. To avoid inadvertently interrupting business-critical communications, make sure that you set critical hosts, such as your external partners, to be permitted.

Geographic filters

Geographic filters detect and manage traffic based on a computer's IP address/hostname within a geographic region or country. These filters enable you to perform actions based on the countries that you allow or deny in a filter. An IP address can be tied to real-world geographic regions or countries, and identifying a client's geographic location may provide clues about the user's intentions. The SMS supports real-time geolocation analysis through the integration of the free MaxMind GeoLite City binary database.

Note

If you have a paid MaxMind subscription, you can import the database file. *Learn more on page 8-137*.

A Geographic filter is similar to a Reputation filter in that it associates an action set, and when the profile containing the Geographic filter is distributed to a device, the specified actions are applied to traffic that matches the included and excluded countries.

Creating a Geographic filter consists of two steps. In the first step, you define the general settings: the name for the filter, the state, the locked status, and the action set that specifies whether to allow or deny traffic based on the geographic region. In the second step, you search for, select, and evaluate the country criteria as an *inclusion* or *exclusion*. Once you distribute the filter, you will can view events and generate reports based on this filter.

Note

A country can only be assigned to one Geographic filter at a time. For example, if you create a filter and allow Japan, you cannot search for and select Japan in a different Geographic filter until you remove it from the first filter.

Important

Services that attempt to hide their geographic origin through proxies, VPNs, or other obfuscating services cannot be geographically identified by MaxMind. Other services might have IP addresses that belong to an AnyCast network, which masks where their endpoints reside. The SMS might display these locations as `unknown`. In order to maintain your restrictive geographic policies, you can respond with one of the following strategies:

- Add a new **Permit+Notify** rule to the policy for any traffic that matches `country=unknown`.
- Create reputation exceptions as needed. *Learn more on page 5-24*.

Learn more about geolocation accuracy.

Any country

Every time you create a new Geographic filter, the SMS automatically includes **Any** country, which allows you to quickly include all countries in the database without having to search for and select one or more countries. Once you select a country, the SMS removes **Any** country from the Geographic filter; however, if you exclude all countries in the selected filter, the SMS includes **Any** country again.

Inclusions and exclusions

You can include one or more countries in a Geographic filter. In this way, you can track visits from a region that is spread across multiple countries. For example, the sales region known as APLA (Asia Pacific and Latin America) includes the following countries: Argentina, Australia, Brazil, China, Hong Kong, India, Indonesia, Japan, Mexico, New Zealand, Korea, and Taiwan. To track this region, you can create a filter, include all of the countries, and then select an action set. The SMS displays a green check mark icon for each country that is included in a Geographic filter.

In addition, if you want to exclude one or more countries in a Geographic filter, you can search for, select, and exclude a country. The SMS displays a red strikethrough icon for each country that is excluded in a Geographic filter.

You can also edit an existing Geographic filter to exclude a previously included country and vice versa.

Important

An **inclusion** or an **exclusion** does not necessarily indicate that traffic for the selected country is allowed or denied. The action set for the filter determines the action assigned to the country.

Create or edit a Geographic filter

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/ Geo**.
2. Click **New Geographic** or select an existing geographic filter, and click **Edit**.
3. Select the appropriate parameters in the Create Geographic Filter dialog.

   Keep the following information in mind:

   - Use the **Search** field in the Choose Countries dialog to narrow down the list of available countries.

     Note

     You cannot enter an abbreviation or alternative name for a country. For example, you cannot enter “US” or “America” for “United States.”

   - Select **Inclusions** to include (allow) the selected countries in the filter. Select **Exclusions** to exclude (deny) the selected countries in the filter.

Note

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

- An **inclusion** or an **exclusion** does not necessarily indicate that traffic for the selected country is allowed or denied. The action set for the filter determines the action assigned to the country.
- Creating a Geographic filter for a country—that has a large range of IP addresses and a significant amount of traffic—and selecting the Notify action set can affect the device adversely by the large number of events generated.

Reputation filters

A Reputation filter associates an action set with one or more suspect IP addresses, domains, or URLs in the Reputation Database.

When the profile containing the Reputation filter is distributed to a device, the specified actions are applied to traffic that matches the addresses of tagged entries in the Reputation Database that have been screened using specified tag criteria.

When you create a Reputation filter using addresses from the Reputation Database, any tag category associated with the address is included. *Learn more on page 5-75*.

Important

You can create an exception to prevent internal IP address from being used in a Reputation filter.

Creating a Reputation filter consists of two steps. In the first step, you define the general settings: the name for the filter, the state, the locked status, the action set, and the type of Reputation Database entries. In the second step,

you specify the tag criteria to use when matching entries in the Reputation Database.

Note

If the tag criteria contains **Does not have this tag**, when you distribute the profile, the SMS sends all entries that do not have this tag category to the device including Reputation DV, geographic, and user-provided entries.

Reputation filters table

The Reputation filters table displays the available Reputation and Geographic filters. The filters are in precedence order so as to resolve overlapping criteria.

To access the table, select **Profiles > Inspection Profiles > [Profile Name] > Reputation/Geo** and select the Filters and Settings tab.

Column	Definition
Order	Displays the order number and precedence in which the filter is applied in the Reputation engine. By default, the Reputation and Geographic filters display in the order in which they were created. The Reputation engine matches the first filter, applies the selected action, and does not apply additional filters listed in the Reputation Filters table.
State	Displays whether a filter is active. A check mark indicates that the filter is active and can be distributed to a device.
Locked	Determines whether a filter can be edited.
Action	Determines what occurs when traffic matches a filter. Learn more: *Learn more on page 5-3* about actions.
IPv4	Indicates whether the entry type has an IPv4 address.
IPv6	Indicates whether the entry type has an IPv6 address.

Column	Definition
DNS	Indicates whether the filter has a Domain Name System. If the option to apply filter action to HTTP requests with matching DNS hostnames is disabled, DNS requests can only be seen and enforced if the device is between the client and the DNS server.
URL	Indicates whether the filter includes a URL. Select the Filters and Settings tab, and ensure that the **Using Client Hello SNI extension** option is set to **Yes** (default) under Apply Filter Action. This enables you to check whether a URL's server is listed in the Reputation database without having to rely on TLS decryption. To block all URL's from that server, type a single wildcard string (`\*`) after the domain name. For example, `http://badwebsite.com/\*`
Untagged/Tagged	Untagged: A checkmark indicates that the Reputation filter will match all entries in the Reputation Database that do not have tags. Tagged: A checkmark indicates that the Reputation filter will match all entries in the Reputation Database that have tags and will filter the entries by the criteria defined for the filter.
Criteria	Criteria used for the selected filter based on tagged Reputation Database entries. A Geographic filter will display the evaluation (inclusion or exclusion), country icon (if available), and the official name of the selected country, sorted in alphabetical order. If a Geographic filter has an exclusion, **Any** displays to indicate that every other country in the database is included.

Edit Reputation settings

Reputation settings apply to all Reputation filters in a profile.

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/Geo**.
2. Click **Edit Settings**.
3. Enter the appropriate information in the **Edit Reputation Settings** dialog.

Keep the following information in mind:

- The Filter Matching Address setting specifies which address of an incoming packet is used when testing for a filter match.
- The Lookup Packet Handling setting specifies what the device should do with packets that arrive during a Reputation lookup.

4. Click **OK**.

Create or edit a Reputation filter

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/ Geo**.
2. Click **New Reputation** or select an existing Reputation filter, and click **Edit**.
3. Select the selection criteria. Keep the following information in mind:
   - **Entry Criteria** determines the type of address entries from the Reputation Database to include in the filter.

     Note

     You must select the **URLs** checkbox to view Suspicious Objects.

     Learn more: *Suspicious Objects on page 13-7*
   - If a selected tag criteria contains **Does not have this tag**, the SMS sends all entries that do not have this tag category to the device including Reputation DV, geographic, and user-provided entries when you distribute the profile.
4. Click **OK**.

Change the precedence of a Reputation or Geographic filter (move up/down)

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/Geo**.
2. Select a Reputation or Geographic filter from the table, and then click **Move Up** or **Move Down** .

Important

By default, the Reputation and Geographic filters display in the order in which they were created, and the Reputation engine matches the first filter and applies the selected action.

Note

Creating a Geographic filter for a country—that has a large range of IP addresses and a significant amount of traffic—and selecting the Notify action set can affect the device adversely by the large number of events generated.

The new order is automatically saved.

Delete a Reputation or Geographic filter

Important

Deleting a Reputation or Geographic filter will also remove all data relating to that filter; however, any events that were generated for the filter will still be visible. In circumstances in which you no longer need to deny a country but it is linked to events and reports, it may be better to disable the state of the filter rather than delete it.

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/ Geo**.
2. Select a Reputation or Geographic filter from the table, and then click **Delete**.

Create or edit Reputation filter exceptions

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Reputation/ Geo**.
2. Click the tab for the reputation filter exceptions (IP, DNS, or URL) that you want to configure.

Note

IP and DNS blocking rules supersede URL blocking rules. So, for example, if you already set up a DNS rule to block `www.mywebsite.com`, a URL exception rule for `www.mywebsite.com/exception` would not be enforced because the DNS request occurs before the HTTP request. Even if the URL rule belongs to a higher-prioritized filter than the DNS rule, you would have to disable the DNS rule first for this URL exception to succeed. A flow that is *permitted* by an IP rule, however, can still be blocked by a DNS rule or URL rule. Likewise, a flow that is permitted by both an IP rule and a DNS rule can still be blocked by a URL rule.

3. Click **Add** or select an existing exception name, and then click **Edit**.
4. Configure the exception.
   - For IP exceptions:
     - Select **Any IP** to apply the restriction to all traffic sources.
     - Select **IP Address**, and provide or select an IP address to apply the restriction to that specific source.

- For DNS exceptions:
  - Type the name of the domain that you want to exclude from the filter. The domain name must be explicit. Do not use wildcards.
- For URL exceptions:
  - Type the URL that you want to exclude from the filter.

Note

A single wildcard string `\*` can be used only at the beginning and end of user-defined URL entries and exceptions. For example, each of the following wildcard entries successfully matches URL `http://a.com/path/to/resource`:

- **Domain wildcard usage:** `\*/path/to/resource`
- **Path wildcard usage:** `http://a.com/\*`
- **Path wildcard usage:** `http://a.com/path/\*`
- **Path wildcard usage:** `http://a.com/path/to/\*`
- **Both domain and path wildcard usage:** `\*/path/\*`
- **Both domain and path wildcard usage:** `\*/path/to/\*`

5. Click **OK**.

Create or edit domain name exceptions

Procedure

1. Select **Profiles** > **Inspection Profiles** > **Default** > **Reputation/Geo**
2. Click the **Exceptions** tab.
3. Click **Add** or select a domain name, and then click **Edit**.

Important

You must explicitly list each domain name that you want to exclude from the filters. Wildcards, such as an asterisk (*), do not work.

4. Click **OK**.

Traffic Management filters

Traffic Management filters react to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values. For example, you might define the following Traffic Management filters for your web servers in a lab that denies access to external users:

- Block traffic if the source is on an external subnet that arrives through port 80 and is destined for the IP address of your web server.
- Block traffic if the source is your web server, the source port is 80, and the destination is any external subnet.

These filters detect issues in bandwidth usage. Because the SMS does not include these filters, you must create them.

Note

Traffic Management filters differ from other traffic-shaping filters, such as *Traffic Normalization on page 5-34*, which are Infrastructure Protection filters that enforce valid packet processing within the Threat Suppression Engine. Traffic Normalization filters protect the engine by detecting invalid or abnormal packets. By protecting the engine, the filters scrub the network of possible issues.

Maximum filter limits

The SMS enforces the maximum number of Traffic Management filters that can be distributed to a device based on device capacity. The SMS groups devices into three categories (low-end, medium-end, and high-end) with an assigned maximum to each category for enforcement purposes.

The SMS takes into consideration the expanded Traffic Management filters as well as the target device model. If the number of Traffic Management filters for a device exceeds the limit, the SMS displays a message.

Traffic Management filter limits include:

- Medium-end device limit: 8,000 filters (Medium-end devices include NX-Platform, 440T, and vTPS devices).
- High-end device limit: 12,000 filters (High-end devices include 2200T, TX Series, and TXE Series devices).

Create or edit a Traffic Management filter

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Traffic Management**.
2. Click **New** or select an existing Traffic Management filter, and click **Edit**.
3. Select the appropriate parameters in the Traffic Management Filter dialog.

   Keep the following information in mind:

   - Traffic Management filter names must be unique within a profile. The SMS gives each filter a unique ID, which it uses as a reference in the system.
   - Enter the IP address in the Source or Destination address field to create an unnamed IP address group. Click the **Right arrow** next to the address field to select or create a named IP address group. *Learn more on page 8-126*.
     - Sending too many Traffic Management filters to the device can exceed the device maximum. For more information, see *Maximum filter limits on page 5-47*. To prevent this, ensure that the source or destination addresse has a value of **Any/Any IPv6**. For example, if you select the **IPv6** protocol, select **Any IPv6** for the source or destination addresses. Learn more.

- The SMS uses cross multiplication when distributing Traffic Management filters to pair the source and destination addresses. For example, a single Traffic Management filter that has 10 addresses in its source group and 10 addresses in its destination group will produce 100 Traffic Management Filters upon distribution.

Advanced DDoS

Advanced Distributed Denial of Service (DDoS) filters enable you to create filters for detecting denial of service attacks. When using Advanced DDoS Protection filters, keep in mind the following:

- You must place the device in a Symmetric Network.
- You must disable Asymmetric Mode for the device.
- The device must see both sides of the traffic.

Create or edit an Advanced DDoS filter

Procedure

1. Select **Profiles** > **Inspection Profiles** > **[Profile Name]** > **Advanced DDoS**.
2. Click either **New** or select an existing filter, and click **Edit**.
3. Select the appropriate **Filter Parameters** in the Advanced DDoS Filter dialog.

   Keep the following information in mind:

   - Before you can create a new Advanced DDoS filter, you must have an action set that has a block action and does not perform a packet trace.
4. Select **SYN Proxy Settings** to:

   - Protect against SYN floods of the system. Typical SYN Flood attacks overwhelm a server with malicious connection requests (TCP SYNs)

with spoofed source IP addresses and prevent legitimate clients from accessing the server.

- The IPS acts as a proxy, synthesizing and sending the SYN/ACK packet back to the originator, waiting for the final ACK packet. After the IPS receives the ACK packet from the originator, the IPS then "replays" the three-step sequence to the receiver.
- In the event of a distributed attack with random spoofed source addresses, SYN Proxy protection temporarily blocks new connections to the server without interfering with existing connections.

If you select the **Enabled** check box, specify the number of SYN requests allowed per second (1 to 10,000) for the **Notification Threshold**.

5. Click **OK**.

Editing filters

You can tune filters to meet the needs of your enterprise. You can modify a filter or add an exception to a filter. You also can alter the system response to an attack filter by editing the action set, changing how or when contacts are notified, or even disabling the filter.

The following tasks apply to most security and application filters:

- *Edit a filter on page 5-50*
- *Edit multiple filters on page 5-51*
- *Add a filter exception on page 5-51*

Edit a filter

If a filter has inherited settings and the base filter is locked, you cannot edit the filter with inherited settings.

Procedure

1. Select **Profiles** > **Inspection Profiles**, and search for or locate the filter you want to edit.

2. Select a filter from the Search Results, and click **Edit**:
   - Select **Use Filter Specific Settings** to customize the action setting for the selected filter.
   - To modify the action set for multiple filters within a category, edit Category Settings.
   - To apply the adaptive filter settings for flow control, configure adaptive filtering.
   - To create a custom filter exception, click **Add** under **Exceptions**.
3. To re-distribute the modified filter, click **Distribute**.
4. Click **OK**.

Edit multiple filters

When viewing a list of filters, you can select multiple filters to edit.

Procedure

1. Select multiple filters within a global search or within a selected profile search.
2. Select **Filter Settings**, and modify the appropriate settings.
3. To re-distribute the modified filters, click **Distribute**.
4. Click **OK**.

Create or edit a filter exception

When you create a filter exception, you exclude the IP address group from being the target of the action set for the selected filters. The filter exception applies only to the selected filter; it does not globally affect all filters.

Important

The SMS restricts the number of IP addresses used in filter exceptions, restrictions, and quarantined access for a profile to 65,536. If a profile exceeds this limit, you cannot distribute the profile. This limit promotes better performance for your system. Saving and distributing too many filter changes to a device at one time can cause problems with performance, out-of-memory errors, and fallback mode for High Availability (HA).

Procedure

1. Select **Profiles** > **Inspection Profiles**, and search for or locate the filter you want to edit.
2. Click **Add Exception**.
3. Enter a **Name** for the exception.
4. Under **Source IP Address**, do one of the following:
   - Select **Any IP** to indicate that traffic flowing from any IP address will not be inspected by this filter.
   - To create an unnamed IP address group, select **IP Address** and specify an IP address.

     After you create the filter exception, select **Admin** > **Named Resources** > **IP Address Groups** > **Show Unnamed Items** to view this IP address group.
   - To select (or create) a named IP address group, click the **Right arrow** next to the **IP Address** field.

     From here, you can search for, select, or create a new IP address group. For more information, see *Named resources on page 8-123* and *Create or edit named resource groups on page 8-126*.

     Traffic flowing from the specified source will not be inspected by this filter.
5. Enter the **Destination IP Address**.

Follow the same guidelines for the **Source IP Address**.

6. Click **OK**.

Filter details

When you search for and select a filter, you can review the settings and details for the filter. Trend assesses each filter and assigns a category, severity, and recommended action. You can also view the filter name, and the dates the DV filter was distributed or last modified, and the name of the profile the filter is assigned to.

Note

You must activate a new DV before you can search for filters by released or last modified dates or view the dates in the Search Results.

Digital Vaccines

A Digital Vaccine is a security package that includes filters for protecting your network system against vulnerabilities. These filters provide new signatures to protect against researched threats to network security. Digital Vaccines help you control your organization's software management life cycle by providing coverage between the discovery of a vulnerability and the availability of new software. Digital Vaccines also protect your network from deprecated software. Delivered weekly, or immediately when critical vulnerabilities emerge, you can deploy Digital Vaccine filters automatically to your devices.

Select **Profiles** > **Digital Vaccines** > **DV Inventory** to view the active Digital Vaccine package. The DV Inventory table lists the Digital Vaccine packages that have been downloaded and are available for distribution to your devices.

The Distribution Progress table provides information on distribution status of a Digital Vaccine. *Learn more on page 5-61*. You can schedule one time or recurring Digital Vaccine distributions. *Learn more on page 5-63*.

Column	Description
Version	Digital Vaccine package version. An updated Digital Vaccine is released every week, separate for different TOS versions. We recommend that you download the same Digital Vaccine for all of your managed devices. Note the following: • 3.2 = Devices must run TOS v3.2.0 or later for this Digital Vaccine. • 4.0 = This Digital Vaccine is available only on vTPS and TXE devices.
Active	Indicates that the Digital Vaccine is active. You cannot delete an active package.
vTPS DV	A check mark indicates that the Digital Vaccine package is only available for vTPS devices.
Released	Date and time the package was released.
Downloaded	Date and time the package was downloaded.
Size	Digital Vaccine file size.
Devices	The number of devices that have received the package.

Auxiliary Digital Vaccines

Auxiliary Digital Vaccines are specialized filter packages that address specific security needs. Threat DV is a type of Auxiliary Digital Vaccine that prevents and disrupts malware activity. The combination of *malware filters on page 5-76* and the *Reputation feed on page 5-36* protects your data and helps optimize network performance. Threat DV augments the protection provided by the Digital Vaccine, and is independent of the Digital Vaccine that is installed on the SMS. For more information about obtaining the Threat DV subscription service, contact your TippingPoint representative.

Select **Profiles** > **Auxiliary DVs** to view the active Auxiliary Digital Vaccine package. The Auxiliary DV Inventory table lists the packages that have been downloaded and are available for distribution to your devices.

The Distribution Progress table provides information on distribution status of an Auxiliary Digital Vaccine. *Learn more on page 5-61*.

You can schedule a one time or recurring Auxiliary Digital Vaccine distribution. *Learn more on page 5-63*.

Column	Description
Category	Filter category. Threat DV malware filters fall into the same categories used for Digital Vaccine vulnerability filters, and display accordingly when you view the filters for a profile.
Version	Threat DV package version. An IPS device must be running TOS v3.7 or later for Threat DV.
Active	Indicates that the Threat DV package is active. You cannot delete an active package.
Released	Date and time the package was released.
Downloaded	Date and time the package was downloaded.
Size	Threat DV package file size.
Description	Threat DV package description.
Devices	The number of devices that have received the package.

Automatically download, activate, and distribute packages

You can configure the SMS to automatically download the latest Digital Vaccine and Auxiliary Digital Vaccine packages from the TMC. When a package is automatically downloaded, you can activate it on the SMS. However, the Digital Vaccine or Threat DV package has no impact on your current profiles until you distribute it to a device.

Procedure

1. Do one of the following:
   - Select **Profiles** > **Digital Vaccines** > **Auto DV Activation** > **Edit** to edit Digital Vaccine settings.
   - Select **Profiles** > **Auxiliary DVs** > **Auto Auxiliary DV Activation** > **Edit** to edit Threat DV settings.

2. Select **Automatic Download** to automatically download packages as they become available on the TMC.
3. Select **Automatic Activation** to automatically activate the package on the SMS.

Note

An automatically downloaded package will not be activated if its major version is different than the major version of the currently active Digital Vaccine on the SMS. You must activate the Digital Vaccine or Auxilary Digital Vaccine before you can search for the filters that are within that package.

4. Select **Automatic Distribution** to enable the SMS to automatically distribute the package to all available devices.
5. Select **DV Notification Popups** to display a notification dialog box when a new package is available. This option is available when the **Automatic Download** is disabled, and only affects the current user.
6. Click **OK**.

Manually download, import, and activate packages

You can manually download, import, and activate Digital Vaccine and Threat DV packages.

Procedure

1. Do one of the following:
   - Select **Profiles** > **Digital Vaccines** > **Download from TMC**, and then select a Digital Vaccine version to download.
   - Select **Profiles** > **Auxiliary DVs** > **Download**, and then select a Threat DV version to download.
2. (Optional) Click **Import** to browse to and select a package that has been previously downloaded from the TMC. To avoid unexpected behavior on the SMS, do not change the name of this file.

3. Select a package from the inventory, and then click **Activate**.

Note

Activate the package in order to search for filters that are within the package.

View Digital Vaccines or Auxiliary Digital Vaccines

You can view a list of Digital Vaccine or Auxiliary Digital Vaccine packages installed and activated on the SMS.

Procedure

1. Do one of the following:
   - Select **Profiles** > **Digital Vaccines** to view the inventory of Digital Vaccine packages.
   - Select **Profiles** > **Auxiliary DVs** to view the inventory of Auxiliary Digital Vaccine packages.
2. Select a Digital Vaccine or Auxiliary Digital Vaccine from the inventory, and do the following:
   - Click the **Details** tab to view information about the file size, release date, and download date.
   - Click the **Release Notes** tab to view a list of new filters, in addition to filters that have been modified or removed from the package.
   - Click the **Deployments** tab (only available for Digital Vaccines) to view descriptions about the different deployment types on the SMS. *Learn more on page 5-12*.

Distribute a Digital Vaccine or Auxiliary Digital Vaccine

After you activate a Digital Vaccine or Auxiliary Digital Vaccine on the SMS, you must distribute it to a device. Activating a package only enables it for distribution, it does not enable the filters within it. When you distribute a

package, the SMS updates filter settings on the device including new filters in addition to filters that have been modified or removed from the package.

Note

We recommend that you distribute the active Digital Vaccine, Auxiliary Digital Vaccine, or DV Toolkit to the device before you distribute the profile to the device.

Uninstall an Auxiliary Digital Vaccine

Uninstalling an Auxiliary Digital Vaccine uninstalls filters associated within that package but does not remove the filters from the profile. You must distribute the profile to the device to completely uninstall Auxiliary Digital Vaccine filters from the device.

Profile distribution

When you distribute a profile, you send the modified and updated profile to selected segments or devices.

To distribute an inspection profile to segments, select **Profiles** > **Inspection Profiles**, and then select a profile and click **Distribute**.

Note

If the profile distribution is unsuccessful due to a time-out, contact a TippingPoint technical support representative to assist in extending the time-out setting for your profile distribution needs.

Distribution considerations

Keep in mind the following distribution best practices:

- **Segment groups** - To control which updates segments receive, you can create segment groups. You can then send profile updates, including all custom changes to filters, shared settings, action sets, and notification contacts according to the group.

When distributing a profile, you can also select to distribute to the entire segment group, a single segment, several segments, or a combination of segments and segments groups.

- **Filter overrides** - Filter modifications that require distribution include the following items:
  - New, modified, or deleted shared and custom filter exceptions.
  - New, modified, or deleted filters.
  - Modified Traffic Management filters. The SMS enforces the maximum number of Traffic Management filters that can be distributed to a device based on device capacity.
  - Changing the order of the Traffic Management filters.

Note

When you enter a significant number of changes to filters within a profile, the period of time required for distributing the profile increases.

- **Named resources** - Devices are not aware of named resources. When you distribute a profile that contains named IP address groups, the SMS sends every combination of the source and destination IP address pairs to the device. For example, if a filter exception has a source and destination named IP address group and each group has two IP addresses, then the SMS will send four filter exceptions to the device, and each exception will contain a pair of source and destination IP addresses.
- **Digital Vaccine, Auxiliary Digital Vaccines, and DV Toolkit packages** - When you distribute a profile, the SMS verifies that all managed devices run the same Digital Vaccine, Auxiliary Digital Vaccine, or Digital Vaccine Toolkit versions. We recommend that you distribute the active Digital Vaccine, Auxiliary Digital Vaccine, or DV Toolkit to the device before you distribute the profile.
  - An active DV Toolkit package enables the package for distribution; it does not enable the filters in the DV Toolkit package. You must

distribute the package and the profile to the device to enable the filters within the DV Toolkit package. When you distribute a DV Toolkit package, you update the filter settings for the device. A package may include modifications, such as new filters, modified filters, and removed filters.

- The SMS merges multiple DV Toolkit packages into a single package as the device only supports one DV Toolkit package.

High priority

When performing a distribution of the update, you can select a high or low priority. The priority aids in performance of the system. High priority updates distribute before low priority. Low priority updates are regulated to ensure the best performance of the system.

When you select a high priority, it takes precedent over a low priority update. However, during the update, you might have dropped packets as traffic and performance are hampered during the update. If you do not want this loss of packets, you can select a low priority.

From a device perspective, unless the traffic through the device is low (or in fallback mode), you should always do high priority updates from the SMS. Selecting low priority updates can take hours to perform a full update without a loss in traffic packets depending on the level of traffic.

To designate a distribution as high priority, select the **High Priority** check box on the Distribution dialog.

Distribute a profile

Distribute a profile to a device or segment.

Procedure

1. Select **Profiles** > **Profiles** > **Inspection Profiles**.
2. Select one or more profiles, and then click **Distribute**.
3. Select **Allow Segment Selection** to view segments organized by device or segment group.

4. For a high priority distribution, select the **High Priority** check box.
5. (Optional) If there is a profile you do not want to distribute at this time, clear the **Distribute this profile when I click 'OK'** check box for that profile.
6. Click **OK**.

Multiple profiles

Distributing multiple profiles together allows you to save time. Each profile must still be targeted to a specific group, but you can configure the distribution of the profiles so they will all start distributing when you click **OK**.

To avoid distributing a profile when you have multiple profiles selected, deselect the **Distribute this profile when I click 'OK'** check box for profiles that you do not want to distribute.

This allows you to distribute some profiles when you click OK but not distribute others, without losing work. For example, if you have spent the past 20 minutes configuring the profile distribution of 5 profiles and realize you don't have the information you need to distribute the 6th profile, deselect this check box for the 6th profile. When you click OK, the other profiles will distribute but the 6th profile will not.

Distribution progress

You can view distribution progress for the following:

- Profiles
- Digital Vaccines
- Auxiliary Digital Vaccines (ThreatDV)
- DV Toolkit packages
- TippingPoint OS

Column	Description
Device	Distribution to the number of devices. Expand to display a list of devices.
Package	Name/package version.
Submit Time	Date and time the distribution was submitted.
Start/End time	Start/end date and time of the distribution.
Status	Distribution status. For ease of monitoring, distribution tasks are grouped by status including Pending, Success, Failed, or Canceled.
Extended Status	Indicates whether additional status information related to this specific distribution is available.
Progress	Current progress of the distribution. You cannot cancel a distribution after the device begins installing the package. To view distribution progress, click **Details**. Click **Clear Obsolete** to remove all distribution records except for the last distribution.

Scheduled distributions

The SMS provides the flexibility to schedule distributions to meet the specific needs of your network. For example, you can schedule distributions during off-peak times or take advantage of a maintenance window.

Select **Profiles** > **Scheduled Distributions** to view Profile, Digital Vaccine, and Auxiliary Digital Vaccine distribution schedules.

The Scheduled Distributions page also displays the current SMS server time.

Column	Description
Schedule Name	Name of the schedule.
Package	Name of the profile, or the Digital Vaccine or Auxiliary Digital Vaccine package version.

Column	Description
Schedule	Scheduled distribution time.
Last Run	Date and time the package was last distributed.
Status	Distribution status. *On Going* displays for a recurring distribution and *Scheduled* displays for a single distribution.
Targets	Name of the segment, segment group, or device that will receive the distribution.

Create a new scheduled distribution

You can schedule distributions for the following:

- Profiles
- Digital Vaccines
- Auxiliary Digital Vaccines (ThreatDV)

Procedure

1. Select **Profiles** > **Scheduled Distributions**.
2. Click **New** to create a new schedule, or **Edit** to change an existing one.
3. Under the General Settings tab:
   a. Enter the name of the schedule.
   b. Select whether the schedule type is one time or recurring. For a **one time** schedule, click the calendar and select a date and time. For a **recurring** schedule, select the days and enter the time.
   c. Select a package. For Inspection profiles, select a profile name. For Digital Vaccines and Threat DV, select the *latest available*, or select a package.
   d. Click **Next**.
4. (Profiles) Under the Segment Targets tab:

a. Select **Allow Segment Selection** to view segments organized by device or segment group.

5. (Digital Vaccines and ThreatDV) Under the Device Targets tab:

   a. Choose **Select Devices** from the Device Targets, and then select one or more devices.

6. Select **High Priority** if you want the distibution delivered at a high priority.

7. Click **Finish**.

Digital Vaccine Toolkit Packages

Digital Vaccine Toolkit is a TippingPoint application that lets you write custom filters for use on devices and the SMS. Custom filters are saved into package files, imported into the SMS, activated, and then distributed to devices.

When you activate a DV Toolkit package, a new SMS filter number is created. When you distribute the package, the filter number is synchronized across:

- **SMS Profiles** (search results and filter details)
- **SMS Reports**. However, if an existing or saved report has a DV Toolkit filter number (generated in a previous SMS release), the report still displays that number, not the new filter number.
- **SMS Events**. However, if an event listing has a DV Toolkit filter number from a previous SMS release, the event still displays that number, not the new filter number.
- **CLI** (`show filter` and the `show np rule` commands)
- **DV Toolkit application**. When you export a DV Toolkit package from the SMS and import it on the DV Toolkit application, the package retains the filter number assigned to it by the SMS.

Note

The SMS only preserves filter numbers when the DV Toolkit package is exported and imported back on to the same SMS. The SMS might not preserve the filter numbers if the DV Toolkit package is imported into a different SMS.

Original filter names and numbers assigned from the DV Toolkit application are included on the SMS

The SMS saves the filter name and number that was originally created from the DV Toolkit application. You can view this information on the SMS in the Search Results and the Events table.

Note

These table columns are hidden by default. To display them, right-click the Search Results table, select **Table Properties**, and click the **Visible** checkbox for those columns.

View DV Toolkit filter numbers on the device CLI

Use the `show filter` and the `show np rule` commands to view the SMS-assigned filter number. When entering these commands on the device CLI, do not include `C` with the filter number.

You cannot view the original filter number that was created from the DV Toolkit application on the device CLI.

Associate DV Toolkit packages with devices and profiles in the SMS

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

Procedure

1. *Create a DV Toolkit package on page 5-66*.
2. *Import a DV Toolkit package on page 5-67*.

3. *Activate a DV Toolkit package on page 5-68*.
4. *Create an inspection profile on page 5-14* (or edit an existing profile). Using this profile, you can *review filters from the active DV Toolkit packages and enable filter settings on page 5-69*.
5. Distribute a DV Toolkit package to the device.
6. *Distribute a profile to the device on page 5-58*.

Create DV Toolkit packages

Use the DV Toolkit application to create and save custom filters to a package file. For instructions on creating DV Toolkit packages, see the *Digital Vaccine Toolkit and Converter User Guide* available on the TMC at https://tmc.tippingpoint.com/TMC/.

Limit access to DV Toolkit packages

You can use role-based access control for DV Toolkit packages. Access control lets you independently customize access rights and restrictions for each user based on role and group settings. As a result, you can set up DV Toolkit packages that only a certain group of users can see. Multiple users can have separate, active DV Toolkit packages running on the same SMS.

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

- Create (or edit) a role and set capabilities for DV Toolkit Management.
- Create (or edit) a group for each role and set which DV Toolkit packages the group can access (**Create Group** > **DV Toolkit Packages**).
- Create (or edit) a user and assign the group to the user (**Create User** > **Group Membership**).

DV Toolkit Packages

The DV Toolkit Packages page lists the DV Toolkit packages that have been imported and are available for distribution. The Distribution Progress table

provides information on distribution status of a DV Toolkit package. *Learn more on page 5-61*.

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

Import a DV Toolkit package

When importing DV Toolkit packages, keep in mind:

- You must have a DV Toolkit package file. You can create this file using the DV Toolkit application.
- If you do not provide a name for the properties when you create the package it in the DV Toolkit application, the package name displays "untitled" in the SMS after you import it. It's a best practice to use a distinct name for the properties when you create the DV Toolkit package file. Within the DV Toolkit application, select **File** > **Properties** to change the name of the properties for the package.
- You can activate a new DV Toolkit package, or you can replace a currently active package (the SMS keeps the filter overrides for the previously active package).

Procedure

1. Select **Profiles** > **DV Toolkit Packages**.

2. Click **Import**.
3. Click **Browse** to browse to and select a DV Toolkit package file.
4. To automatically activate the package and replace an existing (active) package, do the following:
   a. Select the **Activate the imported DV Toolkit package** check box.
   b. Click **OK**.
   c. Do any of the following:
      - To activate the new DV Toolkit package, click **Activate**. (The DV Toolkit package will be activated as a new package and will not be associated with existing filter overrides in any other package).
      - To replace an existing, active package, select the **Overwrite a currently active DV Toolkit with the activating DV Toolkit** check box, select a DV Toolkit package from the list of active packages, and then click **Overwrite**. The DV Toolkit package will replace the selected package and the SMS will keep the filter overrides for the previously active package. If a filter is deleted from a package, then those filter overrides will also be removed from the profile.
5. Click **OK**.

   The package displays in the DV Toolkit Inventory table and the DV Toolkit Packages navigation pane. If the package is active, a green check mark displays under the Active column, and (active) displays after the package name in the DV Toolkit Packages navigation pane.

Activate a DV Toolkit package

There are three ways to activate a DV Toolkit package.

- *When you import the DV Toolkit package on page 5-67*
- From the DV Toolkit Inventory
- From the DV Toolkit Details

When activating DV Toolkit packages, keep in mind:

- You can have multiple, active DV Toolkit packages on the SMS.
- After you activate a DV Toolkit package, you can search for (or create) an Inspection profile to review the filters in the DV Toolkit package. You can select one or more filters and edit the filter settings. By default, all filters in the DV Toolkit package are not enabled and have no recommended action set.
- You cannot delete an active DV Toolkit package. To delete a package, you must first deactivate it.

Procedure

1. Do any of the following:
   - Select **Profiles** > **DV Toolkit Packages** and select a package from the DV Toolkit Inventory table.
   - Click **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select a package.
2. Click **Activate**.

Search for DV Toolkit filters

When searching for DV Toolkit filters, keep in mind:

- After you activate a DV Toolkit package, you can search for (or create) an Inspection profile to review the filters in the DV Toolkit package. You can select one or more filters and edit the filter settings. By default, all filters in the DV Toolkit package are not enabled and have no recommended action set.
- After you activate a DV Toolkit package, the SMS assigns a new filter number. You can view this filter number in the Search Results and the Filter Settings.
- The SMS also saves the filter number that was created from the DV Toolkit application. You can view this filter number in the Search Results and Events.

- You can only search across the active DV Toolkit packages that you have access to. Access control lets you independently customize access rights and restrictions for each user based on role and group settings. See *Limit access to DV Toolkit packages on page 5-66*.

Procedure

1. Select **Profiles** > **Inspection Profiles** and select an existing Inspection Profile. Alternatively, you can create a new profile. See *Create a new profile on page 5-14*.
2. To search for the filters in a DV Toolkit package, do any of the following:
   - Click **Global Search** to search across all listed Inspection Profiles for a DV Toolkit package.
   - Expand the name of a profile, and then click **Search** to perform a search within a selected profile. See *Search on page 5-26*.
3. Expand the **Source Criteria** panel, select the **DV Toolkit** check box, and then do the following:
   - Select an active DV Toolkit package from the drop-down list.
   - Select **ANY** to search across all active DV Toolkit packages.
4. Click **Search**.

   Based on the source criteria, the filters display in the search results.
5. To edit a filter, do any of the following:

SELECT A FILTER	EDIT FILTER SETTINGS - ACTIONS
To enable one filter in a DV Toolkit package, double-click a filter name from the search results.	• Select **Use Filter Specific Settings**. • Select the **Enabled** check box. • Select an action from the **Action Set** drop-down list.
To enable more than one filter in a DV Toolkit package, select one or	• Select **Change filters to use the settings below**. • Select **Use Filter Specific Settings**.

Select a filter	Edit filter settings - Actions
more filters from the search results, and then click **Edit**.	• Select the **Enabled** check box. • Select an action from the **Action Set** drop-down list

View original DV Toolkit filter names and numbers in the search results and events

After you *activate* a DV Toolkit package, you can view the original DV Toolkit filter name and number in the Search Results. To view the DVT filter name and numbers in the Search Results, you must first set the visibility as the Original DVT Filter # and Original DVT Filter Names columns are hidden by default.

Procedure

1. Select **Profiles** > **Inspection Profiles** > **Search**.
2. Right-click on the Search Results, and then select **Table Properties**.
3. Locate the **Original DVT Filter Name** column name, and then select the **Visible** checkbox.
4. Locate the **Original DVT Filter #** column name, and then select the **Visible** checkbox.
5. Click **OK**.

View DV Toolkit details

The DV Toolkit Details screen includes the following information:

- **DV Toolkit Details —** Provides information about the imported DV Toolkit package.
- **Device DV Toolkit Inventory —** Lists the name of the devices that have received the distributed package. You can distribute the DV Toolkit package to more than one device at a time.

Do any of the following:

Procedure

- Select **Profiles** > **DV Toolkit Packages**, select a package from the DV Toolkit Inventory table, and then click **Details**.
- Select **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select a package.

Remove DV Toolkit packages from the device and the SMS

Removing DV Toolkit packages from the device and the SMS involves these steps.

Procedure

1. *Deactivate a DV Toolkit package on the SMS on page 5-72*.
2. Redistribute the profiles that have filter overrides from the DV Toolkit package to the device(s).
3. *Uninstall a DV Toolkit package from the device on page 5-73*.
4. *Delete a DV Toolkit package from the SMS on page 5-74*.

Note

If you deactivated or deleted a DV Toolkit package from the SMS that you want to uninstall from the device, you must re-import the package and then uninstall it from the device.

Deactivate a DV Toolkit package on the SMS

When deactivating DV Toolkit packages on the SMS, keep in mind:

- You can only deactivate packages that are active. You must deactivate a package before you can delete it.
- The package is still available on the device. To remove a package from the device, you must uninstall it. See *Uninstall a DV Toolkit package from the device on page 5-73*.

- When you deactivate a package, the SMS:
  - Removes all existing profile filter overrides in the package.
  - Removes the name of the package from the Inspection Profile search and global search (Source Criteria panel).
  - Keeps the name of the package in the DV Toolkit Inventory table, DV Toolkit packages navigation pane, and the configuration and summary areas (Device Summary screen, Device Configuration Summary, and Device Configuration wizard). You must distribute the active DV Toolkit packages to the device to remove the package from the configuration and summary areas. You must delete the package to remove it from the inventory table and navigation pane. You can also uninstall the package that was deactivated.

Procedure

1. Do any of the following:
   - Select **Profiles** > **DV Toolkit Packages** and select an active package from the DV Toolkit Inventory table.
   - Select **Profiles**, expand **DV Toolkit Packages** in the navigation pane, and then select an (active) package.
2. Click **Deactivate.**

Uninstall a DV Toolkit package from the device

When uninstalling DV Toolkit packages to the device, keep in mind:

- You can only uninstall packages that have been distributed to the device.
- When you uninstall a package, the SMS:
  - Removes the package from the device. However, if the device has other active packages, these packages will be distributed to the device, and a new package will be created. To remove a package from the SMS, you must deactivate it. See *Deactivate a DV Toolkit package on the SMS on page 5-72*

- Removes the name of the package from the Device Summary screen, the Device Configuration Summary screen, and the Device Configuration wizard.
- Keeps all existing profile filter overrides in the uninstalled package.
- Keeps the name of the package in the DV Toolkit Inventory table, the DV Toolkit packages navigation pane, and the Inspection Profile search and global search (Source Criteria panel).

Procedure

1. Select **Profiles** > **DV Toolkit Packages**.
2. Select a package that has been distributed to a device from the DV Toolkit Inventory table.
3. Click **Uninstall**.
4. Do any of the following:
   - Click the **All Devices** check box to uninstall the package from all of your managed devices.
   - Expand **All Devices**, and then select one or more devices.

     Select a device to be aware of the impact of the DV Toolkit package. Use the icons to see if a package will be added, removed, or replaced on the selected device.
   - (Optional) Click the **High Priority** check box to designate the DV Toolkit package distribution as high priority. High priority updates will run before low priority updates.
5. Click **OK**.

   The package distributes to the selected device.

Delete a DV Toolkit package from the SMS

When deleting DV Toolkit packages from the SMS, keep in mind:

- You can only delete packages that are inactive. See *Deactivate a DV Toolkit package on the SMS on page 5-72*
- If the package was distributed to the device, it will still be available on the device. To remove the package from the device, you must uninstall it.

Procedure

1. Select **Profiles** > **DV Toolkit Packages**.
2. Select an inactive package from the DV Toolkit Inventory table, and then click **Delete**.

Reputation database

The TippingPoint Reputation Database is a collection of IP addresses within a geographic region or country, DNS names, and URLs on an SMS that represent potential risks to network security. Entries can be user-provided, provided from the ThreatDV Feed, or both. There is no limit to the number of entries a user can provide. Entries in the Reputation Database can be tagged or untagged. A tagged entry consists of an IP address, a DNS address, or a URL, plus a reputation tag category and associated values. A tag category can be created manually or by ThreatDV. Tag categories created by the reputation service are read-only and may not be modified.

Entries can also be imported from a CSV file and must follow specific import Reputation rules. Untagged entries contain only an IP address, a DNS address, or a URL, and function as a user-defined list of sites to block.

You can create an exception to prevent internal IP address from being used in a Reputation filter.

Note

The SMS ignores any invalid entries imported from a CSV file. All IP, DNS, and URL tagged entries must be valid and correctly formatted before the SMS can apply the tag category values.

Reputation entries in the Reputation Database are used to create Reputation filters that target specific security needs of your network. See *Reputation filters on page 5-40*.

Malware filters

Malware filters are delivered weekly through the Threat DV package to protect you from the latest advanced threats. These filters provide alerts on a wide range of malware families and are designed to detect post-infection traffic, including:

- Bot activity
- Phone-home
- Command-and-control (C&C)
- Data ex-filtration
- Mobile threats
- Domain Generating Algorithm (DGA)

Note

A majority of filters in a malware filter package are disabled by default to prevent false positives or performance impacts.

In general, when you deploy a malware filter package:

- Use your initial deployment as a trial run to detect potential problems.
- To establish an initial baseline or to monitor events and enable filters without blocking or other disruptive action sets, enable a subset of malware filters with **Permit + Notify**.
- Monitor events and evaluate filters that trigger to determine if they constitute a true threat or a false-positive. If you suspect an imminent threat, enable the filter that addresses the threat with **Block** or **Block + Notify**.
- Adjust filter settings accordingly to ensure the appropriate response and continue monitoring, evaluating, and adjusting to mitigate threats.

- If you enable Adaptive Filter Configuration (AFC), the behavior of a Threat DV malware filter might be altered according to the AFC mode enabled for the device.

DGA filters

Various malware families use Domain Generating Algorithms (DGA) to randomly generate a large number of domain names to avoid hard-coding IP addresses or domain names within the malware. The infected host then attempts to contact some of the generated domain names to communicate with its C&C servers.

DGA filters use pattern recognition and linguistic analysis to detect algorithmically generated DNS requests from infected hosts. As part of the malware filter package, these filters protect your system against known malware families, in addition to suspicious domain names generated by unknown malware families.

Note

To effectively use DGA filters, your device must be deployed so that it is in the flow of DNS requests from your network. If your device is deployed between the DNS server and the Internet or other DNS servers, it could block normal DNS traffic. To avoid inadvertently blocking normal DNS traffic, add filter exceptions for your DNS servers. In some networks, a DNS server or aggregator may be behind your device, which may result in the DNS server or aggregator appearing to be infected with malware when it is actually just forwarding requests.

DNS response

There are two types of DNS Response DGA filters: NOERROR and NXDOMAIN.

- NOERROR filters detect a NOERROR DNS response. A NOERROR response to a DNS query means that the hostname that was queried exists and is well-formed.

Evaluate these filters individually to ensure that there are no performance impacts. You can safely deploy these filters with **Permit + Notify + Trace** enabled to examine each event and make an informed decision. If, after evaluation, you decide a filter is necessary, change the action set to **Block** without a trace.

- NXDOMAIN filters detect an NXDOMAIN DNS response. An NXDOMAIN response to a DNS query means that the hostname that was queried does not exist.
  NXDOMAIN filters are much less likely to have performance impacts or false positive concerns. Enable **Trace** so that you can identify the domain name that is being requested to determine if it is a DGA or a valid host. You can safely deploy these filters with **Block + Notify + Trace** enabled.

19665: DNS: Suspicious DNS Lookup NOERROR Response (DGA)

This filter detects a NOERROR response to a DNS query for a hostname that appears to be using a generic or unknown DGA. The NOERROR response means that the queried domain is valid and exists. This could indicate an active attempt by a malware campaign to exfiltrate data or otherwise control a compromised host. However, due to the nature of this detection method, this filter is prone to false positives in certain situations as outlined below.

What It Does

This filter is effective at detecting hosts that are compromised by an unknown family of malware and are involved in active communication with a C&C server. It can be used to find and remediate malware infections.

What It Doesn't Do

This filter will not prevent a host from becoming compromised in the first place. This detection method is post-infection only. It should also be noted that this filter only detects the DNS portion of communication with a C&C server. Other parts of the exploitation chain such as HTTP, FTP, or other protocols are out-of-scope for this filter.

Deployment Recommendations

There is some risk of false positives as well as performance impacts in DNS-heavy environments. Because of this, the filter is not enabled by default, and it is recommended that you fully vet this filter in your particular environment before enabling it. This filter is most effective when deployed with **Trace** enabled so that you can examine the hostname that was being queried and decide on further actions from there.

Examples

True positives:

- tvjky3xzsmbxvpqgd.com
- zbjvpmtovtusimgw.com
- mzqdx.com

False positives:

- Acronymized domains, especially Chinese acronyms, such as sxbznqp.com

20602: DNS: Suspicious DNS Lookup NXDOMAIN Response (DGA)

This filter detects an NXDOMAIN response to a DNS query for a host name that appears to be using a generic or unknown DGA. The NXDOMAIN response means that the queried domain does not currently exist. This is an extremely strong indicator that the host sending out the DNS queries has been compromised and is attempting to contact a C&C server to receive further instructions.

What It Does

This filter is effective at detecting compromised hosts that are compromised by an unknown family of malware. It can be used to find and remediate malware infections before the host is able to find and communicate with a C&C server.

What It Doesn't Do

This filter will not prevent a host from becoming compromised in the first place; it is post-infection only. This detection method is not effective for catching malware that is actively in communication

with a C&C server. It should also be noted that this filter only detects the DNS portion of communication with a C&C server. Other parts of the exploitation chain such as HTTP, FTP, or other protocols are out-of-scope for this filter.

Deployment Recommendations

This filter does not suffer from any known false positives or performance impacts and can be safely enabled by default. If you are wanting an even more conservative approach, it can be enabled with thresholding, but you should be aware that different families of malware send their DNS queries at different frequencies, so some fine-tuning may be required. This filter is most effective when deployed with **Trace** enabled so that you can examine the host name that was being queried and decide on further actions from there.

Examples

True positives:

- tvjky3xzsmbxvpqgd.com
- zbjvpmtovtusimgw.com
- mzqdx.com

False positives:

- none

HTTP response

HTTP response filters detect an HTTP response from a web server for a hostname that appears to be using a generic or unkown DGA.

24119: HTTP: Suspicious HTTP Host Header HTTP Response (DGA)

This filter detects an HTTP request to a web server for a host name that appears to be using a generic or unknown DGA.

What It Does

This filter is effective at detecting hosts that may be compromised by malware and are involved in active communication with a C&C server. It can be used to find and remediate malware infections.

What It Doesn't Do

This filter will not prevent a host from becoming compromised in the first place. This detection method is post-infection only. It should also be noted that this filter only detects the HTTP portion of communication with a C&C server. Other parts of the exploitation chain such as DNS, FTP, or other protocols are out-of-scope for this filter.

Deployment Recommendations

There is some risk of false positives as well as performance impacts in HTTP-heavy environments. Because of this, the filter is not enabled by default, and it is recommended that you fully vet this filter in your particular environment before enabling it. This filter is most effective when deployed with **Trace** enabled so that you can examine the host name that was being queried and decide on further actions from there.

Examples

True positive: Host: aadcd15734d97346bb85f545dc8ca03e7e.com

Reputation database interface

The Reputation database interface includes a tabbed screen that displays Summary, Activity, and Tag Categories tabs. Each tab provides information about Reputation database activity.

Summary tab

The Summary tab provides a summary of the number of entries in the database and the status of the database synchronization progress.

Database summary

The Database Summary area lists the number of entries contained in the Reputation Database. Each entry in the database contains an IP address, a domain name, or a URL, and may have one or more associated tag categories with specified values. A Reputation Database entry must contain an IP address, a domain name, or a URL, but does not have to be associated with a tag.

Activity tab

The Activity tab provides information about Reputation Database activity including:

- Sync Progress — Information about the synchronization of the Reputation Database on the SMS to one or more target devices.
- Tasks — Information about Reputation Database tasks such as adding, editing or importing entries.

Sync progress

Changes to the Reputation Database are automatically synchronized to devices which have reputation filters active. A complete (Full) database synchronization is performed when reputation filters are distributed to a device. After the reputation filters are distributed and the full synchronization is performed, subsequent synchronizations contain only changed (Delta) entries. A full synchronization is only needed for recovery purposes. The Reputation Database updates the list of Reputation entries to be included on the device. Entries are selected according to the criteria provided in any active Reputation filters existing on the device.

This area provides the following information about a Reputation Database package:

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

Tasks

The tasks listed in this area include changes to the Reputation Database such as adding, editing or importing entries to the Reputation Database on the

SMS. For status information about synchronizing the database with target devices, see the Sync Progress area of this tab.

This area provides the following information about Reputation Database tasks:

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

View Reputation database details for distribution to device targets

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Details**. The Sync to Device dialog provides information:
   - Status Details — Summary information about the Reputation Database Synchronization/Distribution.
   - Target Details — Information about target devices associated with the Reputation Database Synchronization/Distribution.
4. Click **Close**.

Perform a full synchronization of the Reputation database

Changes to the Reputation Database are automatically synchronized to devices which have reputation filters active. A full database synchronization is only needed for recovery purposes.

Procedure

1. Select **Profiles** > **Reputation Database**.
2. On the **Edit** menu, click **Full Sync**.

Stop a synchronization of the Reputation database

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Stop Sync**.

Clear obsolete distribution entries

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Activity** tab.
3. Select a device on the Sync Progress pane, and then click **Clear Obsolete**.

Tag Categories

Use tag categories to define the types of tags that are used to tag reputation database entries. A tag category can be created manually, by ThreatDV, or be predefined on the SMS. Tag categories can be imported or exported as a group in .xml format.

To prevent duplicate definitions when importing profiles from another SMS or when managing a device that was managed by another SMS, export the Reputation tag categories from one SMS to the other. As a result, all SMS devices will recognize these tag categories as identical and will not treat them as different tag categories. You can then import or export tag categories many times between all SMS devices without resulting in duplicate

definitions because each SMS will recognize previously imported or exported tag categories and will not duplicate them.

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

Important

Only users with SuperUser permissions should use tag categories. For more information on account settings, see *Authentication and authorization on page 8-15*.

View integrated Advanced Threat Prevention data

The SMS integrates Advanced Threat Prevention from Deep Discovery devices.

The advanced threat intelligence provided in tag categories keeps the Reputation Database updated, and enables robust reputation filters for enhanced protection of your system.

You can either configure your DD device to send this data automatically to the SMS (as a tag entry), or you can use the SMS to manually add or import the entries. To configure this integration from your DD device, refer to the

documentation on the Trend documentation site. To add these entries manually, you must define the tag categories listed in the following table so that the specific data you need can be mapped to the SMS.

The SMS automatically includes the following predefined tag categories for Advanced Threat Prevention data.

Name	Type	Settings	Notes
Trend Micro Detection Category	List	Pre-defined values of: • Suspicious Object • C&C Callback Address	Specifies which category the detection falls under.
Trend Micro Publisher	Text	Up to 255 characters	Identifies the Trend product name that discovered the threat.
Trend Micro Severity	List	Pre-defined values of: • High • Medium • Low	Identifies the threat severity.
Trend Micro Source	Text	Up to 255 characters	Identifies the configured host name of the Trend device that discovered the threat.

Add or edit a Reputation tag category

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Tag Categories** tab.
3. To create a new tag category, click **New**.

4. To edit an existing tag, select a tag from the table, and then click **Edit**, or right-click the selected tag entry, and then click **Edit**.

5. On the General area, complete the following information:

   - Name —a unique name that identifies the tag category.
   - Type — type of data that the tag category contains. Tag category types cannot be edited.

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

   - Description — a brief description (up to 255 characters) indicating how the tag category is to be used.

Note

You must activate a Reputation DV package on the SMS to use the **Reputation DV Score** tag category. Select **Profiles** > **ThreatDV Entries** to view your license details.

6. In the **Settings** area, enter the appropriate information for the type of tag category you selected.
7. Click **OK**.

Import tag categories

You can import up to 100 user-defined tag categories. The time it takes before you begin to see your imported entries appear on the SMS depends on a number of factors:

- The number of user entries being added.
- The number of user entries that already exist.
- The number of tags for each user entry.
- The congestion of the reputation processing queue.

Importing and updating entries is correlated to the number of entries and the number of tags. User entries that have more tags consume more time. We recommend the following as an import threshold:

- <= 500,000 entries can imported with up to 100 applied tags for every entry.
- 500,000 ~ 1,000,000 entries use (at most) 50 applied tags for every entry.
- 1,000,000 ~ 2,000,000 entries use at most 20 applied tags for every entry.

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Tag Categories** tab.

3. Click **Import**.
4. Enter the name of the file to import or browse to its location.
5. Click **Next** to upload the file.

Export all tag categories

Procedure

1. On the Profiles navigation pane, click **Reputation Database.**
2. Click the **Tag Categories** tab.
3. Click **Export**.
4. Enter the name of the file to save and browse to the area where you want to save the file.
5. Click **Save**.

Delete a Reputation tag category

Important

Deleting a Reputation Tag category or LIST tag category value from a LIST tag category results in removal of that tag category or LIST tag category value from any Reputation entry or Reputation filter that uses those items. Before deleting any of these items, create an SMS backup. See *Restore the SMS database on page 8-85*.

Procedure

1. Select **Profiles** > **Reputation Database**.
2. Click the **Tag Categories** tab.
3. Select a tag category from the inventory, and then click **Delete**.

ThreatDV entries

Threat DV is a subscription-based service that identifies and delivers suspect IP, DNS, and URL addresses to subscribers. The addresses are tagged with reputation, geographic, and other identifiers for ready and easy security policy creation and management.

Threat DV provides the addresses and tags multiple times a day in the same manner as the Digital Vaccine. You can choose to download addresses into the Reputation database automatically or manually.

The ThreatDV IP/DNS Reputation Feed pane provides a summary of the IP/DNS Reputation Feed, including:

- License status — License status indicator and information for managed devices.
- Automatic DV download — Enabled/disabled status.
- Manual DV download — Check for the latest package.
- Last DV installed — Date and time the last Digital Vaccine was installed.
- DV version — Version number of the Digital Vaccine.
- DV type — Type of Digital Vaccine.
- IPv4 — Number of entries with IPv4 addresses.
- IPv6 — Number of entries with IPv6 addresses.
- DNS — Number of entries with domain names.
- URL — Number of entries with web addresses.
- Total — Total of entries.

The Threat DV URL Reputation Feed pane provides similar information for the URL Reputation Feed.

Note

You must activate a Threat DV package to use the **Reputation DV Score** tag category. Select **Profiles** > **ThreatDV Entries** to view your license details.

Import a ThreatDV package

ThreatDV is a subscription-based service.

Procedure

1. In a Web browser, open https://tmc.tippingpoint.com/TMC/.
2. From the top menu, select **Releases** > **ThreatDV** > **SMS Full Reputation Feed** or **SMS URL Reputation Feed**.

   The page lists all packages that are available. If you have a current ThreatDV subscription, reputation packages are included in the list. The most recent version is at the top of the list.
3. In the Download File page, click the **Download** button.
4. Click **Save**. To avoid unexpected behavior on the SMS, do not change the name of this file.
5. Select **Profiles** > **Reputation Database** > **ThreatDV Entries**, and do one of the following:
   - To import the SMS Full Reputation Feed, click **Import** under Threat DV IP/DNS Reputation Feed.
   - To import the SMS URL Reputation Feed, click **Import** under Threat URL Reputation Feed.

Reset a ThreatDV

Important

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

Procedure

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

2. To reset the DV for IP/DNS entries, click **Reset DV** in the ThreatDV IP/DNS Reputation Feed pane at the top. To reset the DV for URL entries, click **Reset DV** in the ThreatDV URL Reputation Feed pane at the bottom.
3. Verify that you want to delete ALL Reputation DV entries in the Reputation Database, and then click **OK**.

User entries

The SMS supports an unlimited number of user-provided entries to the Reputation Database. Reputation entries represent IP addresses, domain names, or URLs that are known to be malicious or that are otherwise listed for specific handling by reputation filters. Address entries in the Reputation Database can be tagged or untagged. Untagged entries contain only an address and function as a user-defined list of sites to block. A CIDR counts as a single entry.

The time it takes before users begin to see their imported entries appear in the SMS interface depends on a number of factors:

- The number of user entries being added.
- The number of user entries that already exist.
- The congestion of the reputation processing queue.

In a typical scenario—a few hundred entries contained in the file import, less than 100K user entries already on the system, and an empty reputation processing queue—entries can begin to appear in the SMS interface in as little as a minute's time. However, processing time increases along with the number of user entries and the number of tasks staged in the processing queue, which could include profile distributions and full Reputation DV feeds. In fact, entries cannot be imported until previously existing tasks in the queue have been completed.

When an address is added to the database, you can associate one or more tag categories. For existing address entries, you can add or remove one or more associated tag categories. When you associate a tag category with an address, you must also specify one or more of the possible values for that tag

category. Reputation entries are used to create filters. See *Reputation filters on page 5-40*.

Import entries into the Reputation database

You can create a file that contains the information you want to add to the Reputation Database. For IP and DNS entries, the import file must be in comma-separated value (CSV) format with each line made up of one or more fields separated by commas.

The file can contain addresses only or addresses and one or more associated tags. For URL entries, the import file must be delimited by a pipe (|) instead of commas, and entries can be URLs only or URLs with one or more associated tags.

There is no limit to the number of entries you can add to the file that you import. When importing entries, the file should not contain any blank lines.

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

Procedure

1. Select **Profiles** > **Reputation Database**, and then click **User Entries**.
2. Click **Import**.
3. Specify the path of the file you would like to import, or click **Browse** and select the file
4. Click **Next** to upload the file.
5. On the Import Reputation Entries dialog, select the types of entries in the import file: **IPv4**, **IPv6**, **DNS names**, or **URLs**, and then click **Next**.
6. Specify the tags to use with the imported entries.
   - Import tags from file — Indicates that tags in the import file should be applied to imported entries.
   - Specify tags to apply to all imported entries — Select this option to display a screen from which you can choose the tags, and their values, to apply to imported entries.

- Import tags from file and specify tags to apply to all imported entries — Select this option to apply both tags from the import file and tags you select from the next screen to imported entries. Conflicts are handled according to the setting of the User-specified tags override tags from import file option.
- User-specified tags override tags from import file — This option is available only when the Import tags from file and specify tags to apply to all imported entries option is selected. This item specifies how to handle tags in the file and tags you specify on the next screen that have the same name. If this option is selected, tags you select on the next screen will take precedence over tags from the import file. If this option is not selected, tags from the file will take precedence over tags you specify on the next screen.

7. Click **Next**.
8. Review the summary information about the import, and click **Finish**.

Adding user-provided entries to the Reputation database

You can manually add address and URL entries in the Reputation database. When you add entries, you have the option to add addresses and URL entries only or add addresses and URL entries with tag categories and values. A CIDR counts as a single entry. Entries with tags provide more options for tracking and blocking suspicious traffic. See *Reputation filters on page 5-40*.

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

Procedure

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Entries**.
2. Click **Add**.
3. Select the type of address and enter the corresponding information:
   - IP Address

- DNS Domain For DNS, you can select **Exact Match** for the domain name
- URLs

4. Click **OK**.

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

Procedure

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Entries**.
2. Click **Add**.
3. Add Address information. Select the type of address and enter the corresponding information:
   - IP Address
   - DNS Domain. For DNS, you can select **Exact Match** for the domain name
   - URL
4. Add one or more tags with specific value. For each tag:
   a. Select the tag.
   b. Add the value for selected tag.
5. Click **OK**.

Exporting user-provided Reputation entries

You can export user-provided Reputation entries to a file. For IP and DNS entries, the file must be in comma-separated value (CSV) format with each line made up of one or more fields separated by commas. For URL entries, the file must be delimited by a pipe (|) instead of commas. You can export

entries to capture the state of the Reputation database and then quickly restore it at a later time.

Export a user-provided entry from the Reputation Database

Procedure

1. On the Profiles navigation pane, expand **Reputation Database**, and then click **User Entries**.
2. Click **Export**.
3. Click **Browse** to select the location where the file will be exported to.
4. Click **Next** and then select the type of entry to export:
   - IPv4
   - IPv6
   - DNS names
   - URL
5. Click **Finish**.

Automatically remove user-provided entries

You can configure the SMS to automatically remove Reputation entries for each Indicator of Compromise (IOC) type: IP addresses, domain names, or URLs.

Procedure

1. Select **Profiles** > **Reputation Database** > **User Entries** > **Add**.
2. Select one of the following:
   - IP Address
   - DNS Domain

- URL

3. Select the **Reputation Entries TTL** checkbox, and then click the calendar icon to select a date and time in which the SMS will automatically remove any revoked or out-of-date entries.

Note

Expired Reputation entries are deleted on the SMS and device. Use caution when you set the time to live (TTL) date on an entry as it might be associated with an action set in a filter package that is used to protect your network.

4. Click **OK**.

Edit database synchronization

Edit the frequency that the SMS polls the User-Defined URL Entries for new or updated entries. Depending on the database polling rate and how many entry updates have been made, shorter intervals can result in continuous distributions and clogged queues.

Longer intervals avoid clogged queues but extend the time before any updates to the database are automatically synced to the device. However, you can still perform a Full Sync to bypass the automatic distribution so that devices receive the updated URL entries immediately.

Procedure

1. Select **Profiles** > **Reputation Database** > **User Entries**.
2. Click **Edit** under User Entry Distribution Settings.
3. Specify the interval (in minutes) between SMS distributions of the User-Defined URL Entries to managed devices. A value of a minimum of 1 minute and a maximum value of 1440 minutes (1 day) is required. The default is 10 minutes.
4. Click **OK**.

Geographic entries

For information on import information and Lookup services for the Geo Locator database, see *Geo Locator Database on page 8-137*.

Reputation database search

The Search Entries screen provides a convenient area to search for entries in the Reputation Database using user-defined filter criteria to build a search query. The search criteria are specified by including tag categories and values for the various tag categories. By default, all tag categories known to the SMS are displayed as columns in the result table.

Search criteria

When building a search query, you can use the following criteria:

- Entry criteria — Search criteria based on the type of address entry in the Reputation database.
- Tag criteria — Search criteria based on the tags in the Reputation database. This area lists the available tag categories in the Reputation database that can be included in the search.

Criteria	Description
IP Address	Select this option if the entry represents an IP address or block of IP addresses. The specified address may be either IPv4 or IPv6. If the value represents a block of IP addresses, the value should end with a "/" followed by a prefix length.
DNS Domain	Select this option if the entry represents a DNS name. If this option is selected, DNS lookup requests for the specified entry are dropped by the IPS.

Criteria	Description
URL	Select this option if the entry represents a URL. The URL must be less than 4K in length. A single wildcard string * (backslash and asterisk) is supported. URL categories, such as Travel, are not supported. **Note** Selecting this option searches for *user-defined* URL entries only. To look up entries and scores in the ThreatDV URL Reputation Feed, select **ThreatDV URL Lookup** in the navigation pane.
Include Untagged Entries	Includes addresses that do not have tags associated with them.
Include Tagged Entries	Includes addresses that have tags associated with them.
Include Rep DV Entries	Includes Reputation Digital Vaccine entries, an optional subscription-based service. These entries are displayed in a separate column on the search results table.
Include User Entries	Includes user entries. These entries are displayed in a separate column on the search results table.
Include Geographic	Includes Geographic information based on a computer's IP address/ hostname within a geographic region or country. These entries are displayed in the Address and Geo Filter Country columns on the search results table.

See *Tag Categories on page 5-84*.

Search results

The Search table lists the results of your customized search. User-Created Reputation entries can be included in a Reputation or a Geographic filter. When you add a new entry to the Reputation Database, the listing is automatically added to the results table.

Search for entries in the Reputation database

Procedure

1. Review the information in *Search criteria on page 5-98*.
2. On the Profiles navigation pane, expand **Reputation Database**, and then click **Search**.
3. For Entry Criteria to include in the search, select from the following and enter the associated entry:
   - IP Address — An IP address or block of IP addresses
   - DNS Domain — A DNS name. To search for an exact DNS match, select the **Exact Match** check box
   - URL — Any URL less than 4K in length
4. For **Tag Criteria** to include in the search, use the check box next to the name of the tag category to include it in the search criteria. Use the expanded view to add specific tag search criteria.
5. Select one or more tag categories to include in the search.

   When you select a tag, the default criteria is "Tag is present and has a value."
6. To select other criteria, expand the entry and select desired criteria. See *Reputation database interface on page 5-81*.
7. Click **Search**.

   The results display in the results table in the bottom of the screen.

Edit bulk (all searched database entries)

Procedure

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database on page 5-100*.

2. Click **Edit Bulk** to change all the user-provided entries that match the current search criteria.
3. The Edit Reputation Entry dialog displays.

   The Query Expression indicates the current search criteria used for the screened entries.
4. You can add or remove one or more tags to the entries.
   - To remove a tag, deselect the category.
   - To add a tag, select the tag category and add a specific value.
5. To create a new tag category, click **Add Tag Category**.
6. To change or modify values for an existing tag, click **Different Values** next to the name of the tag and enter the new value.

Important

When you select Edit Bulk, all user provided entries that match the current search criteria are edited. The operation can NOT be undone

7. Click **OK**.

Delete bulk (all searched database entries)

Procedure

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database on page 5-100*.
2. Click **Delete Bulk** to delete all the user-provided entries that match the current search criteria

Important

When you select Delete Bulk, all user provided entries that match the current search criteria are deleted. The operation can NOT be undone.

3. To confirm that you want to delete all matching user-provided entries, click **Yes** in the **Delete All User Reputation Entries** dialog.

Edit a user provided entry in the Reputation database

Note

The Address, URL, and DNS Domain fields cannot be edited.

Procedure

1. Search the database using the appropriate criteria to find desired user provided entries. See *Search for entries in the Reputation database on page 5-100*.
2. Select an entry from the table and click **Edit**.

   The Edit Reputation Entry dialog displays.
3. You can add or remove one or more tags to the entries.
   - To remove a tag, deselect the category.
   - To add a tag, select the tag category and add a specific value.
4. To create a new tag category, click **Add Tag Category**.
5. Click **OK**.

Edit multiple user-provided entries in the Reputation database

Procedure

1. Search the database using the appropriate criteria to find desired user-provided entries. See *Search for entries in the Reputation database on page 5-100*.
2. To select multiple entries, do one of the following:
   - Hold down the **SHIFT** key, and then select desired range of user-provided entries.

- Hold down the **CTRL** key, and then select specific user-provided entries.

3. Select one or more listings from the Reputation Entries area.
4. You can add or remove one or more tags to the entries.
   - To remove a tag, deselect the category.
   - To add a tag, select the tag category and add a specific value.
5. To create a new tag category, click **Add Tag Category**.
6. Click **OK**.

ThreatDV URL Lookup

From the **Reputation Database > ThreatDV URL Lookup** page, you can query the ThreatDV URL Reputation Feed to see if a specific URL is in the database.

After you specify the URL that you want to look up and click **Search**, the results table lists any matching entry in the database along with its Reputation score.

Because ThreatDV does not support wildcards, a wildcard string (*) cannot be used as a query string. For example, the following use of the wildcard string is not permitted:

```
http://mywebsite.com/path/to/resource?\*
```

View open threat intelligence - STIX/TAXII data

The SMS exchanges cyber threat intelligence using the Trusted Automated Exchange of Intelligence (TAXII) application layer protocol. The information is exchanged in a serialization format using the Structured Threat Information Expression (STIX) language. The integration of STIX/TAXII feeds with the SMS enables you to easily identify threats so that you can keep your existing security controls updated.

Prerequisites

- Threat Protection System (TPS) running TOS v5.0 or later
- *Web security certificate on page 8-7*
- *TAXII client used to send STIX data to the SMS on page 5-106*

Note

Some third-party TAXII clients may require an appropriate certificate for verification. Anomali STAXX, a tool to collect and share STIX/TAXII feeds, is used as an example. STAXX requires 4 Gb RAM, 2 processors, and 100 Gb storage. For more information, see https://www.anomali.com/community/staxx.

Import rules

This section describes the rules you must follow when importing STIX data to the Reputation database.

- To automatically send STIX data to the SMS, enable the TAXII service. The TAXII service is enabled by default. For more information, see *Enable SMS services on page 8-88*.
- Only STIX Indicator objects can be added to the Reputation database.
- STIX Indicator objects must only contain a single comparison expression.
- You cannot export STIX objects from the SMS.

Tag categories

The SMS automatically includes the following predefined tag categories for STIX/TAXII data. Use the following table to map STIX objects with user-provided Reputation tag categories. Observable objects display as Reputation entries on the SMS. You can use these entries to create a Reputation filter to protect your environment.

Reputation tag	STIX object property	Description
STIX - ID	id	ID of the STIX **Indicator** object, which is the only STIX 2.0 Domain Object the SMS imports. Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity. For example, an indicator may be used to represent a set of malicious IP addresses, domains, or URLs. To be imported to the Reputation database, an indicator STIX object must: • Only contain a single comparison expression. • Object path pattern must be domain, URL, IPv4, or IPv6.
STIX - Severity	labels	Identifies the severity for the discovered threat, based on rules that match severity. Severity is not standard property for STIX 2.0.
STIX - Confidence	labels	Identifies the confidence for the discovered threat, based on rules that match a confidence score. Confidence is not standard property for STIX 2.0.
Reputation Entries TTL	valid_until	Identifies the date SMS will remove the entry.
-	revoked	If revoked is `true`, the SMS deletes the entry tagged with the same STIX-ID.

Install a TAXII client

Before you begin

You must have a public key for the SMS (smscert.pem) before you can install the certificate in the TAXII client.

Procedure

1. Install Anomali STAXX. When installation is complete, access the console from the Virtual Machine (VM), and do the following:
   a. Enter a new Anomali password for sudo escalation.
   b. Enter the following command to enable SSH access, which allows you to access the instance remotely:

```
systemctl start sshd.service
```

> **Note**
> Some third-party TAXII clients may require an appropriate certificate for verification. Anomali STAXX, a tool to collect and share STIX/TAXII feeds, is used as an example.

2. (Optional) Enter the following commands to enable NTP:

```
sudo systemctl enable ntpd
systemctl start ntpd
```

3. (Optional) Set a static IP address.
   a. To discover the current IP address, enter the following command:

```
ifconfig
```

   b. To discover the interface/adapter name, enter the following command:

```
sudo vi /etc/sysconfig/network-scripts/<interface name>
```

a. Once open, scroll down and modify `BOOTPROTO= static`.

b. Add the following:

```
IPADDR= <host IP address>
NETMASK= <subnet mask>
GATEWAY= <default gateway>
NS1= <DNS record>
NS2= <secondary DNS server>
```

c. To exit the editor, click **ESC** followed by `wq!`.

4. Upload the public key to STAXX. The following example uses the Secure Copy (scp) command-line tool. You can also use SFTP from the command line or client.

a. Locate the directory that has the public key.

b. Enter the following command to transfer the file:

```
scp smscert.pem root@ip_staxx_server:/usr/share/pki/ca-trust/anchors
```

c. After you upload the file, enter the following command:

```
update-ca-trust
```

5. (Optional) Add the **certificate common name** to the `/etc/hosts` on the STAXX server. This is required if the SMS DNS entry does not match the certificate common name.

a. From the VM console (or the SSH instance), connect as the Anomali user.

b. Enter the following command:

```
sudo vi /etc/hosts
```

c. Press **i** to enter insert mode.

d. Add the corresponding IP address of the SMS server, and then map it to the common name of the created web certificate.

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.49.24   TrendMicroTippingPoint
192.168.49.25   Tippingpoint
[root@anomali-staxx anchors]#
```

6. Access the Anomali web console at `https://staxx_ip_address:8080`, and then do the following:

   a. Click the **Gear** to open the Settings page.

   b. Click **Add Site**.

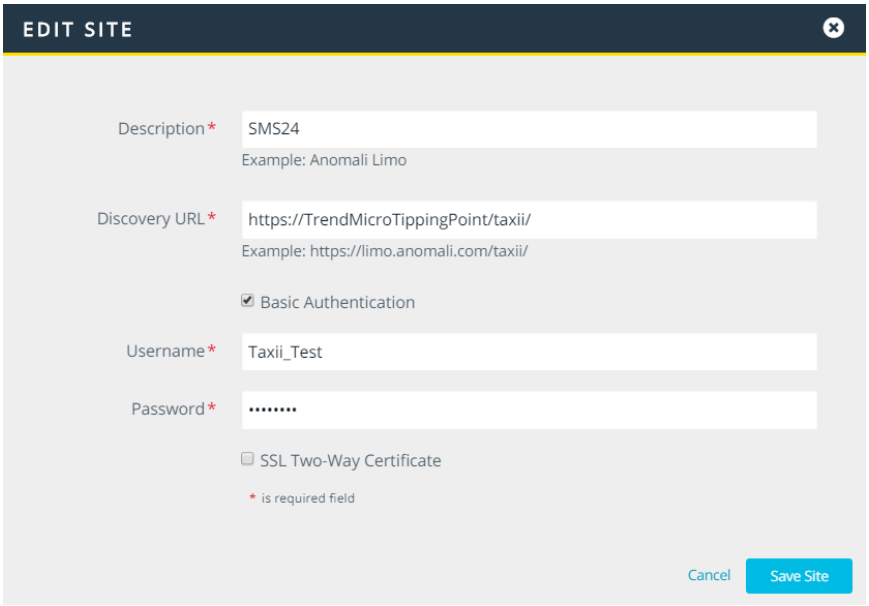
   c. Enter a **Description**.

   d. Use the common name of the web certificate and the path of `/taxii/` for the **Discovery URL**. For example, `https://TrendMicroTippingPoint/taxii/`.

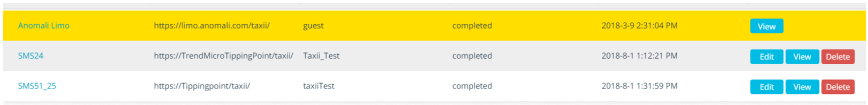
7. Select **Basic Authentication**.

8. Enter a user which has permissions to access SMS Web Services, and note the following:

   - You can use any account that has the default superuser role.
   - You can create a new SMS user that has limited rights, but includes the ability to access SMS user rights.



9. Test and verify that you have a successful connection.

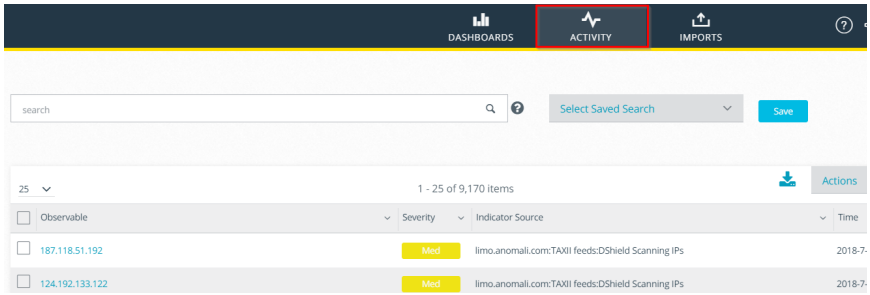


Push observable objects from the TAXII client to the SMS

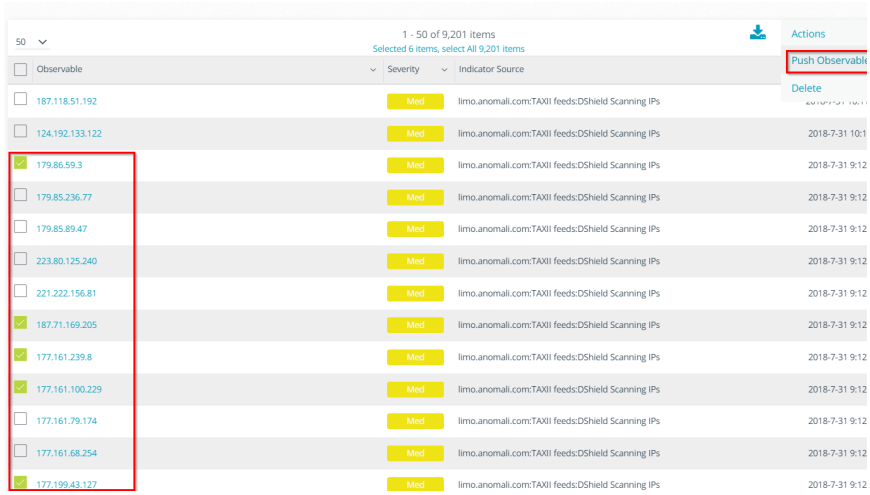
Push observable objects from the TAXII client to the SMS. Anomali STAXX is used as an example below.

Procedure

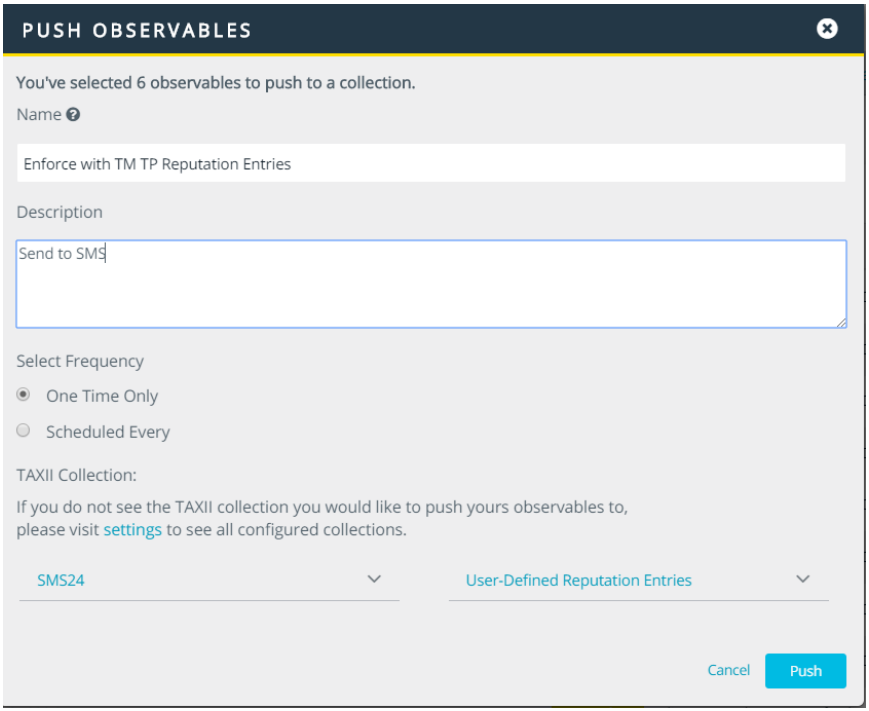
1. Click **Activity**.



2. Select the observable URL or IP address.
3. Select **Actions** > **Push Observable**.



4. Click **Push**.



Vulnerability Scans (eVR)

Enterprise Vulnerability Remediation (eVR) enhances visibility into your network by allowing you to pull in data from third-party vulnerability management vendors, match publicly known Common Vulnerabilities and Exposures (CVEs) to DV filters, and take immediate action on your security policy by tuning your IPS enforcement security policy to protect against the known vulnerabilities in your network, all within the SMS.

Custom converters are available for Qualys®, Rapid7 Nexpose®, and Tenable™ Nessus®.

Note

When you perform a backup restore on the SMS, if the backup version does not match the current SMS version, the vulnerability scan (eVR) converters are not restored. The vulnerability scan (eVR) converters are only restored during a backup if the backup version and the current version of the SMS are the same.

When you delete a vulnerability scan, you delete all data including CVEs, matching DV filters, and assets, such as the host IP addresses and the asset groups

Enable sharing CVE coverage gaps with the TMC

Select **Edit** > **Preferences** > **TMC Information Share** > **Enable sharing CVE coverage gaps to help TippingPoint improve DV coverage** to enable the SMS to send CVE IDs that are included within a scan file but are not yet identified within a DV filter to the TMC. Learn more: *TMC information share on page 11-4*.

Import vulnerability scans

Import a vulnerability scan. After you pull in the vulnerability information, you can add comments and show CVEs for a selected vulnerability scan. You cannot import a file that has a non-ASCII filename.

Procedure

1. Run a vulnerability assessment report (vulnerability scan) using supported vulnerability management products from Qualys, Rapid7, and Tenable.
2. Export the result of the vulnerability scan to a supported file format for use on the SMS.
3. Select **Profiles** > **Vulnerability Scans (eVR)**.
4. Click **Import**.

5. Click **Browse** and select a vulnerability scan.
6. Depending on the vulnerability management tool used to run the scan, select the appropriate converter:
   - Select **Native** if the vulnerability scan is an SMS-Standard CSV file.
   - Select **Custom**, and select the respective vulnerability management product: **Qualys-CSV**, **Nessus**, or **Nexpose**.

   To successfully import or convert a vulnerability scan, review the *eVR scan specifications on page 5-113*.

   The Converter Properties displays the converter version, the export format of the vulnerability scan (for example, CSV or XML), and the name of the vulnerability management vendor.
7. (Optional) Enter comments about when the scan was imported.
8. Click **OK**.

   The SMS converts the file and imports the data from the vulnerability scan. The SMS also displays the conversion results and the number of import errors. You can download the **Conversion Information File**. If the SMS detected any errors while converting or importing the vulnerability scan, you can download the **Conversion Error File**.
9. Click **OK**.

Note

You can also import vulnerability scan data using the Vulnerability Scans (eVR) API. For more information, see the *SMS Web API Guide* on the Online Help Center.

eVR scan specifications

Vulnerability scans must be in a native, comma-separated value (CSV) format before they can be used on the SMS. If you use a supported vulnerability management product from Qualys, Rapid7, or Tenable, the SMS can automatically convert those vulnerability scan results into native format.

CSV file specifications

Note the following CSV file specifications (and sequence) before you import a vulnerability scan:

- The first line in the CSV file must be the column headers for each of the columns.
- Each row after the header must contain the same number of columns that are in the header.
- Each column must be delimited with a comma.
- The value within each column must be wrapped in double quotes; however, embedded double quotes are not permitted ("This is "invalid" data").
- Each row in a CSV file must be less than 65536 bytes.

Vulnerability scan specifications

The minimum data required for a vulnerability scan is:

- **IP Address** - (host IP addresses) The maximum number of host IP address and vulnerability combinations that you can import on the SMS is 10 million. When the SMS reaches the maximum limit, it displays an error message, and you must delete vulnerability scans before you can *import a new scan on page 5-112*.
- **CVE IDs** - CVE must be in the format CVE-YYYY-NNNN where YYYY is a 4 digit year and NNNN is a sequence number.
- **Severity** - Vulnerabilities are assigned severity levels to define the urgency associated with remediating each vulnerability. Rankings are based on a variety of industry standards including CVE.

Comment on a vulnerability scan

You can comment on a vulnerability scan. For example, you can add notes about when a scan was imported, or you can track all remediation changes in subsequent scans.

You can also *comment on a CVE on page 5-119*.

Procedure

1. Select **Profiles** > **Vulnerability Scans (eVR)**.
2. Select a vulnerability scan, and click **Comments**.
3. Enter **Comments**.
4. Click **OK**.

Show CVEs for a selected vulnerability scan

After you import a vulnerability scan, you can view the CVEs.

1. Select **Profiles** > **Vulnerability Scans (eVR)**.
2. Select a vulnerability scan, and click **Show CVEs** to view the *CVE Search Results on page 5-117*.

Search vulnerability scans for CVEs

Search for CVEs imported on the SMS vulnerability scan database. You can review the vulnerabilities identified in your network, sorted by CVE, and which assets are impacted by these vulnerabilities.

Procedure

1. Select **Profiles** > **Vulnerability Scans (eVR)** > **CVE Search**.
2. Click **Scan Criteria** to search for:

SELECT THIS CRITERIA:	TO SEARCH FOR ...
Scans	• Select **All** to perform a global search through all imported vulnerability scans. • Select the check box next to the vulnerability scan for a specific file.
Scan Vendor	• Select **Any** to search for a supported vendor.

SELECT THIS CRITERIA:	TO SEARCH FOR ...
Scan Time	Start and end dates for when the vulnerability scan was generated. Start time: • Select **Start Time** to enter a date in MM/DD/YY HH:MM format. • Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**. End time: • Select **End Time** to enter a date in MM/DD/YY HH:MM format. • Select **End Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.
Import Time	Start and end dates for when the vulnerability scan was imported on the SMS. Start time: • Select **Start Time** to enter a date in MM/DD/YY HH:MM format. • Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**. End time: • Select **End Time** to enter a date in MM/DD/YY HH:MM format. • Select **End Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.

3. Click **CVE Criteria** to search for:

SELECT THIS CRITERIA:	TO SEARCH FOR ...
CVE Details	• Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE).

Select this criteria:	To search for ...
Discovered Time	Start and end dates for when the CVE vulnerability was discovered. Start time: • Select **Start Time** to enter a date in MM/DD/YY HH:MM format. • Select **Start Time**, click the calendar icon to select a date/time from the calendar, and click **OK**. End time: • Select **End Time** to enter a date in MM/DD/YY HH:MM format. • Select **End Time**, click the calendar icon to select a date/time from the calendar, and click **OK**.
Assets	• One or more IP addresses for an asset. An asset is the network IP address of the host vulnerable to the CVE identified in the vulnerability scan.
Flagged Status	• **Flagged** - All CVEs that are flagged for follow-up. • **Not Flagged** - All CVEs that are not flagged.

4. Click **Search**.

View CVE search results

The CVE Search Results displays the following information:

Column	Description
CVE	Unique tracking number used to identify Common Vulnerabilities and Exposures (CVE). CVEs are publicly known security vulnerabilities.

Column	Description
Filters	Unique name and number used to identify the *security filters on page 5-30* or *application filters on page 5-30* that are associated with a CVE. If there is more than one filter associated for a CVE, the SMS displays the number of filters in parentheses. Click the **+** symbol next to the CVE to view all of the filter names.
Not Protected Profiles	List of *profiles on page 5-12* on the SMS that are not currently protected from a CVE. If there is more than one profile that is not protected from a CVE, the SMS displays the number of profiles in parentheses. Click the **+** symbol next to the CVE to view all of the profiles that are not protected. **Note** Ignored profiles do not display in this list. See *View CVE details on page 5-119* to ignore or show profiles for the CVE.
Protected Profiles	List of *profiles on page 5-12* on the SMS that are currently protected from a CVE. If there is more than one profile that is protected from a CVE, the SMS displays the number of profiles in parentheses. Click the **+** symbol next to the CVE to view all of the protected profiles. **Note** Ignored profiles do not display in this list. See *View CVE details on page 5-119* to ignore or show profiles for the CVE.
Assets	Network assets discovered in a vulnerability scan. Assets include IP addresses of the host vulnerable to the CVE and the Asset Group. If there is more than one asset associated for a CVE, the SMS displays the number of assets in parentheses. Click the **+** symbol next to the CVE to view all of the assets.
Flagged	Indicates if the CVE has been flagged for follow-up.
Comments	User-provided comments for the CVE.

You can right-click on entries in the CVE search results and do the following:

- **Find/Filter** — Search for a filter using a keyword
- **Details** — View or edit CVE details
- **Set Flagged**— Quickly change the flagged status for one or more CVEs

View CVE details

A vulnerability scan captures vulnerability information in your network at a single point in time. After you import the scan on the SMS, you can view CVE details for every CVE identified within the vulnerability scan.

Procedure

1. Select **Profiles** > **Vulnerability Scans (eVR)** > **CVE Search**.
2. Select a CVE from the *CVE Search Results on page 5-117* and click **Details**. Alternatively, you can double-click a CVE in the CVE Search Results.
3. Click **Details** to:
   - Access the **URL** link to the CVE database.
   - **Flag** the CVE for follow-up. You can quickly *search for flagged CVEs on page 5-115* on the SMS.
   - Add or edit comments for the CVE. You can also add *comments to the vulnerability scan on page 5-114*.
4. Click **Ignored Profiles** to view a list of profiles, and do the following:
   - Select a profile, and click **Ignore** to hide the profile from the list of **Not Protected Profiles** and **Protected Profiles**. See *View CVE search results on page 5-117*.
   - Select a profile, and click **Show** to display the profile on the list of **Not Protected Profiles** and **Protected Profiles**. See *View CVE search results on page 5-117*.
5. Click **Filters** to view a list of active DV filters that correlate with the CVE.

6. Click **Assets** to view a list of network assets, such as the host IP addresses and the asset groups vulnerable to the CVE, as identified in the vulnerability scan.
7. Click **OK**.

Profile tuning

Profile tuning enables you make the right decision on how to remediate a vulnerability. Remediation might involve updating an asset, scheduling a change window to execute a patch, or turning the Digital Vaccine filter on in absence of an update from the software vendor.

Procedure

1. Select **Profiles** > **Vulnerability Scans (eVR)** > **Profile Tuning**.

   The SMS displays a list of available profiles including the version and the dates the profile was last modified and distributed.

2. Select a profile, and click **Next**.

   The SMS correlates the CVEs provided through a scan to the CVEs of DV filters, and lists all filters that are currently Not Protected and Permit Traffic.

Column	Description
Name	Unique name and number used to identify a filter.
Action Set	Current action set assigned to a filter and are set to disabled by default.
Category	Every DV filter is assigned to a category and cannot be changed.
Source	All CVEs that match a filter.
Severity	Severity level assigned to a filter, which helps you prioritize the vulnerabilities found.

3. Review the list of **Not Protected/Permitting Filters**.

   To remediate these vulnerabilities, you should apply a blocking action set (Block, Block + Notify, or Block + Notify + Trace) to every filter.

However, in some cases, you may need to override the recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network. After a filter is customized, it is not affected by the global category settings that specify the filter State and Action.

- To use the recommended policy: Select one or more filters, select a blocking action set from the **Change these filters to** drop-down list, and click **Apply to Selected**.
- To override the recommended policy: Select a filter, and select an action set from the **Pending Action Set** drop-down list.

  If you ignore an action set for a filter, select **Show Ignored Filters** to show or hide these filters.

Click **Next**.

The SMS lists all of the CVEs that are included in a vulnerability scan, but that do not match the CVEs of a DV filter.

4. Review the list of **Vulnerabilities with no Protection**, and do one of the following:

   - Enter comments for the selected CVE.
   - View CVE Details.

   Click **Next**.

   The SMS lists all of the modified filters including the pending action set changes.

5. Review the list of **Modified Filters**, and do one of the following:

   - Enter the same comments for all of the modified filters within the profile.
   - Click **Launch distribution wizard when finished** to immediately distribute the profile.
   - Click **Finish** to save the updates to your security policy without distributing the profile.

Chapter 6

Events

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

- Create, run, and save queries regarding events against the alert logs of the TippingPoint system. The SMS provides export functionality to save the results to a comma- or tab-delimited file.
- View event details, such as the contents of packets that comprised that event and information identifying where the event originated from including the geographic location.
- Export event data to an external file and generate reports. This aids with diagnostics, and you can export event data to an external file and generate event reports.

Note

When SuperUser or Admin User access or authority is specified, the user must have the respective SuperUser or Admin capabilities. See *Authentication and authorization on page 8-15*. Users have access to events if they have access to either the device or the segment group.

Inspection events

The SMS includes different types of Inspection events: Quarantine, Rate Limit, and Reputation events, which also includes the geographic location information for an IP address. The following table describes the columns in the Inspection Events table. By default, events are shown for the last 15 minutes. As traffic moves through your network, new events appear at the top. The initial view of certain segment and device tables are empty and have the option to customize the table listing by adding list items using the Add option. You can also use the table to define the order, visibility, sorting, and aggregation properties of each column.

Note

By default, DNS data does not display in the events table. To configure the IP Identifier and enable the DNS lookup service, see *IP address identifier on page 8-129*.

Column	Description
Time	Date and time that the event was processed by the inspection. **Note** The time displayed in the Time column for events reflects the time of the actual event on the detection device. This might not correspond to the SMS Receipt Time or the Device Log Time reported in the Event Details dialog. The differences might depend on the timekeeping configuration of the systems and on the speed of the network.
Severity	Indicates the importance of the event.
Name	Name of the filter that generated the alert or block.
Category	Type of event filter.
Action	Type of action for the filter.
Hit Count	Number of times there was a filter match.

Column	Description
Profile	Profile associated with the alert or block.
Device	Name of the device responding to the traffic.
Segment/Rule	Segment for inspection events.
Src. Addr.	Source IP address of the traffic that caused the event. Expand this column for location details, including geography map, region, city, and named resource.
Src. Port	Port of the source IP address.
Src. User	Login name of the source user.
Client Addr.	The IP address of the attacking client. Expand this column for location details, including geography map, region, city, and named resource.
Dst. Addr.	Destination IP address of the system at which the event was targeted. Expand this column for location details, including geography map, region, city, and named resource.
Dst. Port	Port of the destination IP address.
Dst. User	Login name of the destination user.
Seg	Number of the segment.
VLAN	VLAN on which the event took place.
Trace	Indicates if the event has a packet trace (or saved portion of the packet used in the event).
SSL Inspect	Indicates whether the event was part of an SSL session.
HTTP Hostname	Indicates whether there is an HTTP URI associated with the event and identifies the hostname. URI information displays in the Permit, Block, Rate Limit, and Trust logs.
Comment	Information added by the user.

Search for Inspection events

Use criteria to search for Inspection events.

Procedure

1. Select **Events** > **Inspection Events**, and then click the arrow next to Inspection Events to search by the following criteria: filter, filter taxonomy, network, user info, device, segment, rule, or events.
2. Select the following **Filter Criteria**.

SELECT:	TO ...
Filter Details	Search for filter name or filter number.
Filter Category	Select filter categories. Expand a listing to select individual entries, or select a top-level list item to include every item listed under it.
Profile	Select a profile.
Filter Severity	Select the severity level or importance of the event. • **Red/Critical** — Indicates critical events that must be looked at immediately. • **Yellow/Major** — Indicates major events that must be looked at soon as possible. • **Cyan/Minor** — Indicates minor events that should be looked at as time permits. • **Gray/Low** — Indicates traffic that is probably normal, but may have security implications.  **Note** For corresponding SANS terminology, “Major” equates to “High” and “Minor” equates to “Moderate”.
Filter Type	Search for events by security or application filters.

Select:	To ...
Reputation Type	Search for events by the following Reputation types: • All • Both Reputation and geographic • Reputation only • Geographic only • Non-Reputation
Action	Select an action including permit, block, trust, rate limit, or quarantine.
Suspicious URL Metadata	Include or exclude events with suspicious URL metadata.

3. Select the following **Filter Taxonomy Criteria** based on the classification, protocol, and platform. To select a consecutive range of entries, press the **SHIFT** key. To select multiples entries, press the **CTRL** key.

Select:	To ...
Classification	Select filter classification.
Protocol	Select a protocol.
Platform	Select a platform.

4. Select the following **Network Criteria**.

SELECT:	TO ...
Addresses and Ports	Search based on single, multiple, or ranges of source and destination IP addresses or ports. For source or destination IP addresses: • Enter multiple IP address separated by commas. • Enter a range using a dash (-). • Enter one address or a CIDR block. • Exclude IP addresses in a CIDR block by using the "!" symbol. Enter both types of parameters for ports. For example, to display events that had a source port of 22,25, or between 1000 and 32000, enter "22,25,1000-32000".
Packet Trace	Locate action sets with packet trace enabled: • All • Events with Packet Trace • Events without Packet Trace
VLAN	Search based on the VLAN ID.
Additional Event Information	Use the client IP address for the source address if available or to search for an HTTP hostname.

5. Select from the following **User Info Criteria**.

SELECT:	TO ...
Users	Include or exclude users based on login names or user groups. If no users are specified, **Any** is the default. Click **+** to add a user. Click **-** to remove a user.
Domains	Specifies the source and destination IP address of the user domains.
Machines	Specifies the source and destination IP address of the user machines.

6. Select from the following **Device, Segment, Rule Criteria**.

Select:	To ...
Segment/ group	Group of hosts protected through a licensed pair of ports on a device. You can select and add everything within a group, or you can select multiple options within each grouping. Click **Add** to add a segment, group, device, or stack.
Device/ group/stack	Devices managed by the SMS.

7. Select from the following **Event Criteria**.

Select:	To ...
Has comment/ Comment	Locate events based on whether it has a comment. • All • Events with comments • Events without comments
Event Number	Search by event number.

8. Enter the number of matching rows (1 – 10,000) to list in the Events table. Limiting the number of row may decrease the query processing time.

9. Select a time range from the following:

   - **Real-time** — Displays entries as they occur on the SMS. This option displays data by refreshing the screen. It calculates the refresh rate based on the time it takes to run the query and display the results.
   - **By set amount** — Displays entries according to a selected time: Last minute, last five minutes, last hour, last 24 hours, and so on. By default, events are shown for the last 15 minutes.
   - **By time range** — Displays entries during a range of time you select. Type in the field, or click the calendar to select a date.

10. Click **Refresh** to update query results.

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

11. To save this query, click **Save As**, enter a name, and click **Save**.

Right-click options from the events table

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

Option	Description
Export to File	Exports selected rows or all rows to a delimited text file.
Find & Filter	Find a term or search for a filter.
Details	View event details.
Event Comment	Adds annotation to event listing. To edit a comment, do one of the following: • Select one or multiple rows, right-click and select **Event Comment**. • Double-click the row with the comment you want to edit, and click **Edit** next to the Comment area of the Event Details dialog. **Note** If you select multiple rows that do not have the same comment, any new comment you enter replaces the previous comment for all of the selected rows.
Search on	Allows you to search all results based on the column heading for the selected event. For example, you can search for all events with the same Source Address as the selected event.
ThreatLinQ	Displays globally aggregated information about filters, source IP addresses, and source/destination ports.

Option	Description
Packet Trace	Provides the following Packet Trace options: • View • Save • Download to the SMS • Configure View Settings
IP Addr ID Config	Allows you to configure the ID for the IP address or edit the IP address by opening the New/Edit IP Addr ID Entry window.
Reputation	Create any number of reputation entries based on the source or destination address.
New Traffic Capture	Create a new traffic capture for a segment on the device.
Reports	Provides the following report options: • Specific Filter Report • Specific Source Report • Specific Destination Report • Specific User Report • Specific Peer Report (Src. Addr.) • Specific Peer Report (Dst. Addr.)
Profile	Allows you to edit filters, create exceptions, or create a Traffic Management filter.

Option	Description
IP Lookup	• Geo Locator • Named Resource • DNS • User ID • Who is • Reputation • End Point Attributes • Multiple Lookups
Create Response	Create a manual response based on Source Address, Source NAT, Destination Source, and Destination NAT.
Query IDResolver	Provides access to IP address information for A10 Networks.
Create Named Source	Create a named source based on Source Address, Source NAT, Destination Source, and Destination NAT.
Table Properties	Allows you to define the order, visibility, sorting, and aggregation properties of each column in your table.

Export Inspection event results

Export Inspection event results to a comma- or tab-delimited file.

Procedure

1. Select **Events** > **Inspection Events**.
2. Search for Inspection events.
3. Select a time frame. You cannot export **Real-Time** results.
4. Click **Export Results** and browse to and select a location.
5. Enter a file name.
6. Select a **Files of Type** from the drop-down menu.

7. Click **Save**.

Open or edit a saved query

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

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

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

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

Procedure

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

View event details

Procedure

1. In the Events table, locate an event.

2. Do one of the following:
   - Double-click the event row.
   - Select the event row, right-click, and select **Details**.
3. The Events - Event Details dialog opens. From this dialog you can:
   - Edit an event comment.
   - Edit the associated filter or rule.
   - View packet trace information, where available.
   - Copy event details to your clipboard, to be pasted into other applications.
   - View details for the previous or next event in the list.
4. To close this dialog, click **Close**.

View event details

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

Event section: information about the event

- **Event No.**- The order in which the event appeared in the SMS.
- **Hit Count** - The number of packets aggregated before notification was sent. Click **Packet Trace** at the bottom of the screen to view more information about the packets involved in the event. The **Packet Trace** button is disabled when packet trace information is not available. See *View the packet trace on page 6-22*.
- **Event Time** - The time on the device that the traffic was first encountered.
- **Action** - The flow control action associated with the event filter that matched the event.
- **Severity** - The importance of the event.

- **Event Msg** - The message for the event.
- **Comment** - User-generated text added to the event.

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

- Rule - The rule that triggered the event
- Device - The device that responded to the traffic
- Interface In and Out

Note

Device information is based on whether it is an IPS generated inspection event, and may not display the information listed above.

Segment/device section: information about the segment and/or device that triggered the event

- Segment
- Segment Port In
- Device
- VLAN

Network: information about the source and destination of the event

This section provides the Source Address and Port, and the Destination Address and Port of the event. If the additional event information option has been selected, the client IP address also appears in addition to the geographic location for the IP address including the country and flag icon (if available), region, and city.

If both an X-Forwarded-For value and a True-Client-IP value are available, and they differ from each other, the Client IP field reflects the X-Forwarded-For value.

Filter info

- Filter Name - The name of the filter that triggered the event. If the filter is editable, the Edit Filter button will allow you to easily modify the filter.
- Description - Description of the filter
- Class - Class of the event/filter
- Category - Type of event filter
- Profile - Profile associated with the alert or block
- Protocol - Protocol the filter monitors
- Platform - Platform the filter applies to
- CVE ID - The CVE ID (if available) of the event trigger. The CVE is a dictionary of publicly known information security vulnerabilities and exposures.
- Function
- Globally Collected Filter Info (via ThreatLinQ) - Helps you to understand the global impact of the issue. See *TMC ThreatLinQ charts and graphs on page 6-17* for more information.

Additional event information

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

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

- URI

URL/URI information

A URL Information panel appears only when an HTTP URI value is displayed in the Additional Event Information panel. If a valid URL is established, this panel displays a table that dissects the URL according to its components. If a valid URL cannot be constructed from the URI string, the SMS attempts to construct a URI, which, if successful, appears in a URI Information panel. If the attempt fails, the URI Information panel displays a message describing why the URI is malformed.

The device collects URI Metadata on a web request. If the corresponding web response triggers a filter, the log displays the URI Metadata only if the device successfully correlated the request with the response. In typical network scenarios, this normally occurs. However, in network scenarios where the response has a different VLAN, IP address/port, or protocol than the request, the device interprets the two flows as non-related and does not correlate the URI information. Without the URI Metadata in the log, the SMS cannot forward the URI information to the Deep Discovery Analyzer as part of URL Threat Analysis.

TippingPoint devices enforce a maximum length of 8 KB for URI strings. URI strings are transmitted over HTTP, which might or might not be encrypted (HTTPS) with Transport Layer Security (TLS) or Secure Socket Layer (SSL).

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

For example, the following unencoded data:

`/foo\bar.html`**`DEL`**`baz`

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

```
/foo\\bar.html\x7Fbaz
```

Filter information

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

Edit a geographic filter

Procedure

1. Click **Edit Filter**.

   The Edit Geographic Filter dialog opens.

2. Update any fields as required.

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

   Important

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

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

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

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

Note

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

7. Click **OK**.

View geographic filter description

Procedure

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

Reputation information

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

The following information is included:

- Criteria for the filter that created the event.
- Tag values for the matching entry from the reputation database. This includes both Reputation DV and user-defined tags.

TMC ThreatLinQ charts and graphs

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

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

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

```
http.proxyHost=

http.proxyPort=

Http.nonProxyHosts=
```

Table properties

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

Customize table property settings

Procedure

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

Note

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

5. Click **Apply**.

Add a comment

Procedure

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

Edit a comment

To edit a comment, do one of the following:

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

Note

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

Tuning event filters (Inspection events)

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

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

Note

If the segment specified in the event was not updated from the SMS, you may receive an error indicating that the correct Profile cannot be determined. If the Profile cannot be determined, you must modify the filter directly through the **Profiles** screen. See *Profiles on page 5-1*.

Filter modifications

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

- **Edit event filters** — When you review event information, you may want to modify event filter settings to better react to events. For example, a filter that is generating a high number of alerts may need to be changed so that it is not invoked against certain types of events.
- **Create event filter exceptions** — Filters may not always respond correctly to source and destination IP addresses. For example, you may have a filter set to block packet traffic to all hosts; however, some benign traffic is destined for a specific host in your network. In that case, you can create a filter exception. *Learn more on page 5-24* about filter exception limits.
- **Create traffic management filters** — When you review event information, you might want to create a Traffic Management filter to block, trust, permit, or rate limit traffic based on different protocols and specific source and destination IP addresses.

Packet trace

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

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

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

For more information, see *Packet trace on page 3-93*.

Packet trace options

Packet trace options are available from the Events area or Device area of the SMS. You can request multiple packet trace files from multiple events or all packet traces on a specific device. Packet trace options are available for devices that support the packet trace feature. Devices, such as the Core Controller and the SSL do not support packet trace. For information on packet trace options available through the Device area of the SMS, see *Save all packet trace information for a device on page 3-93*.

The **PCAP Download** option can be enabled through the **System Preferences** wizard. See *PCAP download on page 11-8*.

Right-click packet trace menu options

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

External packet trace viewer

You can configure the Packet Trace Viewer to use:

- Internal Packet Capture Viewer

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

View the packet trace

Procedure

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

Save packet trace files

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

Procedure

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

Download packet trace files to the SMS

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

Procedure

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

Configure packet trace view settings

Procedure

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

URL Threat Analysis

URL Threat Analysis enables the SMS to automatically use the Deep Discovery (DD) Analyzer device. The DD device analyzes suspicious content in HTTP traffic to detect malware threats to browsing clients in your network.

Configure URL Threat Analysis to send inspection event URLs from the SMS to the DD Analyzer. The DD device analyzes the URLs and then sends the threat analysis results to the SMS. The results are displayed in the URL

Threat Analyzer Results panel and indicate which event URLs might pose a threat. Based on the results, you can make device configuration adjustments, such as modifying profile action sets or creating a manual response to quarantine an infected host.

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

- *Prerequisites on page 6-24*
- *Configure URL Threat Analysis on page 6-26*
- *URL Threat Analyzer results on page 6-27*

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

Prerequisites

Complete the following tasks before you configure URL Threat Analysis. See *Configure URL Threat Analysis on page 6-26* for steps to connect the DD Analyzer device and enable URL Threat Analysis.

- SMS v4.6.0 or later
- Use devices that support HTTP metadata collection, which includes the following versions:
  - **IPS (NX Series)** — TOS v3.7.0 or later
  - **TPS (440T or 2200T)** — TOS v4.2.0 or later
  - **TPS (1100TX or 5500TX)** — TOS v5.2.0 or later
  - **TPS (8200TX or 8400TX)** — TOS v5.0.0 or later
  - **TPS (9200TXE)** — TOS v6.0.0 or later
  - **DD Analyzer** — v5.5.0 or later
- Ensure that TCP port 443 is available so that the SMS can send event URLs to the DD Analyzer. See *Ports on page 4-1* for more information about the SMS network ports.

- Configure one or more profiles to generate events with URL data using the following steps:

  1. Navigate to **Profiles** > **Inspection Profiles** > **<profile name>**.
  2. In the Details tab, click **Edit Details**.
  3. Select **HTTP Context**.
  4. Click **OK** to configure the profile to extract HTTP metadata from filter alerts.
  5. Distribute the profile. See *Profile distribution on page 5-58* for more information.

- Review the filter settings for your profile. Trend recommends including action sets with **+ Notify**.
- Save an inspection event query in **Events** > **Inspection Events**.

  When creating a saved inspection event query, keep the following information in mind:

  - Include any parameters that create a set of events with URLs that you want to send to the DD device to analyze.
  - Trend recommends that you include Events with suspicious URL metadata. In **Filter Criteria**, under Suspicious URL Metadata, select **Include**.

    Note

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

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

For more information about creating an inspection query, see *Search for Inspection events on page 6-3*.

Configure URL Threat Analysis

Before you begin

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

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

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

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

Procedure

1. From the Events workspace, click **URL Threat Analysis** in the navigation pane.
2. Under URL Threat Analyzer Configuration, click **Edit**.
3. In the URL Threat Analyzer Configuration options, select **Enable URL Forwarding**.
4. Select a saved inspection event query.

   For more information about the saved inspection event query, see *Prerequisites on page 6-24*.
5. Select **Add High Risk Analysis Results to URL Reputation Database** to ..
6. Enter the DD Analyzer device IP address.

7. Enter the API key.
8. Enter the certificate.
9. Click **OK**.
    - If registration is successful, the SMS starts sending URLs from the events to the DD Analzyer, and the DD Analyzer device configuration is displayed in the URL Threat Analyzer Configuration panel on the URL Threat Analysis page.
    - If registration is unsuccessful, an error message is displayed, and the SMS redirects you to the URL Threat Analyzer Configuration options.
10. (Optional) To unregister the DD Analyzer from the SMS and stop the SMS from sending URLs to the DD device, do one of the following:
    - Clear **Enable URL Forwarding** in the URL Threat Analyzer Configuration options to simply disable URL forwarding. The configuration settings are still saved when you clear **Enable URL Forwarding**.
    - Click **Reset** on the URL Threat Analysis page to delete the current DD device configuration settings as well as disable URL forwarding.

URL Threat Analyzer results

Use the URL Threat Analyzer results panel to identify potential URL threats to your network and adjust your profile filter action sets if necessary. After the SMS sends a set of inspection event URLs to the DD Analyzer device for analysis, the progress and results are displayed in this panel. For steps to set up URL Threat Analysis, see *URL Threat Analysis on page 6-23*.

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

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

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

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

To update the table results

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

To resubmit a URL to the DD Analyzer

The SMS does not automatically resubmit event URLs to the DD Analyzer after the initial submission. However, if the DD Analyzer did not properly receive the event URL because of a **NonComm** status, for example, you can manually resubmit that URL.

To resubmit URLs to the DD Analyzer, right-click on one or more entries in the results table, and then select **URL Forwarding** > **Resubmit URL**.

Note

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

To create a manual response

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

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

Column	Description
Event Number	The order in which the event appeared in the SMS.
Event Time	The time on the IPS/TPS device that the traffic was first encountered.
Filter Name	The name of the filter that triggered the event.
URL	The event URL.
Risk Level	• **NoRiskFound** — The object did not exhibit suspicious characteristics. • **Low** — The object exhibited mildly suspicious characteristics that are most likely benign. • **Medium** — The object exhibited moderately suspicious characteristics. • **High** — The object exhibited highly suspicious characteristics that are commonly associated with malware. • **Unknown** — The DD Analyzer was unable to determine the risk level. When a URL is resubmitted, the risk level resets to Unknown until the SMS receives the updated results from the DD Analyzer. Details are available for the entry in the DD device management console.

Column	Description
Status	Informational statuses: • **Queued** — The SMS sent the event to the DD Analyzer, but analysis has not begun. • **InProgress** — The event is currently being analyzed by the DD Analyzer. • **Complete** — The event analysis is complete. • **Canceled** — The event analysis was canceled from the DD Analyzer user interface. • **NonComm** — The SMS is not connected to the DD Analyzer. This condition may be caused by network connectivity issues. Error statuses: • **BadURL** — The URL format is incorrect. • **Error** — The DD Analyzer encountered an error. Resubmit the URL by right-clicking the entry and selecting **URL Forwarding** > **Resubmit URL**. If resubmitting does not correct the condition, search for the corresponding URL in the **Virtual Analyzer** > **Submissions** panel in the DD device management console for more specific information about the type of error. • **Timeout** — The URL entry has been in an active state (Queued, InProgress, or NonComm) for over 24 hours. After 24 hours, you can view the entry in the DD device management console.
HTML Reports PDF Reports	Link to the HTML or PDF formatted report generated by the DD Analyzer that provides a comprehensive summary of the event URL. The link only appears in the SMS URL Threat Analyzer Results panel if the submission is in a **Complete** state. Click the report link to download either report file. The content of the HTML and PDF reports is the same; only the format is different. You can also download the report, in either format, in the DD device management console.
Source IP Address	Source IP address from the event. Expand this column for location details, including geography map, region, city, and named resource.

Column	Description
Device	Name of the IPS/TPS device that generated the event.
Segment/Rule	Segment for IPS/TPS-generated events.
Submit Time	The time that the event was submitted from the SMS to the DD Analyzer.

Chapter 7

Reports

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

Navigate the Reports workspace

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

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

From the Reports workspace, you can do the following:

- **Find a report template.** Use the Templates folder to quickly navigate to a set of reports in a particular category. See *Templates on page 7-21*.
- **Display or run the report.** Click a report title. Either the previously generated report appears, or you can apply criteria filters to run the report. See *Run a report on page 7-12*.
- **Create, save, and schedule a report.** Click **Create Report** (on the Saved Reports screen) to generate the report. Alternatively, you can save a report by selecting a report template and applying criteria filters. For example, you can create a report from scratch by uploading a logo, selecting default colors, editing criteria filters, and then saving it. The next time you need to run a report, you can select the saved report to automatically use what was saved from the report template. See *Create a saved report on page 7-22*.
- **View saved report results and schedules.** Click the **Saved Reports** folder to view a list of saved report results and originating report templates. You can modify the criteria filters and customize a saved report. You can also review, edit, or delete the report schedule. See *Saved reports on page 7-22*.
- **Export the data.** On saved reports, click **Export Result** to convert the report to a different format and to select an export type. See *Export report results on page 7-18*.

- **Manage report schedules.** Click **All Schedules** to view all of the report schedules that you created. See *All schedules on page 7-26*

Inspection reports

The SMS has the following Security report templates:

- All attacks
- All destinations
- All sources
- Specific attack
- Specific country
- Specific destination
- Specific source
- Specific user
- Top attacks
- Top attacks by country
- Top destinations
- Top IPS VLANs with attacks
- Top sources
- Top users

The SMS has the following Application report templates:

- All applications
- All destinations
- All P2P peers
- All sources
- Specific applications

- Specific country
- Specific destination
- Specific P2P peers
- Specific source
- Specific user
- Top applications
- Top destinations
- Top P2P peers
- Top sources
- Top users

The following table lists the criteria panels that are available for those report templates.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Filter Criteria	Details including filter name and number, category, profile, severity, Reputation Type, and action. Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded to help you quickly identify and respond to attack traffic. The SMS uses the following severity levels: • **Critical** — Indicates critical attacks that must be looked at immediately. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.

Use this criteria panel...	To filter the report by:
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, and/or client IP.
User Info Criteria	Login IDs of source/destination users and user groups, and the IP addresses of the source/destination domains and machines.
Device or segment	Segment, device or stack. • Click **Add** to add a device or segment. • Click **Delete** to remove an existing device or segment.

Reputation templates

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

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

The following table lists the criteria panels that are available for those report templates.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Filter Criteria	Details including filter name and number, category, profile, severity, Reputation Type, and action Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded to help you quickly identify and respond to attack traffic. The SMS uses the following severity levels: • **Critical** — Indicates critical attacks that must be looked at immediately. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, URL, and/or client IP.
User Info Criteria	Source and destination information for users, domains, and machines.
Device or segment	Segment, device, or stack. • Click **Add** to add a device or segment. • Click **Delete** to remove an existing device or segment.

Rate Limit templates

Rate Limit reports provide options for reporting the percentage of bandwidth used in a pipeline of traffic for rate limit action sets. You can generate reports by device and by rate limit action set. Rate limiting through an action set defines a maximum bandwidth that can be used by traffic that

matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth.

The SMS includes two rate limit report templates: Rate Limits by Specific Device and Specific Rate Limit Action Set.

The following table lists the criteria panels that are available for these report templates.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Device / Rate Limit Criteria	Device or Rate Limit action set. • Click **Add** to add a device. • Click **Remove** to select or clear Rate Limit action sets.
Device Rate Limit Report Options	Time (minute, hours, or days) and/or throughput.

Device Traffic templates

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

The SMS includes one device traffic report template: IPS Physical Port. The following table lists the criteria panels that are available for this report template.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Device Criteria	Device or stack, or specific segment of a device.
Device Traffic Report Options	Time (minute, hours, or days), data display, data aggregation, and/or traffic direction.

Advanced DDoS templates

Advanced DDoS reports provide information about the detection of SYN flood attacks. These attacks enact a series of requests with false SYN flags that constantly request a connection. SYN Proxy enables the use of SYN traps to block all new TCP connection requests from a single attacker against a host.

Note

Only devices that support Advanced DDoS have access to these reports. Only devices that have Advanced DDoS Protection filters can provide data for these reports.

The SMS includes one advanced DDoS report template: DDoS. The following table lists the criteria panels that are available for that report template.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Filter Criteria	Inspection Profile and Advanced DDoS filters are required to run this report.
Segment Criteria	Segment or group for a device.
Advanced DDoS Report Options	Time (minute, hours, or days) and/or one or more DDoS types.

Use this criteria panel...	To filter the report by:
Report Options	Use the Report Options pane to specify various aspects of your report. Report Options selections provide options that directly correlate with how your Report appears. The Report Options panel may include some or all of the following options: • Chart Type • Classification labels • Include All Details Table • Number of matching details • Report logo • Report style • Security Classification label

Executive reports templates

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

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

The SMS includes one executive inspection security report template: Inspection Executive Report. The following table lists the criteria panels that are available for that report template.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Filter Criteria	Details including filter name and number, category, profile, severity, and action set. Attack filters are assigned a severity level which indicates the importance of attack traffic. Severities are color-coded to help you quickly identify and respond to attack traffic. The SMS uses the following severity levels: • **Critical** — Indicates critical attacks that must be looked at immediately. • **Major** — Indicates major attacks that must be looked at soon. • **Minor** — Indicates minor attacks that should be looked at as time permits. • **Low** — Indicates traffic that is probably normal, but may have security implications.
Filter Taxonomy Criteria	Classification, protocol, and/or platform. Click the Lookup icon to quickly search the list.
Network Criteria	Addresses and Ports, VLAN, country, URL, and/or client IP.
User Info Criteria	Source and destination information for users, domains, and machines.
Device, Segment Criteria	Segment, device, or stack. • Click **Add** to add a device or stack, device group, or physical segment. • Click **Remove** to remove an existing device, device group, or physical segment.

Use this criteria panel...	To filter the report by:
Report Options	provide options that directly correlate with how your Report appears. The Report Options panel may include some or all of the following options: • Chart Type • Classification labels • Include All Details Table • Number of matching details • Report logo • Report style • Security Classification label

Traffic Analysis templates

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

Before an analysis report can be generated, you must complete a successful profile distribution to all devices that the sFlow reports will be run against. This creates a policy association, which the Vertica database requires in order to generate a report. The data that is sampled gets sent as an sFlow datagram packet to a collector server where analysis occurs.

The SMS includes the following traffic analysis report templates:

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

Note

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

The following table lists the criteria panels that are available for those report templates.

USE THIS CRITERIA PANEL...	TO FILTER THE REPORT BY:
Protocols, Services Criteria	Protocols, such as GGP, ICMP, TCP, and UDP, and services to be included or excluded. Services are defined collections of TCP/UDP ports, IP protocols, or ICMP type and code values. Service groups are collections of services and are available for selection in this same list.
Segment, Device Criteria	Available physical segments and devices. • Click **Add** to add a device or stack, device group, or physical segment. • Click **Remove** to remove an existing device, device group, or physical segment.
Network Criteria	Source and destination addresses and ports, and VLAN.
Report Options	• Bandwidth: A to B, B to A, or Both • Endpoint: Source, Destination, or Both

Run a report

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

- **Criteria panels**. This section is at the top of the screen. You can use it to filter and perform other options on a report. For example, you can use

the Report Options to choose a chart type and classification label, determine the number of data to include, upload your company logo, and select a color and font as the report style.

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

Run a report

Procedure

1. Select **Reports** > **Templates** , and then select a report.
2. Click the arrow on the left side of the report template name, and use the criteria panels to limit the results of your report.

   Depending on the report, some filters are selected by default (i.e., every severity filter is selected for the All Destinations reports) and others include required fields that must be completed before you can run a report (i.e., you must provide a filter name or filter number to run the Specific Attack report). Your applied filters display in italics to the right of the criteria panel name.
3. (Optional) Click **Customize Query** to build a custom report formula. For more information about building a criteria query, see *Customize a query on page 7-16*.
4. (Optional) From the Last Hour drop-down list, adjust your time frame from the following:
   - Last —Select a standard time interval, such as last minutes, hours, days, or month.
   - User Defined — Type in the field, or click the calendar to select a time duration between two dates (Start Time and the End Time).

- General — Click **Edit** to choose a custom range by selecting a day of the month or day of the week, and then specifying the duration in hours and 5-minute intervals.
- Incremental - Choose increments of minutes, hours, days, or weeks.

5. Click **Run**.

Important

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

Note

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

6. From the generated report, you can perform a variety of functions:
   - Drill down in to view Event details. Click a Filter Name in the report to view the Reputation Events for the selected filter name. The criteria for the event matches the criteria that was assigned when the report was generated, such as the name of the filter and the IP address.
   - Save, save as a custom template, or print the report. For more information about saving a report template, see *Create a saved report on page 7-22*.

Clear filters

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

Procedure

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

Customize the criteria panels

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

Change the criteria panels that display on a report

Procedure

1. Click the arrow on the left side of the report template name.

   The SMS displays the available criteria panels for the selected report.

2. Click **Customize Panels**.

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

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

The Reports screen opens, and your criteria panels reflect your changes.

Customize a query

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

Create a custom query for a report

Procedure

1. Select **Reports**, and then select a report template name.
2. Click **Customize Query**.
3. Type your query in the Query Structure field.

   As you type your query, the syntax displays in the Full Query Expression list box. Syntax that contains errors will automatically display bold, and you will not be able to proceed.
4. Click **OK**.

Report results

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

Open a saved report

Procedure

1. Select **Reports** > **Saved Reports**.

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

Edit result settings and permissions

Procedure

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

   The Report Results table opens.

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

   The Edit Report Result wizard opens.

3. On the Result Settings screen, provide the following information:

   a. Saved Result Name — Update the existing report title as needed.

   b. Specified Cleanup Date — Select this option, and then click to schedule a date in which the report will be kept until. After this date/time, the report result will be deleted from the SMS.

   c. No Cleanup — Select this option to keep all report results.

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

5. Click **OK**.

Delete a saved report

Procedure

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

   The Report Results table opens.

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

3. Click **Delete**.

The report is removed from the Saved Reports table and the Reports navigation pane.

Export report results

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

Exported results can be in the following formats:

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

Important

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

Export a report result

Procedure

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

   The Report Results table opens.

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

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

3. Click **Finish**.

Report schedules

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

Create a new schedule

Procedure

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

   The Schedules table opens.

2. Click **New**.

   The Create Schedule wizard opens.

3. On the Schedule screen, select one of the following:

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

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

5. Click **Export Results** (or click **Next**), and then do the following:

   a. Email Results — Add all the email address that apply, separated by commas. Alternatively, click **Current User Email** to use the email address of the currently logged in user.

   b. (Optional) Select the **Include HTTP(s) link to online web report** check box to include the logged in user.

   c. Format — Decide in what format you want to send the report.

   d. Remote Copy/Archive — Use the radio buttons to select whether you want to archive the report and enter the remote directory, server, filename, and user credentials. From — Enter the email address where the notifying email originates.

6. Click **Finish**.

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

Edit an existing schedule

Procedure

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

Delete a schedule

Procedure

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

Templates

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

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

Report permissions

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

When you create a report, you become the owner of the report. If a report has no owner, then the report and its schedule items and results are visible only to SuperUsers. Saved reports are only visible if the user's user group has permission to view the report.

Saved reports

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

- **Create a saved report**. A fast and easy way to generate a report is to customize an existing report template by using the Create Report wizard to determine the schedule, to set permissions, and to configure where to export the data to.
- **Maintain your saved report library.** Click a report title to view its current template and to run the report. You can update an existing report as needs arise; use a saved report as a template to create a new saved report; and delete unnecessary reports.
- **Track report results.** Use the Report Results table to review a list of every time the report was generated. You can open a report result in a new window; edit the result settings and permissions of a report result; export a report result to a local file, email, or external source; save the report result to a popular document format, such as a PDF; or delete a report result. For more information about tracking report results, see *Report results on page 7-16*.
- **Manage report schedules.** Use the Schedules table to drill down into the schedules for a saved report. You can create a new report schedule; edit the result settings and permissions of a report result; export a report result to a local file, email, or external source; or delete a report schedule. Alternatively, you can access this information on the All Schedules table. For more information about viewing all report schedules, see *All schedules on page 7-26*.

Create a saved report

The Create Report wizard guides you through the steps for creating a custom report. At a minimum, you must name your report and select a template. Use

the icons located in the navigation pane to quickly see if all of the required fields for a category are complete; incomplete categories display a red x, complete categories display a green check mark.

Procedure

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

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

2. Click **Create Report**.

   The Create Report wizard opens.

   Note

   You can also access the Create Report wizard if you click **Save Report** on a report template or **Save As** on a saved report. For details, see *Run a report on page 7-12*.

3. On the Report Name screen, provide the following information:

   - Name — Enter a title for the report in the Name field.
   - Description — (Optional) Type a description that will help you remember the purpose of the report.
   - Template — Select the desired report template from the Template drop-down list.

4. Click **Template** (or click **Next**), and then do the following:

   a. Report Time Period — From the Last Hour drop-down list, adjust your time frame from the following:

      - Last —Select a standard time interval, such as last minutes, hours, days, or month.
      - User Defined — Type in the field, or click the calendar to select a time duration between two dates (Start Time and the End Time).

- General — Click **Edit** to choose a custom range by selecting a day of the month or day of the week, and then specifying the duration in hours and 5-minute intervals.

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

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

5. Click **Schedule** (or click **Next**), and then do the following:

a. Run Now — Select the **Run Now** check box to immediately execute the report. “Immediate execution” will display on the Report Results and Schedules tables.

b. Run on Schedule — Select the **Run on Schedule** check box, and then do the following:

- Schedule Name — Enter a name for the schedule in the Schedule Name field.
- Time — Specify the time. First select a time range option, and then for the selected option, create a custom range. For example, if you want to look at a weekly report, select Weekly, and then define the interval.
- Duration — Specify when the report schedule will end.

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

7. Click **Export Results** (or click **Next**), and then do the following:

- Email Results — Add all the email address that apply, separated by commas. Alternatively, click **Current User Email** to use the email address of the currently logged in user.

- (Optional) Select the **Include HTTP(s) link to online web report** check box to include the logged in user.
- Format — Decide in what format you want to send the report.
- Remote Copy/Archive — Use the radio buttons to select whether you want to archive the report and enter the remote directory, server, filename, and user credentials. From — Enter the email address where the notifying email originates.

8. Click **Finish**.

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

Run a saved report

Procedure

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Use the criteria panels to limit the results of your report. For details, see *Run a report on page 7-12*.

3. Click **Run** to apply your selected filters.

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

Edit a saved report

Procedure

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Edit the report as needed.

Note

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

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

Save as a new report

Procedure

1. Click a saved report title.

   The Report screen for the saved report template opens.

2. Edit the report as needed.

Note

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

3. Click **Save As**.

   The Create Report wizard opens. For details, see *Create a saved report on page 7-22*.

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

All schedules

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

From here, you can:

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

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

Note

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

Edit a report schedule

Procedure

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

Delete a report schedule

Procedure

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

Chapter 8

Administration

The SMS client provides administration options to enable you to manage user access, system and audit logs, and system settings. Options are also available to back up the SMS database, configure the SMS server, and upgrade SMS software and licenses.

The Admin workspace enables you to manage user access, system and audit logs, and system settings. Options available through the Admin workspace are limited to users with the appropriate role and access level.

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

General administration

General administration of the SMS server includes tasks, such as upgrading or patching the SMS software, administering licenses, reviewing system health, and other maintenance tasks.

The General screen in the Admin workspace displays information about your SMS including system time and server uptime, current software version and installed patches, software and patches available for download, license information, security certificates, and the certificate key.

SMS server

The SMS Server panel displays the system date and time according to the time zone and network time options configured on the SMS. Buttons in this panel allow you to **Refresh** the connection with the SMS, or **Reboot** or **Shutdown** the SMS server.

CAUTION!

Before rebooting or shutting down an SMS Server consult your company's policies for handling service interruptions of key servers. At a minimum, you might need to communicate that all connections to the SMS server will be disrupted.

Important

When you shut down or reboot an HA-configured cluster, both nodes of the cluster are shut down or rebooted.

SMS software

The SMS Software panel displays the current SMS software version installed on the server, any SMS software that is available for you to download, and SMS software that has been downloaded and is ready to be installed. From this panel, you can download, import, and install SMS software.

When it is connected to the TMC, the server monitors for newer versions of the SMS software. When a version newer than the current version is

detected, the Available for Download field displays the software version number, and the **Download** button on the SMS Software panel becomes available.

Before you download and install a new version of the SMS software, read the SMS Release Notes thoroughly and take note of the following caveats:

- The SMS server can obtain the software automatically from the TMC or can import an upgrade package file from storage media or a hard drive.
- You cannot roll back an upgrade.
- An SMS software upgrade can take up to thirty minutes. Connect to the SMS server by display console to monitor the process.
- Installing a new version of SMS causes the SMS server to reboot and close all client connections. If you perform an upgrade from an SMS client, the client eventually loses connection because the SMS server to which it is connected must reboot.
- When the SMS server is unavailable during the reboot process, the availability and operations of TippingPoint devices managed by the SMS are not affected. IPS and other devices continue to operate as usual and without interruption.
- The version of SMS client software should match the version of the SMS server. When you upgrade the SMS server, you might be unable to connect to the server through an SMS client until you have upgraded the SMS client software. You can still connect to the SMS server through the command-line interface and through a Web browser.
- If your SMS server is configured for High Availability (HA), you must disable HA prior to performing an upgrade of the SMS servers. To upgrade a HA cluster, break down the cluster, upgrade each SMS individually, and then re-establish the cluster.

Download and install SMS software

Procedure

1. Click **Download** (when the button is available) to download the software update.

When the download is complete, the value in the Available for Download field matches the value in the Available for Install field.

2. Click **Install** to install the downloaded package.
3. Click **Yes** to confirm the installation.
4. Update each SMS client that connects to the SMS server.

   You can also obtain SMS software through media such as a USB drive, or you can download the software to a system through a direct login to the TMC. In this case, you must first import the software package, and then install it.

Note

Do not modify the name of the file prior to importing it.

Import and install SMS software from the TMC

Procedure

1. Click **Import**.
2. Select the SMS software package, and click **Open**.
3. Click **Install** to install the imported package.
4. Click **Yes** to confirm the installation.
5. Update each SMS client that connects to the SMS server.

SMS patches

The SMS Patches panel displays information about software patches that are currently installed and software patches that are available for download from the TMC. The SMS Patch Notifications field indicates whether SMS patch notifications are enabled or disabled.

SMS patches provide updates to the SMS server, the SMS client, or both. Patches are cumulative; the latest patch includes all previously released

patches for a particular version of the product. For more details, refer to the Release Notes available during the patch upgrade process or on the Software Details page for the patch on the TMC.

The SMS server, when connected to the TMC, monitors the TMC for SMS software patches. In the SMS client, you can enable or disable SMS patch notifications that indicate when a more recent patch is available. If patch notifications are enabled, a green check and the value “Enabled” are displayed in the SMS Patch Notifications field. If patch notifications are disabled, the value “Disabled” is displayed. Click the button to the right of the field to enable or disable patch notifications.

Before you download and install an SMS patch, read the SMS Release Notes thoroughly and take note of the following caveats:

- The SMS server can obtain the software automatically from the TMC or can import a patch file from storage media such as a USB drive or hard drive.
- You can typically roll back a patch; refer to the patch Release Notes for rollback information. If you choose to roll back a patch, it rolls back the cumulative patch, effectively removing *all* patches from the SMS server. A patch rollback typically requires a restart of the SMS server application.
- Installing an SMS patch typically causes the SMS server application to restart, and in some cases requires the SMS server to reboot. All client connections to the SMS are stopped during the patch process.
- When the SMS server is unavailable during the reboot process, the availability and operations of TippingPoint devices managed by the SMS are not affected. IPS and other devices continue to operate as usual and without interruption.
- The version of SMS client software should match the version of the SMS server. Some patches require an update to the SMS client as well as the SMS server. In this case, all clients are prompted to upgrade to the newer version when they try to connect to the patched SMS server.
- If your SMS server is configured for High Availability (HA), see *Apply software updates to a cluster on page 8-156*.

Install an SMS patch

Procedure

1. Click **Update** to open the SMS Patch wizard.
2. Do one of the following:

   Import an SMS patch file from storage media or your local drive:

   a. Select **Import from File**, and then click **Next**.

   b. Choose the SMS patch file to import.

   c. Click **Import**.

   d. Click **Finish**.

   Note

   Do not modify the name of the file prior to importing it.

   Download an SMS patch file from the TMC website:

   a. Select **Download from TMC**, and then click **Next**.

   b. If there are any available SMS patches, select the appropriate patch from the list. The Release Notes section displays information about the selected patch.

   c. Click **Download** to download the selected patch.
3. Click **Install** to install the downloaded package.
4. Click **Finish**.

   If necessary, update each SMS client that connects to the SMS server.

Roll back an SMS patch

Procedure

1. On the SMS Patches panel, click **Rollback**.
2. Click **Rollback** again on the Confirm Rollback screen to confirm the operation.
3. Click **Finish**.

   The SMS server rolls back the patch, which requires a restart of the SMS server software. When the rollback process is complete, the SMS server is running the base SMS software (without any patches).

SMS web security SSL certificate

The SMS uses a web security SSL certificate to establish secure communication between a web browser and the SMS server. When the SMS is configured for high availability (HA), the certificate is synchronized across nodes in the SMS HA cluster.

You can import a certificate now, or if you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see *View certificates on page 8-56*.

Note

The web security SSL certificate is included in an SMS backup. The certificate is reset during a factory reset operation.

The SMS web security SSL certificate panel displays the following information for the current certificate:

- **Current Certificate** – The SMS name of the certificate.
- **Pending Certificate** – If you edit the name of the certificate, the SMS will display the new name until you reboot the SMS. After you reboot the SMS, the certificate name will appear as the current certificate.

The SMS provides a <Default Certificate>. If you experience problems with the certificate, you can reset the certificate to the default.

Reset the SMS web security SSL certificate

Procedure

1. On the SMS Web Security SSL Certificate panel, click **Reset**.
2. In the Confirm Reset dialog, click **Yes**.
3. Restart the SMS server for the new certificate to take effect.

Note

Resetting the certificate generates and installs a default SMS Web Security SSL Certificate, which replaces the current certificate.

In some cases, you might want to replace the default certificate with a root Certificate Authority (CA) signed certificate to establish a trusted relationship between Web clients and the SMS Web server. The SMS client enables you to import an X.509 certificate and corresponding PKCS#8 DER-encoded private key for use as a Web server certificate.

Import a custom Web security SSL certificate

You can specify a custom Web security SSL certificate with a root CA signed certificate to establish a trusted relationship between web clients and the SMS web server.

Procedure

1. On the SMS Web Security SSL Certificate panel, click **Edit**.
2. In the dialog, specify the certificate you want to import into the SMS with a private key.

Important

The PKCS#8 file must not be password protected.

3. Click **Import**.
4. Restart the SMS server for the new certificate to take effect.

Note

When you import a custom Web security SSL certificate, a dialog box will appear at your first SMS client login attempt prompting you to trust the new certificate.

SMS certificate key

The SMS Certificate Key panel displays information about the currently installed certificate key including the certificate number, key size, and description. The SMS certificate key is an RSA certificate that contains the serial number used to identify this SMS. It is also used as the SSL certificate for communication between the SMS client and the SMS server.

By default, the SMS comes from manufacturing with a 2K (2048 bits), which also uses stronger hashing functions.

Important

To manage a 9200TXE TPS device, the SMS must have a 2K key installed to communicate with the device.

Note

Only users with SuperUser capabilities are able to upgrade the SMS certificate key.

Before you upgrade the SMS certificate key, note the following caveats:

- The SMS can obtain the certificate key package automatically from the TMC, or you can import the key from a file.

- Installing the 2K key requires a restart of the SMS. The 2K key will not be in use until you restart the SMS. When you install the 2K key without restarting the SMS, a message will display on the SMS Certificate Key panel.
- After you install the 2K key, you will lose device management functionality on the SMS, if you roll back to TPS devices running TOS v4.0.

For more information, see *Rollback to a previous version on page 3-105*.

FIPS mode and certificate key size

If the SMS is currently running a 1K key, it will display a message about upgrading to a 2K key to be fully FIPS compliant. You can still enable FIPS mode on the SMS without installing the 2K key, but when the SMS is in FIPS mode, you cannot install the 2K key. Any SMS device that is running in FIPS Crypto Core mode with a 1K certificate key cannot be upgraded to SMS v6.1.

High Availability (HA)

When the SMS is configured for HA, keep in mind:

- You cannot install the 2K key in either SMS while the SMS is running in HA. You must first disable the HA cluster, install the 2K key on each SMS, and then reconfigure the SMS HA cluster.
- Both SMS systems in the HA cluster must be running the same key size. For example, the primary SMS cannot be running a 1K key and the secondary SMS be running a 2K key.

For more information, see *SMS High Availability on page 8-145*.

Update the SMS certificate key

By default, the SMS will be running with the 1K key installed. Follow these steps to upgrade to the 2K key.

Procedure

1. Click **Upgrade** to open the SMS Certificate Key Upgrade wizard, review the list of incompatible devices, and then click **Next**.

2. Do one of the following:
   - Download the SMS certificate key from the TMC:
     a. Select **Download from TMC**, and then click **Next**. The SMS displays the status of the certificate key package download. The SMS displays an error message if a connection cannot be made to the TMC, the file is not found, or the file is invalid.
     b. Click **Download** to download the selected patch.
   - Import the SMS certificate key file from storage media or your local drive:
     The SMS certificate key is available on the TMC at **My Account** > **FIPS Certification Package**
     a. Select **Import from File**, and then click **Next**.
     b. Click **Browse**, and then select the SMS certificate key package.
     c. Click **Import**.
3. (Optional) Select the **Restart the SMS when finished** check box to immediately restart the SMS.

   The 2K key will not be in use until you restart the SMS. If you install the 2K key without restarting the SMS, a message will display on the SMS Certificate Key panel.
4. Click **Finish**.

View system health

The System Health screen in the Admin workspace enables you to monitor and review the health of the SMS server, including hardware and software. To open the screen, expand the General node in the navigation pane and select **System Health**.

The System Health screen displays a summary of the current state of the monitored statistics in a table, and shows longer-term historical statistics in a series of graphs. When the SMS is configured in a HA cluster, the System Health screen displays information for both the active and the passive server using a separate tabbed view for each server.

The SMS monitors memory usage, CPU utilization, swap usage, and various file system categories (archive, database, package, system, report, and operating system). The top portion of the screen displays current health statistics in a table view. The Refresh button directly below the table refreshes the current statistics.

Note

The System Health screen displays temperature for a physical SMS appliance, but not for a virtual deployment (vSMS).

You can adjust this to customize how the SMS client presents this information. The bottom portion of the screen displays Memory, CPU, and File System graphs that represent historical statistics over time. To view realtime data from any of the historical graphs, click the **Realtime** icon.

View port health

The Port Health screen in the Admin workspace enables you to view statistics related to the SMS server ethernet ports. To open the screen, expand the General node in the navigation pane and select **Port Health**.

The Port Health screen displays a summary of port usage statistics in a table, and shows longer-term historical statistics in a series of graphs. When the SMS is configured in a HA cluster, the Port Health screen displays information for both the active and the passive server using a separate tabbed view for each server.

The top portion of the Port Statistics screen displays current port statistics in a table view. For each interface, the table displays the number of bytes incoming and outgoing, the number of packets discarded, and the number of errors, as described in the following table.

Information	Description
Interface	Network interface, typically shown as primary port or secondary port.
Total In: Bytes	Total number of bytes that have passed into the port.

Information	Description
Total Out: Bytes	Total number of bytes that have passed out of the port.
Total In: Discards	Number of inbound packets discarded, although no errors were detected.
Total Out: Discards	Number of outbound packets discarded, although no errors were detected.
Total In: Errors	Sum of all errors that prevented the final transmission of inbound packets.
Total Out: Errors	Sum of all errors that prevented the final transmission of outbound packets.

The Refresh button directly below the table refreshes the current statistics. The bottom portion of the screen displays a graph for each ethernet port. Data in the graph shows historical statistics over time.

View or export SMS system log messages

The SMS system Log contains information about software processes that control TippingPoint devices, including startup and maintenance routines. By default, the SMS system log contains information about events that have occurred during the current day.

For each event, the system log displays the date and time it took place, the severity level of the event (Info, Warn, or Error), and a message-level description of the event.

Note

You must have SuperUser privileges to access the SMS system log.

You can adjust table properties to customize how the SMS client displays system log information.

Procedure

1. Select **Admin** > **General** > **SMS System Log**.
2. On the Date Range panel, do one of the following:

a. Click the first option, and select a duration from the drop-down menu.

b. Click the second option, and specify Start Time and End Time.

3. Click **Refresh**.

4. Do one of the following:

   a. To export the full set of results, click **Export All**.

   b. To export specific events, select the events in the list, and then click **Export Selected**.

5. In the dialog, specify a name and location for the file and click **Save**.

   To change the file format, select another option in the file type drop-down menu before you click Save.

   Note that you can use the **Find** utility to locate a specific event. Also, you can select **Details** from the right-click menu to view System Log Record Details for an event.

View or export SMS audit log messages

The SMS Audit Log contains detailed information about user activity. By default the log contains information about events that have occurred during the current day.

The following table describes the information shown on the SMS Audit Log screen.

Information	Description
Number	System-assigned identification number for reference purposes.
Time	Date and time the operation occurred.
User	User name for the account that performed the action. The field might include a user entry for SMS and CLI. These entries are entered by those applications into the audit log as a Super User level of access.

Information	Description
Host	Name of the host from which the user operation occurred.
Operation	Description of the action performed by the user.
Status	Result of the operation; valid status is either success or failure.

Audit log events can help you investigate user-initiated activities. You can export one, or all, of the events and send them to a customer support organization for a detailed analysis of the information.

Note

The system log is accessible only to users with superuser privileges.

Procedure

1. Select **Admin** > **General** > **SMS Audit Log**.
2. Select the appropriate options on the Date Range Panel to view the SMS system log.

Authentication and authorization

Authentication and Authorization includes tasks such as configuring authentication, managing user roles, configuring user groups, and setting up user accounts.

Note

Users must meet authorization requirements to perform tasks described in this section. The user account must be a member of a group with SuperUser role capabilities or the SMS Authentication and Authorization Admin capabilities.

Manage active sessions

The Admin (Authentication and Authorization) screen displays information about active sessions on the SMS. This screen allows you to view and manage client sessions active on the SMS. In addition to viewing information about active client sessions, you have the ability to terminate user sessions if necessary.

The following table describes the fields in the Active Sessions table.

Field	Description
User Name	User name of the account with which the session connection is established.
IP Address	IP address of the system that initiated the session and with which the SMS has an active connection.
Groups	Groups to which the user account is a member. Also specifies the New Resource Group (target creation group for the account).
Login Time	Date and time, based on the time zone of the SMS Server, that the session initiated its connection with the SMS Server.

A New Resource Group is the target group into which objects created by a user are contained and verified for authorized access. When a remote user logs on to the SMS, the user may be prompted to set a New Resource Group if one is not already assigned in SMS or mapped to an Active Directory group.

If the New Resource Group is not set through automatic mapping to an Active Directory group, then you can set or change the New Resource Group for a user logged on to the SMS.

Set or change a new resource group for a user account

Procedure

1. In the navigation pane for the Admin workspace, click **Authentication and Authorization**.
2. Select the session row in the Active Sessions table, and then click **Set New Resource Group**.

3. In the dialog, select a New Resource Group from the list, and then click **OK**.

Note

When you are using Active Directory for authentication and authorization — If you want to use telephone notes to determine new resource group mapping and the SMS is set to reject login on group mapping failure, you must be a member of any groups listed in your telephone notes. If you include a group in your telephone notes that you are not a member of in AD, then you will not be allowed to login to the SMS. See *Edit Active Directory global group mapping on page 8-26*.

Terminate an active session

Procedure

1. On the Admin (Authentication and Authorization) screen, select the session in the Active Sessions table.
2. Click **Terminate**.

   When a session is terminated, the SMS Server does not request confirmation, nor does it send notification to the SMS client when the connection is ended. From the perspective of the end user, the SMS client closes without warning.

Note

To terminate an active session, your account must have SuperUser privileges or user management capabilities. In addition, you cannot terminate your own active session.

Configure authentication

The Authentication screen enables you to configure the mechanism with which the SMS server authenticates user login requests.

The SMS supports five types of user authentication: local, RADIUS, Active Directory, TACACS+, and CAC. You must choose one authentication method per SMS server:

- **Local** – Authentication is performed locally on the SMS.

  Note

  In order for TPS devices to use this option, SMS port 443 must be open and accessible by the device.

- **RADIUS** – Authentication is performed on the RADIUS server; user role and access rights are maintained on the SMS server. If the RADIUS server is unavailable, the SMS can authenticate local users. You cannot manage the SMS user account on the RADIUS server, and you can modify the user password only from the RADIUS server.
- **Active Directory** – Authentication is performed on the Active Directory (AD) server; for SMS accounts, user role and access rights are maintained on the SMS server. If the AD server is unavailable, the SMS can authenticate local users if the Authentication Mode for the active group mapping is set to "Allow only users defined in the SMS to login." If another mode has been configured, only users whose access privileges are maintained locally on the SMS are able to login. You cannot manage the SMS user account on the AD server; you can modify the user password only from the AD server.
- **TACACS+** – Authentication is performed on the TACACS+ server; user role and access rights are maintained on the SMS server. You can specify up to three TACACS+ servers.

  Because SMS authentication using TACACS+ does not support authorization, you must create a local user for all users that log in to SMS by using TACACS+. Create a local SMS user with the appropriate group memberships and clear the **Local Authentication Only** check box. A local password is only needed for Local Authentication failover (on TACACS+ timeout only).

- **CAC** – Authentication is performed on the SMS server using Certificate Authority (CA) certificates and an ActivClient smart card reader. Users

are validated against their Active Directory accounts. The SMS matches a user's group in Active Directory with a group on the SMS. If the SMS is in CAC Authentication mode, all SMS users must log in using CAC. No local users are allowed to log into the SMS client.

Only one authentication method per SMS server is permitted at any one time, but the SMS does allow an administrator to designate user accounts that must always be authenticated locally regardless of the designated authentication source. In this way, you can configure the SMS to use either RADIUS, Active Directory, or TACACS+ as an authentication source, but to specify user accounts that must be authenticated on the SMS.

Tip

We recommend that you have at least one superuser account that authenticates locally to ensure access for system troubleshooting.

Authentication source

The Authentication Source panel displays the authentication method that is currently enabled. By default, the authentication method is set to Local Authentication.

Before you can change the authentication source to use remote authentication, you must configure those options. See *Authentication and authorization on page 8-15*.

When you enable an authentication source, you can specify users that must always be authenticated locally regardless of the designated authentication source. The SMS does not support the use of RADIUS, Active Directory, TACACS+, and CAC authentication on the same SMS server.

Edit the SMS server authentication source

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click **Edit** on the Authentication Source panel.

3. In the dialog, select an option as the group mapping method:
   - Use Local Authentication
   - Use RADIUS Authentication
   - Use Active Directory Authentication
   - Use TACACS+ Authentication
   - Use CAC Authentication

Note

You cannot select Active Directory, RADIUS, or TACACS+ authentication options until these options are configured. See *Configure authentication on page 8-17*. For more information on configuring CAC Authentication, see *Configure CAC authentication on page 8-31*.

4. In the lower portion of the dialog, select user accounts that are **only** authenticated locally, even if a remote authentication server is selected as authentication source.
5. Click **OK**.

Authentication configuration

The Authentication Configuration panel contains separate tabs for RADIUS, Active Directory (AD), TACACS+, and CAC configuration. Select the appropriate tab to configure one of these authentication options.

To secure information passed during authentication, you can enable SSL-based encrypted communication between the SMS and an AD authentication server, and you can import an x509 certificate from a RADIUS server to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded x509 certificates. TACACS+ servers do not use SSL-based encryption or certificate-based authentication.

To edit authentication configuration, your user account must be a member of a group with superuser role capabilities or the *SMS Authentication and Authorization Admin* capabilities.

Configure RADIUS authentication

Remote Authentication Dial In User Service (RADIUS) is an industry-standard method used to authenticate user login requests.

Although user authentication is performed on the RADIUS server, user authorizations and access rights are maintained on the SMS server. If the RADIUS server is unavailable, the SMS can authenticate local users. The SMS does not permit you to manage SMS user accounts on the RADIUS server; the account password for a RADIUS authenticated user must be changed on the RADIUS server.

Edit the RADIUS server configuration

Procedure

1. On the Authentication screen, select the RADIUS tab on the Authentication Configuration panel.
2. Click **Edit** to the right of the Primary RADIUS Server panel.
3. In the dialog, configure the RADIUS server options described in the following table.

Setting	Description
IP Address	IP address of the RADIUS server.
Port	Port on the RADIUS server that listens for authentication requests; the default value is 1812.

Setting	Description
Authentication Protocol	Authentication method used on the RADIUS server: • PAP • MD5 • PEAP/EAP-MSCHAPv2 To use the PEAP/EAP-MSCHAPv2 protocol, you must first import an X509 certificate for the RADIUS server. You can click **Import** to import a certificate or choose a previously imported one from the SMS certificate repository. For more information about certificate management, see *View certificates on page 8-56*. **Important** A certificate import or reset is a separate operation from configuring the authentication source and takes effect immediately. The SMS administration should carefully coordinate certificate and the RADIUS configuration changes.
Secret/Confirm Secret	String used to encrypt and sign packets between RADIUS clients and the RADIUS server, set in the RADIUS client configuration file.
Timeout	Timeout, in seconds, for communication with the RADIUS server; the default value is 3 seconds.

4. Test the RADIUS configuration by entering a valid User Name and Password for the server (and confirming), and then clicking **Test**.
5. Click **OK** to save the server configuration.

An X509 certificate is required for validating PEAP/EAP-MSCHAPv2 authentication responses. The certificate is generated on the RADIUS server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.

What to do next

You can also change the configuration of RADIUS servers by selecting **Devices > *device-name* > Authentication > RADIUS Groups > Edit > RADIUS Servers > Edit**.

Edit RADIUS group mapping

These settings apply to the entire RADIUS server and all its users.

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click the **RADIUS** tab.
3. Click **Edit** under RADIUS Group Mapping.
4. In the dialog, select a group mapping method and options for the SMS to use.

Setting	Description
Authentication Mode	Select one: **Allow only users defined in the SMS to log in** or **Allow RADIUS users to log in with or without an SMS account**. If you choose to allow access for non-local users, you must also specify how the New Resource Group will be determined for those users. By default, users are allowed to choose a New Resource Group.
Authorization Mode	If you configured Authentication Mode to allow only users defined in the SMS to log in, then you can select either of two options: **Use SMS local group mappings** or **Use RADIUS group mappings**. Otherwise, Authorization Mode uses RADIUS group mappings.
RADIUS Mapping Attribute	Type the RADIUS attribute to determine which group it should map to on the SMS.

Setting	Description
Mapping Failure Action	Select an action to take when a RADIUS group cannot be mapped: • Reject Authentication • Accept Authentication with local SMS group mappings – available only if Authentication Mode is configured to allow only users defined in the SMS to log in. • Accept Authentication – Select an SMS user group to which the user is assigned for authorized access.
Mapped Group	Select a mapped group.

5. Click **OK**.

Configure Active Directory authentication

Active Directory is a Microsoft-produced, Windows-centric method used to authenticate user login requests.

Although user authentication is performed on the Active Directory server, user authorizations and access rights are maintained on the SMS server. You can configure a second Active Directory server that the SMS can use for authentication when the primary authentication server goes down or otherwise cannot be reached. If either Active Directory (AD) server is unavailable, SMS can authenticate the user locally. The account password for an AD-authenticated user must be changed on the SMS. The SMS does not permit you to manage user accounts on the Active Directory server. User credentials for remote AD accounts must be managed on the Active Directory server. The SMS is not permitted to change passwords for user accounts on the Active Directory server.

The SMS server supports using Active Directory to authenticate logon requests as well as mapping users to AD groups for authorization requests. You specify Active Directory Global Group Mapping when you configure the Active Directory server for authentication on the SMS.

Before you configure an Active Directory server for user authentication, the SMS must be able to resolve the IP address of the server. The Domain Name

System (DNS) must be configured and enabled on the Active Directory server, and all domain clients must use the AD server as their primary DNS server.

Note

When using an Active Directory server for user authentication on the SMS, the **User ID** is case-sensitive. You must type the **User ID** on Active Directory exactly as it was entered on the SMS.

Note

If you experience a problem with the DNS configuration on Active Directory, contact customer support (TAC) for assistance.

Note

When the SMS is configured to operate in HA mode and the authentication source is Active Directory, the SMS HA cluster must use the shared virtual management IP address. In addition, the shared virtual management IP address must be configured on the Active Directory server as a location from which to accept authentication requests.

Edit the Active Directory server configuration

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click the **Active Directory** tab.
3. Click **Edit** under Active Directory Server Configuration panel.
4. In the dialog, configure the Active Directory server options described in the following table.

Setting	Description
Server Address	IP address or host name of the Active Directory server.

Setting	Description
Enable SSL	Select **Using LDAPS** to enable Lightweight Directory Access Protocol (LDAP) over SSL. If enabled, you must also import an Active Directory SSL certificate. See *Configure Active Directory authentication on page 8-24*.
Port	The port on the Active Directory server that listens for authentication requests. The default non-SSL port is 389; if SSL is enabled, the default port is 636.
Timeout	Timeout, in seconds, for communication with the Active Directory server; the default value is 30 seconds.
Admin Name/DN	Identifies the account on the Active Directory server that is permitted to search the LDAP directory within the defined search base. This is the bind user on the Active Directory server that enables the SMS to query the LDAP directory and authenticate users. `Example: Administrator@DOMAINNAME`
Admin Password	Active Directory server administrative password.
User and Group Search Base	Top-level distinguished name in the Active Directory hierarchical structure where the authentication request begins. `Example: DC=adomain, DC=example, DC=com`

5. Test the Active Directory configuration, enter the Admin Password for the server, and then click **Test**.
6. Click **OK** to save the server configuration. All SMS users must be identified with a New Resource Group. See *Manage active sessions on page 8-16*.

Edit Active Directory global group mapping

These settings apply to the entire Active Directory server and all its users.

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click the **Active Directory** tab.

3. Click **Edit** under Active Directory Global Group Mapping.
4. In the dialog, select a group mapping method and options for the SMS to use.

Setting	Description
Authentication Mode	Select one: **Allow only users defined in the SMS to log in** or **Allow AD users to log in with or without an SMS account**. If you choose to allow access for non-local users, you must also specify how the New Resource Group will be determined for those users. By default, users are allowed to choose a New Resource Group.
Authorization Mode	If you configured Authentication Mode to allow only users defined in the SMS to log in, then you can select either of two options: **Use SMS local group mappings** or **Use active directory group mappings**. Otherwise, Authorization Mode uses active directory group mappings.
New resource group mapping mechanism	Specify how the New Resource Group is set for Active Directory (AD) authenticated users: • Allow user to choose – users specify an SMS group as their New Resource Group • Use Active Directory Primary Group – automatically sets the AD primary group as the New Resource Group; users are unable to set the group manually. Typically, the default primary AD group is Domain Users. • Use Active Directory ... attribute – specify an AD attribute for the SMS to use in mapping a New Resource Group for all AD-authenticated SMS users.
Mapping Failure Action	Select an action to take when an Active Directory group cannot be mapped: • Reject Authentication • Accept Authentication with local SMS group mappings – available only if Authentication Mode is configured to allow only users defined in the SMS to log in. • Accept Authentication – Select an SMS user group to which the user is assigned for authorized access.

Setting	Description
Mapped Group	Select a mapped group.

5. Click **OK**.

   An X509 certificate is required for validating authentication responses over an SSL connection. The certificate is generated on the Active Directory server, and must be imported to the SMS. The SMS server accepts DER (binary) or PEM (Base64) encoded X509 certificates.

Import an Active Directory SSL certificate

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click the **Active Directory** tab.
3. On the Active Directory tab, click **Import** to the right of the Active Directory SSL Certificate panel.
4. Select the X509 certificate file from your local drive or storage media, and click **Import**.

   Important

   A certificate import is a separate operation from configuring the authentication source and takes effect immediately. The SMS administration should carefully coordinate certificate and the Active Directory configuration changes.

5. (Optional) If you have already imported a certificate into the SMS certificate repository, simply choose the one you want. For more information about certificate management, see *View Certificate Authority (CA) certificates on page 8-62*.

Configure TACACS+ authentication

Terminal Access Controller Access-Control System Plus (TACACS+) is another industry-standard method used to authenticate user login requests.

TACACS+ authenticates over TCP. Because TCP is a connection-oriented protocol, TACACS+ does not require transmission control the way RADIUS does. While RADIUS encrypts only passwords, TACACS+ uses MD5 encryption on all communication and is consequently less vulnerable to attacks.

Unlike RADIUS authorization, the role (privilege level) of a TACACS+ user is determined by the TACACS default-user group configuration on the TPS device. For example, if the TACACS+ default-user group is set to `operator`, TACACS users are assigned the `operator` role. This might not provide sufficient control for the user's environment. To assign a TACACS+ user a higher role from the default-user group role:

1. On the TPS device, create a local user that uses the same name as the TACACS user.
2. Assign that local TPS user to a user group. The TPS device references that user group to determine the authorization level of the TACACS user.

Note

Because authentication is through the TACACS+ server, do not create a password for the local TPS user.

This differs from RADIUS authorization; for that, TPS devices can use the filter ID returned from the RADIUS server during user authentication to determine a RADIUS user role. If the RADIUS server does not return the filter ID, the TPS device uses the RADIUS default-user group configuration to determine the user role.

Although user authentication is performed on the TACACS+ server, user authorizations and access rights are maintained on the SMS server. If the TACACS+ server is unavailable, the SMS can authenticate local users. The SMS does not permit you to manage SMS user accounts on the TACACS+

server; the account password for a TACACS+ authenticated user must be changed on the TACACS+ server.

Edit the TACACS+ server configuration

Procedure

1. On the Authentication screen, select the TACACS+ tab on the Authentication Configuration panel.
2. Click **Edit** to the right of the Primary TACACS+ Server panel.
3. In the dialog, configure the TACACS+ server options described in the following table.

Setting	Description
IP Address / Hostname	IP address or hostname of the TACACS+ server. The IP Address field can contain an IPv4, IPv6, or named IP address. The Hostname field can contain an unqualified hostname or a fully qualified hostname (hostname+domain name).
Port	Port on the TACACS+ server that listens for authentication requests; the default is port 49.
Authentication Protocol	Authentication method used on the TACACS+ server: • ASCII • PAP (default) • CHAP • MSCHAP (supported with IPS devices only)
Secret/Confirm Secret	Case-sensitive string used to encrypt and sign packets between TACACS+ clients and the TACACS+ server, set in the TACACS+ client configuration file. Maximum is 63 characters.
Timeout	Timeout, in seconds, for communication with the TACACS+ server. Default is 15.
Attempts	Number of times, between 1 and 10, communication with the TACACS + server is attempted. Default is 3 attempts.

4. Test the TACACS+ configuration by entering a valid User Name and Password for the server, and then clicking **Test**.
5. Click **OK** to save the server configuration.
6. If a TACACS+ server is already configured, click **Reset** to the right of the TACACS+ Server panel to delete that configuration.

   If the configuration you reset is the last configured TACACS+ server, and if TACACS+ is the current authentication choice, then the SMS changes the current authentication source to Local.

What to do next

You can also change the configuration of TACACS+ servers by selecting **Devices > *device-name* > Authentication > TACACS+ Groups > Edit > TACACS+ Servers > Edit**.

Configure CAC authentication

Common Access Card (CAC) authentication enables you to secure SMS client access by using two-factor authentication, which is more secure than the standard username and password authentication.

CAC AUTHENTICATION ON THE SMS	DESCRIPTION
ActivClient software	ActivClient extracts certificate information from the CAC that the SMS uses to authenticate users. ActivClient interacts with identification tokens, certificate authorities, and smart card readers.
Certificate management	PKI certificates come from an approved Certificate Authority (CA) and are used to verify and authenticate the card holder. Select **Admin** > **Certificate Management** > **CA Certificates** to import, replace, and view certificate details.

CAC AUTHENTICATION ON THE SMS	DESCRIPTION
CAC authentication	When CAC authentication is enabled on the SMS: • All users must use their CAC to log in to the SMS client. • Users will not be able to access the SMS Web client. • The SMS will not allow an administrator to designate user accounts to be authenticated locally (local authentication). Select **Admin** > **Authentication and Authorization** > **Authentication** to select the authentication source that the SMS will use to authenticate users.
Managing user roles and user accounts	The SMS uses capabilities and roles to give users permissions to perform specific actions. Select **Admin** > **Authentication and Authorization** > **Roles** to set the capabilities for each role. Users with enabled access to the SMS CLI capability can log in from the SMS CLI to disable CAC authentication, which sets the SMS back to the default authentication method (local authentication). Select **Edit/Create Role** > **Capabilities** > **Admin** > **SMS Management** > **Access Management** > **Access SMS CLI** to expand or limit this capability.

Prerequisites

All SMS client workstations that are enabled with CAC authentication source require ActivClient software, a Windows compatible smart card reader, and the common access card (CAC). ActivClient must already be installed and configured before you can configure CAC authentication on the SMS. ActivClient is supported on the following Windows operating systems.

WINDOWS OPERATING SYSTEM	ACTIVCLIENT VERSION
Windows 7 (32- and 64-bit)	ActivClient 6.2 or ActivClient 7.0.2
Windows 8 (32- and 64-bit)	ActivClient 6.2 or ActivClient 7.0.2
Windows 10 (32- and 64-bit)	ActivClient 6.2 or ActivClient 7.0.2

Windows operating system	ActivClient version
Windows 11 (32- and 64-bit)	ActivClient 7.4 (recommended)

Perform the following tasks before you configure CAC authentication on the SMS:

Procedure

1. Install the ActivClient software. For additional details, refer to the ActivClient documentation.
2. Install the SMS client.
3. Verify the SMS client references the ActivClient DLL.

   Go to the location where you installed the SMS client, expand the `config` folder, and then open the `cac.properties` file.

   The file contains name, library, and description details, and the path is similar in format to the following:

   ```
   library="C:/Program Files/ActivIdentity/ActivClient/
   acpkcs211.dll"
   ```

   Note

   If the `cac.properties` file is not available under the SMS client program files, make sure you have installed ActivClient and either install the software again or refer to the ActivClient documentation.

Import CA Certificates

Certificates come from an approved Certificate Authority (CA) and are used to validate the CAC certificate when the card holder attempts to log in to the SMS.

Procedure

1. Select **Admin** > **Certificate Management** > **CA Certificates**.

2. Click **Import** and then do the following:
   a. Enter a name for the certificate in the **Certificate Name** field.
   b. Click **Browse** and then browse to and select the certificate.
   c. Select the certificate format according to the certificate file.
   d. Click **OK.**
3. Repeat Steps 1-3 for all Root and Intermediate certificates that are used in the chain of validation.

Configure the Active Directory server for CAC authentication

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Authentication**.
2. Click the **CAC** tab.
3. Click **Edit** under Active Directory Server Configuration.
4. In the dialog, configure the Active Directory server options described in the following table.

Setting	Description
Server Address	Fully qualified host name or IP address of the Active Directory server.
Enable SSL	Select **Using LDAPS** to enable Lightweight Directory Access Protocol (LDAP) over SSL. If enabled, you must also import an Active Directory SSL certificate. See *Configure Active Directory authentication on page 8-24*.
Port	The port on the Active Directory server that listens for authentication requests. The default non-SSL port is 389; if SSL is enabled, the default port is 636.
Timeout	Timeout, in seconds, for communication with the Active Directory server; the default value is 30 seconds.

Setting	Description
Admin Name	Identifies the account on the Active Directory server that is permitted to search the LDAP directory within the defined search base. This is the bind user on the Active Directory server that enables the SMS to query the LDAP directory and authenticate users. `Example: Administrator@DOMAINNAME`
Admin Password	Active Directory server administrative password.
User Search Base	Top-level distinguished name in the Active Directory hierarchical structure where the user search is done. Examples include `DC=adomain`, `DC=example`, and `DC=com`
User Search Attribute	Attribute to use when searching for user login names.
Username Display Attribute	The display name used on the SMS.
Group Search Base	Top-level distinguished name in the Active Directory hierarchical structure where the group search is done.
Group Name Attribute	The attribute to use when searching for group names.

5. Test the Active Directory configuration, enter the Admin Password for the server, and then click **Test**.
6. Click **OK**.

Enable CAC authentication

After you import the CA Certificates and set up the Active Directory server configuration, you can configure the SMS to authenticate user login requests using CAC authentication.

When CAC authentication is enabled on the SMS, keep in mind:

- All users must use their CAC to log in to the SMS client.

- Users will not be able to access the SMS Web client. If a user backs up the SMS database, the backup will not be available on the Web client, but it will be available on the SMS at **Admin** > **Database** > **Backup**.

Procedure

1. Go to **Admin** > **Authentication and Authorization** > **Authentication**.
2. Under Authentication Source, click **Edit**.
3. Select **Use CAC Authentication**.

   Note

   The SMS will not allow an administrator to designate user accounts to be authenticated locally (Local Authentication). However, users (with SMS CLI role capabilities) can log in to the SMS command line interface (CLI) to disable CAC authentication. Disabling CAC authentication sets the SMS back to the default authentication method (Local Authentication).

4. Click **OK**.
5. To enforce CAC authentication, do the following:
   a. Attach the USB card reader to the SMS client workstation.
   b. Log out of the SMS client.

Log in to the SMS using CAC authentication

Authentication is performed on the SMS server using Certificate Authority (CA) certificates and one or more ActivClient smart card readers. If there are multiple card readers with multiple cards inserted, a dialog box is displayed that enables you to select between card readers when you attempt to log in (**Menu > File > Login**) or during session unlocks. Users are then validated against their Active Directory accounts. The SMS matches a user's group in Active Directory with a group on the SMS to determine the user's privileges.

If the SMS is in CAC Authentication mode, all SMS users must log in using CAC. No local users are allowed to log into the SMS client.

Procedure

1. Insert your Common Access Card (CAC) into the card reader.
2. Type the IP address in the **SMS Server** field.
3. Select the appropriate certificate from **Certificates** drop-down list.
4. Click **Login**.

Create or edit a user account

User account administration includes user roles and correlating group assignments, password requirements, and user ID requirements. The tasks users are required to perform on the SMS must have access privileges and permissions defined in the group(s) to which the user account is assigned.

The user inherits the access permissions and user role capabilities defined for an assigned group.

You can delete users whose accounts are enabled or disabled. If you delete a user that has an active session, the user will be deleted but the active session will remain until the user logs off or the session is ended.

Procedure

1. Go to **Admin** > **Authentication and Authorization** > **Users**.
2. Click **New**, or select an existing user account and click **Edit**.
3. Select **Authentication**, and provide the following:

SELECT:	TO ...
Enabled	Enable or disable the user account.
User Id	Enter a username. • Must be 1 to 150 characters in length. • Cannot contain a space. • Cannot contain a backslash.

SELECT:	TO ...
Password	Enter and confirm the password for the user account that adheres to the guidelines set by the security level. The SMS enforces secure access through security policies that are specified by the security level set in the system preferences. Learn more: *Security on page 11-2*. To change a user password, you must either be logged in as the user whose password you want to change or be logged in with SuperUser capabilities. You cannot change Active Directory user account passwords on the SMS. For an AD account used to log on to the SMS, you must change the password on the Active Directory server.
Password Expiration	Enable or disable an expiration date for the user account password. If enabled, specify the number of days (1-365).
Change password on next login	Require the user to change their password the next time that they log in.
Local Authentication Only	Force the user to authenticate using the local authentication source rather than any remote authentication source. Learn more: *Authentication source on page 8-19*.
Regenerate API Key	Generate or regenerate the API key used to access the SMS web API. API keys are long-lasting keys that users can store securely. Learn more: *Generate the API key on page 8-52*.

4. Select **Group Membership**, and assign a group to the account:
   - Click **Add** and select the group(s) to assign to the account. By default, the first group assigned to the user account becomes its New Resource Group.
   - If you assign multiple groups to a user, then you can designate any one of them as New Resource Group. Select the group, and click **Set Resource Group**.
5. Select **Contact Details**, and provide the following:
   - Contact name
   - Email address

- Phone number
- Cell phone number

6. Click **OK**.

User roles and capabilities

User roles and capabilities give users permissions to perform specific actions within the SMS. A *capability* is an ability to affect an object in the system; for example, the ability to add a device. A *role* is a collection of capabilities.

The SMS has three user roles that grant distinct privileges to different functions on the SMS. The user roles are the operator, admin, and superuser.

- Operator — Read-only capabilities including running reports/queries, viewing configuration settings, inspection events, and audit data.
- Admin — Management of basic configuration settings including report management, profile management, and general device management.
- Superuser — All other system functionality including management of advanced configuration settings, responder configuration, device configuration, and authentication and authorization.

User roles have hierarchical permissions; the admin role has all operator privileges, the superuser role has all admin privileges. You cannot modify predefined system roles, but you can use them as starting points to initialize new roles. When you create a role, you can select a base system role from which to initialize the new role. The new role is given the same capabilities as the system role it is initialized from, until you customize the capabilities.

Events

Permissions for Events are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
Event management: Edit event comments and export query results.		x	x

Capability	Operator	Admin	Superuser
Saved query management: Save, save as, and delete.		x	x
View saved packet trace.		x	x
URL forwarding management.			x

Reports

Permissions for Reports are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
Run report.	x	x	x
Saved report management: Save, save as, and delete report.		x	x
Results and schedule management.		x	x
Report logos management: Upload report logo and delete report logo.			x

Profiles

Permissions for Profiles are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
Profile search management: Create, edit, or delete query.	x	x	x
Auxiliary Digital Vaccine package management: Import, active and de-activate, distribute, uninstall, delete Auxiliary Digital Vaccine packages, and edit Auxiliary Digital Vaccine auto activate settings.		x	x

Capability	Operator	Admin	Superuser
Digital Vaccine Toolkit management: Import, activate and de-activate, distribute, uninstall, and delete Digital Vaccine Toolkit packages.		x	x
Digital Vaccine management: Import, download, activate, distribute, delete Digital Vaccines, and edit Digital Vaccine auto activate settings.		x	x
Extended device management: VPN profile management.		x	x
Profile management: Create, edit, delete, export, distribute profile, edit or lock category settings, and manage application groups.		x	x
Exception management (attack filter exceptions, attack filter restrictions, Reputation filter exceptions, and performance filter exceptions): create, edit, lock, and delete.		x	x
Profile filter management: Edit filter and lock filters.		x	x
Advanced DDoS filter management: Create, edit, lock, and delete Advanced DDoS filters.		x	x
Filter exception management: Create, edit, and delete filter exceptions.		x	x
Reputation filter management: Create, edit, lock, reorder, delete Reputation filters, and modify Reputation filter settings.		x	x
SSL filter management: Create, edit, lock, and delete SSL filters.		x	x
Traffic management filter management: Create, edit, lock, reorder, and delete Traffic Management filters.		x	x
Snapshot management: Create, activate, edit, and delete snapshots.		x	x

Capability	Operator	Admin	Superuser
Share settings management: View or manage named services and SSL server management.		x	x
Action set management: Create, edit, and delete action sets.		x	x
Contact management: Create, edit, and delete contacts.		x	x
Vulnerability scan management: Import vulnerability scans.		x	x
Reputation management: Create, update, and delete (delete all) local Reputation entry.			x
Create, edit, or delete Reputation tag category.			x
Import or export local Reputation database, and import or export Reputation dictionary.			x
Reputation database summary distribution and synchronization, and Reputation service management.			x

Responder

Permissions for Responder are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
View responder settings configuration.	x	x	x
Action management: Create, edit, or delete action. Create, export, or delete action type.			x
Netident management: Create, edit, or delete mapping. Create, edit, reorder, or delete netident web service.			x
Policy management: Create, edit, and delete policy.			x

Capability	Operator	Admin	Superuser
RADIUS management: RADIUS proxy management.			x
Responder device management: Discover, create, edit, or delete device. Create, delete, or export device type.			x
Responder management: Create and close active response.			x

Devices

Permissions for Devices are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
Device management: remote login as the **Operator** user.	x		
Device network management: View traffic capture.	x	x	x
Event management: View status, device health, audit logs, or system logs.	x	x	x
General device management: View configurations, DDoS settings, and snapshots.	x	x	x
Device management: Remote login as the **Admin** user.		x	
Device network management: Manage traffic capture.		x	x
Event management: Ability to clear adaptive filter states, blocked IP addresses, trusted streams, rate limited streams, and blocked streams.		x	x

Capability	Operator	Admin	Superuser
Edit device health, flush or re-sync identity sessions or user groups, quarantine management, and view SSL or VPN logs.		x	x
General device management: Manage DDoS settings and snapshots, and VLAN manager.		x	x
Configuration management: Ability to edit: • Adaptive Filter Configuration (AFC) • Global SSL • HA • Host IP filters • NAT • NMS • Servers • TSE • Authentication preferences • Performance protection • Remote syslog • Services • Time • sFlow management configurations		x	x
High privilege management: Identity configuration.		x	x
Manage X-series devices.		x	x

Capability	Operator	Admin	Superuser
NGFW/TPS device management of: • ARP/NDP configuration • DHCP configuration • DNS host and proxy cache configuration • Captive portal settings • Device high availability • Network interfaces and segments • Route configuration • VPN configuration • X509 certificate configuration **Note** You must select these capabilities to manage a TPS device on the SMS.		x	x
Segment group membership: Distribute to a segment group and manage segment groups.		x	x
TOS management: Delete previous TOS versions, roll back TOS, and manage TOS.		x	x
Device group/stack management: Manage device group or stack structure.			x
Device management: Export configuration and remote login as the superuser.			x
Device network management: Ability to manage ports, segments, inspection bypass rules, and Core Controller.			x
Configuration management: Ability to edit management information, management routes, and security configurations.			x

Capability	Operator	Admin	Superuser
High privilege management: Ability to edit permissions, permissions for segment groups, FIPS management, Intrinsic HA, and virtual segment manager.			x
High privilege device management of : • Add • Manage • Unmanage • Replace • Reboot • Delete device • Manage device users • Install certificate • Reset IPS filters • Distribution queue manager			x
Log management: Ability to reset audit, block, misuse, quarantine, device reset alert, and system logs. Reset packet stats and traces.			x

Admin

Permissions for Admin are granted to each user role, as described in the following table.

Capability	Operator	Admin	Superuser
Access management: Access SMS UI.	x	x	x
Administer the logs of the SMS: Read system log.	x	x	x
Authentication and authorization administration: View authorization settings.	x	x	x
Certificate management: View X509 certificates.	x	x	x

Capability	Operator	Admin	Superuser
Database management: View database information.	x	x	x
General SMS management: Ability to view general management, Geo Locator, and IP address ID settings.	x	x	x
High Availability: View HA settings.	x	x	x
ID Resolver: View ID Resolver.	x	x	x
NAT network management: Ability to view NAT and network settings.	x	x	x
SNMP user management: View SNMP settings.	x	x	x
Status management: View port and system health.	x	x	x
View and customize the dashboard.	x	x	x
Export archive management: Read export list.		x	x
Named resource management: View email address groups, named IP addresses, and named VLAN IDs.		x	x
Access management: SMS CLI and SMS web services.			x
Administer the SMS: Access diagnostics, access or manage preferences, and reboot or shutdown the SMS.			x
Administer the logs of the SMS: Read audit log.			x
Authentication and authorization administration: Manage authorization settings and manage and view groups or roles.			x
User management: Manage own resource groups, terminate user sessions, user record management, view other users, and view user sessions.			x

Capability	Operator	Admin	Superuser
Certificate management: SMS certificate key, Web certificate, X509 certificate, and X509 certificate private key.			x
Database management: Manage, backup, or restore database, view backup database information, edit external database information, and clean, edit, or reset database tables.			x
Export archive management: export and delete export archive.			x
General SMS management: Edit services or system information, enable `IpaddrId` settings, manage and view Geo Locator settings, FIPS manager, manage and view IP address IDs and settings, remote Syslog management, TLS management, and view general management settings.			x
High Availability: Configure or manage HA.			x
ID Resolver: Manage ID Resolver.			x
IP address identifier lookups: DNS, Geo, Meta, NR, Rep, UserId, and WhoIs.			x
NAT network management: NAT and network management.			x
Named resource management: Edit email addresses, named IP addresses, named VLAN IDs.			x
SNMP user management: SNMP request settings and SNMP traps.			x
Software administration: Manage software, entitlements, and patches.			x
User ID IP Correlation: Edit User ID IP correlation, Identity Agents, and agent groups.			x

Create or edit a user role

User roles and capabilities give users permissions to perform specific actions within the SMS. A *capability* is an ability to affect an object in the system; for example, the ability to add a device. A *role* is a collection of capabilities.

The SMS uses three predefined roles: **SuperUser**, **Admin**, and **Operator**. You cannot modify predefined system roles, but you can use them as starting points to initialize new roles. When you create a role, you can select a base system role from which to initialize the new role. The new role is given the same capabilities as the system role it is initialized from, until you customize the capabilities. The SuperUser role includes all Admin and Operator capabilities.

You can create new roles to expand or limit the capabilities of existing roles or to target a specific set of capabilities for a group of SMS users. You can further control the access rights and capabilities of users through Groups, but you cannot delete a role when it is in use by a Resource Group. Learn more: *Create or edit a user group on page 8-50*.

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Roles**.
2. Click **New**, or select an existing role and click **Edit**.

Note

When you edit a user role, you can change the base system role that the SMS uses to determine what to do during an SMS upgrade. For example, if you created a user role based on the Admin system role, but you do not want this role automatically updated with new Admin role capabilities during an upgrade, you can change the value for the **Upgrade As** field to "None."

You can copy a system role by selecting it in the User Roles list and clicking **Save As**.

---

3. Select **Name & Description**, and provide the following:

- Role name
- Role description
- Initialize from system role – SuperUser, Admin, Operator, or None (no capabilities are preselected).

4. Select **Capabilities**, select a functional area on the SMS (**Events**, **Reports**, **Profiles**, **Responder**, **Devices**, or **Admin**), and then select the capabilities you want to assign to the role using the following options:
   - **Global capabilities for a functional area:** Select the top-level list item, so that a checkmark appears to the left of every capability in the list.
   - **Group capabilities:** Select a parent list item, so that a checkmark appears to the left of every capability under that parent.
   - **Named capabilities:** Select an individual named capability from the list. If you select a single capability, consider that one capability may depend on others for full access rights to complete a task. Capabilities are listed hierarchically in groups; child capabilities are required for that particular group function.
5. Click **Finish**.

   If a user role was initialized from a system role, the specified system role determines how the user role is affected during an SMS upgrade. Capabilities that were added for a new SMS release are added to this role based on the system role specified.

Create or edit a user group

User groups align user capabilities with functional areas on the SMS. A *user group* pairs a *role* with resources that group members can access.

The SMS uses one predefined group named superuser. This group includes the superuser role, and provides access to all SMS features and functionality. Give careful scrutiny before you assign users to this group. In a typical new installation, you must create a new user group to specify access rights for users who do not have superuser privileges.

Any user account that logs on to the SMS must be assigned to at least one user group, because a user account must have a New Resource Group.

Procedure

1. Select **Admin** > **Authentication and Authorization** > **Groups**.
2. Click **New**, or select an existing user group and click **Edit**.
3. Select **Name & Description**, and provide the following:
   - Group name
   - Role – Select an existing role, create a new role, or select a role and edit the role capabilities. The role assigned to a group specifies the rights to execute the capabilities to manage the group resources, such as devices and profiles. When you assign a role, keep in mind that you cannot modify predefined system roles. If you edit role capabilities for a user role, changes are saved to the role, not just to the group. Learn more: *Create or edit a user role on page 8-49*.
   - Group description
4. Select **Devices** to define the list of devices, device groups, and stacks the user will have permission to access.
5. Select **Segment Groups** to define the list of segment groups the user will have permission to access.
6. Select **Profiles** to define the list of profiles the user will have permission to access.
7. Select **DV Toolkit Packages** to define the list of DV Toolkit packages the user will have permission to access.
8. Select **Action Sets** to define the list of action sets the user will have permission to access.
9. Select **Reports** to define the list of reports the user will have permission to access.
10. Select **SSL Servers** to define the list of SSL servers the user will have permission to access.

11. Select **SSL Client Proxies** to define the list of SSL client proxies the user will have permission to access.
12. Select **SSL Client Decryption Rules** to specify which SSL client decryption rules the user will have permission to access.
13. Select **Active Directory Group Mapping** if Active Directory authentication is configured for the SMS, users may be authorized through a mapped AD group.
    - Map this group to the same named group in active directory.
    - Map this group to a specific active directory group, and then specify the group name by entering the user group without entering the fully qualified distinguished name. Click **Test** to test the mapping.
14. Select **RADIUS Group Mapping** if RADIUS authentication is configured for the SMS, users may be authorized through a mapped RADIUS group.
    - Map this group to the same named group in RADIUS.
    - Map this group to a specific RADIUS group, and then specify the group name by entering the user group without entering the fully qualified distinguished name.
15. Click **Finish**.

Generate the API key

The API key is an alternative way for users to access the SMS Web API without having to authenticate with a username and password. You can use the API key as part of the header for HTTP requests. Include the `X-SMS-API-KEY` header in addition to the API Key. You can generate the API key for a local SMS user account.

Procedure

1. Verify that the role for the selected user account has the `Access SMS Web Services` capability enabled. Learn more: *Create or edit a user role on page 8-49*.

2. Select **Admin** > **Authentication and Authorization** > **Users**.
3. Select the user account, and click **Edit**.
4. Click **Regenerate API Key** to get a new API key. You can reset the API key for any reason. But when you do, from this point, the previous API key can no longer be used.

Certificate Management

Certificate management enables the SMS to maintain a central repository from which certificates and private keys are automatically distributed to the appropriate TippingPoint devices. Unlike previous releases, you no longer need to load the certificates and private keys onto each device. Instead, import your certificates and private keys into the SMS, and update the device configuration to assign the appropriate certificates.

Certificate Management provides general X.509 certificates management on the SMS and its managed devices using the following:

- *The SMS certificate password on page 8-53*
- *Certificates on page 8-56*
- *Certificate Authority (CA) certificates on page 8-62*
- *Revocation on page 8-65*
- *Certificate Signing Requests (CSRs) on page 8-67*

Manage the SMS certificate password

The SMS certificate password protects the private keys in the SMS certificate repository with encryption. The SMS encrypts the private keys using a randomly generated 2048-bit RSA key pair. The private key of this key pair is encrypted using a 256-bit AES cipher based on your SMS certificate password.

Setting up the SMS certificate password is required when you import private keys into the SMS certificate repository.

Note

Managing the SMS certificate password requires the **Admin Certificate Management** capability in your user role.

Private key encryption status

Status	What it means
Unused	There are no private keys in the SMS certificate repository. You can set up the SMS certificate password without importing private keys.
Setup Required	There are private keys pending to be in the SMS certificate repository. Click **Setup Encryption** to set up the SMS certificate password to import private keys.
Password Required	Enter the SMS certificate password to manage certificates with private keys and export them to devices. Go to **Admin** > **Certificate Management** > **Enter Password**.

Set up encryption

Once you set up the SMS certificate password, keep in mind:

- The SMS does not store the SMS certificate password. You must enter this password every time the SMS server restarts.
- There is no way to recover a lost password. If you lose your password, you must reset your password. Resetting the SMS certificate password deletes all of the private keys in the SMS certificate repository, which breaks the corresponding certificates. To repair the broken certificates, re-import your private keys.

Procedure

1. Go to **Admin** > **Certificate Management**.
2. Click **Setup Encryption**.
3. Provide a password in the password and the confirm fields.

4. Click **OK**.

   A new RSA key pair is generated after password validation. The new password encrypts the private key of this key pair which encrypts your private keys in your SMS certificate repository.

Change the certificate password

Change the SMS certificate password to update the password that secures the SMS certificate repository.

Changing the certificate password requires the current SMS certificate password.

Note

Changing the certificate password requires the **Admin Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management**.
2. Click **Change Password**.

   Provide the current password and a new password in the Change SMS Certificate Password dialog.

3. Click **OK**.

Reset the certificate password

Reset the SMS certificate password to delete the private keys in the SMS certificate repository and create a new SMS certificate password. Resetting the SMS certificate password is only necessary when you have lost the SMS certificate password.

If you want to change the SMS certificate password, we recommend that you do not reset the certificate password. Resetting the SMS certificate password breaks the corresponding server certificates for:

- SSL inspection
- SMS web server

A broken certificate cannot be used until it is repaired. For information about repairing a broken certificate, see *Repair a certificate on page 8-60*.

To avoid losing any pending CSRs created by the SMS, we recommend resetting the SMS certificate password after you import the corresponding CA certificate and public key. After the SMS certificate password is reset, the SMS cannot associate the CSR private key in the certificate repository with the new CA certificate and public key.

Note

Resetting the certificate password requires the **Admin Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management**.
2. Click **Reset**.

   Provide a new password in the Reset SMS Certificate Password dialogue.
3. Click **OK**.

View certificates

The Certificates table lists the server certificates in the SMS certificate repository. Right-click the certificate and select **Show Usage** to view certificate usage.

The following table describes the fields in the Certificates table.

Important

The SMS does not notify you when a certificate is about to expire. Use the Certificates table to verify that the certificates are up-to-date and avoid expired certificate errors.

Field	Description
Name	An icon with the private key status and a unique identifier for the certificate. Hover over this column to view data from the certificate.
Issued To	The Subject Common Name (CN).
Issued By	The Issuer Common Name (CN).
Status	An icon with verification status and the state of the certificate.
Expires On	The date and time of the expiration of the certificate.
Private Key	One of the following: • Checkmark – The certificate has a private key. • Empty circle – The certificate does not have a private key. • Broken – The certificate is missing its private key after an SMS certificate password reset. Repair the certificate by reimporting the private key.
Exportable	One of the following: • Checkmark – The certificate and the private key can be exported. • Empty circle – The private key cannot be exported. • N/A – There is no private key associated with the certificate.

Import a certificate

Importing a certificate to the SMS certificate repository makes that certificate available to the SMS and all managed devices for:

- SSL inspection.
- SMS web server.
- Captive portals.

Note

Importing certificates requires the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **Certificates**.
2. Click **Import**.
3. Provide a unique certificate name to reference a PEM/DER certificate or a unique base name for PKCS12 certificates in the **Certificate Name** field.
4. Browse to and open a certificate in the **Certificate File** field.
5. Select the file format of the certificate.
   - PEM/DER format allows optional private key file import. Browse to and open the associated private key. If the private key is encrypted, enter the appropriate password in the Password field.
   - PKCS12 format imports multiple certificates with or without private keys. If the private keys are encrypted, enter the appropriate password in the Password field.
6. Check **Private Key Export** to enable private key export from the SMS, and include private keys in the SMS backup.

   Disabling private key export cannot be undone. If necessary, you can disable private key export later by right-clicking the certificate in the Certificates table and selecting **Make Non-Exportable**.
7. Click **OK**. The certificate appears in the Certificates table.

Export a certificate

Exportable certificates and their associated private keys can be written to a file for external use.

Note

Exporting a certificate and a key to a file requires the **Admin X509 Certificate Private Key Management** capability in your user role and the SMS certificate password.

Procedure

1. Go to **Admin** > **Certificate Management** > **Certificates**.
2. Click **Export**.
3. Select a file format for your certificate, private key, or both.

   You can enter an optional password to encrypt `.p12` or `.key` files.
4. Specify the file name and location under Export To File.
5. Click **OK**.

Replace a certificate

Replace a certificate with a new one, for example, when you have certificates which have expired or will expire soon. When you replace a certificate, the SMS certificate repository automatically updates managed devices with the new certificate.

Simply adding the new certificate and deleting the old one would require you to also update any configuration settings to use the new certificate. Replacing the certificate changes the certificate while preserving any existing references in these configuration settings.

When replacing a certificate, consider the following:

- A certificate with a private key must be replaced by another certificate with a private key.
- A certificate without a private key must be replaced by another certificate without a private key.
- The replacement certificate is not already in the SMS certificate repository.
- You must have the **Device X509 Certification Configuration** capability in your user role for all of the devices where the certificate is replaced.
- All devices with the certificate must be managed by the SMS at the time of replacement. If the SMS cannot communicate with all of the devices with the certificate, the SMS displays an error message.

Note

Replacing certificates requires the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. To replace certificates, go to **Admin** > **Certificate Management** > **Certificates**. To replace CA certificates, go to **Admin** > **Certificate Management** > **CA Certificates**.
2. Click **Replace**.
   - For certificates with a private key, browse to and open a certificate. For PEM/DER certificates, browse to and open the associated private key. (Optional) Provide a password to encrypt the private key.
   - For certificates without a private key or CA certificates, browse to and open a certificate. Private keys in PKCS12 files are ignored. Select the file format of the certificate.
3. Click **OK**.

   The replaced certificate is saved under the original name with `_REPLACED` appended. The new certificate replaces the old certificate on the corresponding devices and the SMS.

Repair a certificate

Repair a broken server certificate to re-import its private key into the SMS certificate repository. Repairing a certificate is necessary, for example, when you reset the SMS certificate password, or when you restore a backup which does not include private keys.

Procedure

1. Go to **Admin** > **Certificate Management** > **Certificates**.
2. Right-click the broken certificate and select **Repair**.

3. Browse to and open the corresponding private key file.
4. Select the file format of the private key.
5. (Optional) Provide a password to encrypt the private key.
6. Click **OK**.

   The new private key is copied to the private key file of the broken certificate.

Make a private key non-exportable

Make a private key non-exportable to disable private key export from the SMS, and if the SMS backup is configured to include private keys, exclude the private key from the SMS backup. This command is useful for securing a private key that was imported into the SMS without disabling private key export.

To make a private key exportable after you make it non-exportable, you must delete the corresponding certificate and private key and then re-import the certificate and private key.

Note

Making a private key non-exportable requires the **Admin X509 Certificate Private Key Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **Certificates**.
2. In the Certificates table, right-click a certificate with an Exportable private key and click **Make Non-Exportable**.

Delete a certificate

Delete a certificate to remove it from the SMS certificate repository and any managed devices. If the certificate is in use by the SMS or a managed device, you cannot delete it.

Note that to make a private key exportable after you make it non-exportable, you must delete the corresponding certificate and private key, and then reimport the certificate and private key.

Note

Deleting a private key requires the **Admin X509 Certificate Private Key Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **Certificates**.
2. In the Certificates table, right-click a certificate and click **Delete**.

View Certificate Authority (CA) certificates

The CA Certificates table lists the CA certificates in the SMS certificate repository. CA certificates are issued by a CA and do not have private keys. Right-click the CA certificate and select **Show Usage** to view CA certificate usage.

The following table describes the fields in the CA Certificates table.

Field	Description
Name	An icon with the type of the CA certificate and a unique identifier for the CA certificate. Hover over this column to view data from the CA certificate.
Issued To	The Subject Common Name (CN).
Issued By	The Issuer Common Name (CN).
Status	An icon with verification status and the state of the CA certificate.
Expires on	The date and time of the expiration of the CA certificate.

Import a CA certificate

Importing a CA certificate to the SMS certificate repository makes that CA certificate available to the SMS and all managed devices for:

- Radius authentication (SMS and device)
- LDAP authentication (SMS)
- VPN configuration
- Remote syslog

Note

Importing CA certificates requires the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **CA Certificates**.
2. Click **Import**.
3. Provide a unique certificate name to reference a PEM/DER certificate or a unique base name for PKCS12 certificates in the Certificate Name field.
4. Browse to and open a CA certificate in the Certificate File field.
5. Select the file format of the CA certificate.
6. Click **OK**. The certificate appears in the CA Certificates table.

Export a CA certificate

CA certificates can be written to a file for external use.

Note

Exporting a CA certificate requires the **Admin X509 Certificate Private Key Management** capability in your user role and the SMS certificate password.

Procedure

1. Go to **Admin** > **Certificate Management** > **CA Certificates**.

2. Click **Export**.
3. Select a file format for your CA certificate.

   You can enter an optional password to encrypt `.p12` files.
4. Specify the file name and location under Export To File.
5. Click **OK**.

Replace a CA certificate

Replace a certificate with a new one, for example, when you have certificates which have expired or will expire soon. When you replace a certificate, the SMS certificate repository automatically updates managed devices with the new certificate.

Simply adding the new certificate and deleting the old one would require you to also update any configuration settings to use the new certificate. Replacing the certificate changes the certificate while preserving any existing references in these configuration settings.

When replacing a certificate, consider the following:

- The replacement certificate is not already in the SMS certificate repository.
- You must have the **Device X509 Certification Configuration** capability in your user role for all of the devices where the certificate is replaced.
- All devices with the certificate must be managed by the SMS at the time of replacement. If the SMS cannot communicate with all of the devices with the certificate, the SMS displays an error message.

Note

Replacing certificates requires the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. To replace certificates, go to **Admin** > **Certificate Management** > **Certificates**. To replace CA certificates, go to **Admin** > **Certificate Management** > **CA Certificates**.
2. Click **Replace**.
   - For certificates with a private key, browse to and open a certificate. For PEM/DER certificates, browse to and open the associated private key. (Optional) Provide a password to encrypt the private key.
   - For certificates without a private key or CA certificates, browse to and open a certificate. Private keys in PKCS12 files are ignored. Select the file format of the certificate.
3. Click **OK**.

   The replaced certificate is saved under the original name with `_REPLACED` appended. The new certificate replaces the old certificate on the corresponding devices and the SMS.

Manage revocation

Revocation in Certificate Management verifies the certificates issued by the CA certificates in the SMS certificate repository. You can specify Online Certificate Status Protocol (OCSP) settings and Certificate Revocation List (CRL) locations for each CA certificate.

View Online Certificate Status Protocol (OCSP) settings

The OCSP Settings table lists the OCSP settings in the SMS. You can specify one OCSP setting per CA certificate.

The following table describes the fields in the OCSP Settings table.

Field	Description
Certificate Authority	The name of the CA certificate using the specified OCSP setting.

Field	Description
OCSP URI	The URI to the OCSP with revocation information.

Specify an OCSP setting

You can specify an OCSP URI that overrides the OCSP URI defined in the CA certificate.

Note

Specifying, editing, and deleting an OCSP setting require the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **Revocation**.
2. Click **New** under OCSP Settings.
3. Choose a Certificate Authority.
4. Specify an OCSP URI for the chosen CA certificate.

View Certificate Revocation Lists (CRLs)

The Certificate Revocation Lists table lists the configured CRLs in the SMS. A CRL contains a list of revoked certificates. You can configure one CRL location per CA certificate.

The following table describes the fields in the Certificate Revocation Lists table.

Field	Description
Certificate Authority	Name of the CA certificate with the configured CRL.
Source	File location or the URL of the CRL.

Field	Description
Entries	Number of the certificates revoked by the CRL.
Status	State of the CRL.
Published	Date and time of the publication of the CRL.
Next Publish	Date and time of when the CRL will publish next.
Last Update	Date and time of when the CRL updated on the SMS.

Configure a CRL location

You can specify a CRL location that overrides the CRL location defined in the CA certificate.

Note

Configuring, editing, and deleting a CRL requires the **Admin X509 Certificate Management** capability in your user role.

Procedure

1. Go to **Admin** > **Certificate Management** > **Revocation**.
2. Click **New** under Certificate Revocation Lists.
3. Choose a Certificate Authority.
4. Specify a Distribution Point URL or browse to and open a Local CRL File.
5. Click **OK**.

View signing requests

The Signing Requests table lists the Certificate Signing Requests (CSRs) in the SMS. A CSR contains information that identifies the requestor.

To request a signed certificate with a CSR and use it in the SMS,

1. *Create a CSR on page 8-68*.

2. *Export a CSR on page 8-70*
3. Send the exported CSR to a CA. The CA signs the CSR and sends back a certificate.
4. *Import the certificate on page 8-70*.

The following table describes the fields in the Signing Requests table.

Field	Description
Name	Name of the certificate request.
Common Name (CN)	CN stored in the CSR.
Requestor	RFC822 name stored in the CSR.
Signing Certificate	One of the following: • Check mark – The CSR has the key certificate sign bit set in the key usage extension. The "Make it a signing certificate" box is checked in the request. • Empty circle – The CSR does not have the key certificate sign bit set in the key usage extension. The "Make it a signing certificate" box is unchecked in the request.
Key Size (bits)	Number of bits used to create the private key.

Create a new signing request

You can create a new CSR, public key, and private key in the New Signing Request dialogue.

Note

Creating and deleting a signing request require the **Admin X509 Certificate Management** capability in your user role and the SMS certificate password.

Procedure

1. Go to **Admin** > **Certificate Management** > **Signing Requests**.

2. Click **New**.
3. Fill out the General section to specify CSR information used in the SMS and to create the private key.
    a. Provide a unique request name for the CSR to be stored in the SMS. The request name is not stored in the generated CSR.
    b. Select a key size. We recommend 2048 bits or greater.
    c. For enhanced security, specify a robust signature algorithm (SHA256, SHA384, or SHA512). The default is SHA512.
    d. Check or uncheck "Make it a Signing Certificate". A signing certificate sets the key certificate sign bit in the key usage extension and sets the basic constraints extension to true.
4. Fill out the Subject Distinguished Name section to define the subject of the certificate to be generated for the CSR.
    a. (Optional) Provide a valid email address for the subject.
    b. Provide a fully qualified domain name or the IP address of the owner for the certificate as the CN.
    c. (Optional) Provide the organization unit or the department name of the certificate's subject DN.
    d. (Optional) Provide the organization name of the certificate's subject DN.
    e. (Optional) Provide the locality or the city of the certificate's subject DN.
    f. (Optional) Provide the state of the certificate's subject DN.
    g. (Optional) Provide the two-letter ISO code for the country of the certificate's subject DN.
5. Fill out the Subject Alternative Name section to add a DNS and RFC822 name to the subject alternative name extension in the CSR.
    a. (Optional) Provide a domain name for the subject alternative name.
    b. (Optional) Provide a user name of the owner as an email address.

6. Click **OK**.

   The CSR fields are saved to the SMS database. A public and private key pair is generated. A certificate is generated from the data and is used to create the actual CSR to be saved in the SMS database.

Export a signing request

CSRs can be written to a `.pem` file to be sent to a CA to generate a certificate.

Note

Exporting a signing request require the **Admin X509 Certificate Management** capability in your user role and the SMS certificate password.

Procedure

1. Go to **Admin** > **Certificate Management** > **Signing Requests**.
2. Select a signing request and click **Export**.
3. Specify the file location and provide a unique name.
4. Click **OK**.

Import the certificate

You can import the CA-signed certificate that is generated from a CSR into the SMS. For more information, see *Import a certificate on page 8-57*.

When you import the certificate, the SMS retrieves the private key associated with that CSR and places it in the imported certificate. You may delete the corresponding CSR after the import.

Database

Administration of the SMS database includes viewing database statistics and managing data retention policies, configuring external access and replication of the database, and backing up and restoring the database.

In the Admin workspace, select Database in the navigation pane to display database-related information and to perform tasks on the database.

Working with the Admin (Database) screen

The Database screen in the Admin workspace displays database statistics and enables you to manage data retention policies, perform cleanup of selected database entries, and configure external database settings.

Database maintenance

The SMS database cleanup processes leverage the retention policies. The database needs to be managed to ensure its size does not exceed a desired maximum. By removing old data and limiting the amount of data stored for a particular data type, the database size can be constrained.

The SMS performs automatic cleanup procedures based on the values specified in the maintenance settings of the retention policies, that is, the age of the data and maximum rows allowed. The cleanup process removes rows that are older than the Age setting and also decreases the number of stored rows so as not to exceed MaxRows. This cleanup process is automatically performed at least one time within a 24-hour period. You have the ability to initiate an immediate clean up and to edit the retention values.

The Database Maintenance area displays the following information.

Column	Description
Data	Name of the database data.
Rows	Current number of rows of data in the database.
Max Rows	Maximum number of rows for the data in the database. The system clears records at the end of the list to make room for the newest entries, always keeping the number of total records equal to or less than this value. You can edit this value.
Age	Number of days to keep data before clearing it. The system clears data older than this setting. You can edit this setting.
Status	Cleanup status.

Column	Description
Last Cleanup	Last time the entries were cleaned. Cleanup occurs daily. You can also initiate an immediate cleanup by clicking **Cleanup Now**.
Events	Filter hits retrieved from managed devices.
Audit Log	Audit log records for the SMS.
Malware DV	Auxiliary DV (Threat DV) filter package for the SMS.
Core Controller Flow Management Method Stats	Flow Management Method Stats for managed Core Controllers.
Device Audit Log	Audit log records for managed devices.
Device Monitoring Data	Monitoring statistics for managed devices.
Device System Log	System log records for managed devices.
Device Traffic Data	Traffic statistics for managed devices.
DV	Digital Vaccine for the SMS.
Historical Events	Filter hit-based data for SMS reporting.
Historical DDOS Stats	Device DDOS statistics for SMS reporting.
Historical IP User Mapping	IP user mapping data for SMS reporting.
Historical Port Traffic Stats	Device port traffic statistics for SMS reporting.
Historical Rate Limit Stats	Device rate limit statistics for SMS reporting.
Network Mapping	Network mapping and IP correlation data for Responder.
IP Address Lookup Results	IP addresses and IP address groups for event IP address lookup.
IP User Mapping	IP user and group mapping.
Device SSL Log	SSL inspection log for managed devices.
Next Generation VPN Log	VPN logs from managed NGFW appliances.
Notifications	Latest SMS and managed device log notifications.

Column	Description
Profile Change History	Inspection profile version history.
Response History	Response History events for Responder.
sFlow®	sFlow® statistics from managed devices.
SMS Monitoring Data	SMS-specific monitoring data.
Events HTTP Context	URI metadata (i.e., hostname, URI, and Method) from managed devices.
User ID IP Correlation	User log in and group information from the Identity Agent.
VPN	X-series VPN logs.
Segment Traffic Stats	Segment traffic statistics from managed devices.

Edit data retention settings

Procedure

1. On the Admin (Database) screen, select the data row for the retention settings you want to edit, and then click **Edit**.
2. Enter a value for the maximum permitted age of data in the **Clear data older than** field.

   Data older than the entered value is removed from the database during the cleanup process.
3. Enter a value for the maximum number of permitted rows in the **Clear records exceeding the newest** field.

   The database cleanup process removes records at the end of the list to make room for the newest entries, always keeping the number of total records equal to or less than this value.
4. Click **OK**.

Reset data statistics

Procedure

1. On the Admin (Database) screen, select the data row for the retention settings you want to reset, and then click **Reset**.
2. Click **Yes** to confirm that you want to delete all data from the selected database table.

Initiate an immediate cleanup of data statistics

Procedure

1. On the Admin (Database) screen, select the data row for the retention settings you want to reset, and then click **Cleanup Now**.
2. Click **Yes** to confirm you want to continue.

   Depending on settings, the system removes or archives all entries older than the **Age** setting and more than the set **Max Rows**.

External database settings

You can configure settings for external access to the SMS database and for database replication. If you enable external database access, an external system can perform a number of read-only tasks, such as reading the SMS database, generating additional custom reports, and replicating the database.

The SMS does not allow modifications to the database through external connections. External systems are restricted to read-only access to the SMS database. You can secure external access by granting access to a specific list of IP addresses.

Note

Enabling external access and enabling database replication to an external system both require a reboot of the SMS server. Follow your company's server downtime policies, including notification to the SMS client of the pending reboot.

The External Database Settings panel indicates whether the following services are enabled or disabled:

- **External Database Access** – Allows read-only access to the SMS database. A typical use of this service is to allow an external reporting tool to generate custom reports. You must reboot the SMS to enable or disable this service. When enabled, the database name to connect to is **ExternalAccess**.
- **External Database Replication** – Allows an external database server to replicate reporting data from the SMS. You must reboot the SMS to enable or disable this service.
- **Access Restrictions** – Restricts external access to a specified list of IP addresses. You select these addresses from a list of user-defined Named Resources.

You can access *Exports and archives on page 8-128* to view snapshots and exported and archived SMS files.

For more information on the external database, see the *SMS Web API Guide*.

Configure the SMS for external access

Open a MariaDB read-only database for any third-party access or reporting tool. The read-only database is named **ExternalAccess**.

Procedure

1. On the SMS, go to **Admin** > **Database** > **External Database Settings** > **Edit**.
2. Select **External Access Settings** > **Enable external database access**.

3. Enter the following:
   - **Username** – Provide the user name for an account with sufficient rights to read all the desired data from the SMS database.
   - **Password** – Enter and confirm the password.
4. If you changed the external access settings, click **Reboot** to restart the SMS server and initialize the service.

Note

Follow your company's server downtime policies, including notification to SMS clients of a pending reboot. Before you reboot the SMS, gracefully stop other client connections to the server.

5. Click **OK**.

   If verification fails:
   - Verify that the username/password on the database matches the SMS.
   - Reboot the SMS before you try to access the database.
   - Running a complex report against SMS server may slow down the SMS response time significantly.

Configure the SMS for replication

This service allows an external database server to replicate data from the SMS. Using an external database for data replication allows you to offload report processing to an external server which can provide performance gains to your existing system. Reboot the SMS to completely enable or disable this service.

Before you begin, make sure that your replication system has sufficient disk space to accommodate the database and any increase in size due to additional data or reporting.

Procedure

1. In the SMS, go to **Admin** > **Database**.
2. On the External Database Settings panel, click **Edit**.
3. In the Edit External Database Settings wizard, select **External Replication Settings**.

Note

To configure external database replication, you must create an SMS database snapshot, and then copy the snapshot to the target replication system and import it into a MariaDB database before the SMS server can replicate its data to the target system.

4. Select **Enable external database replication** to enable the service. (To disable the service, clear the check box.)
5. Provide the following:
   - **Username** – Provide the user name for an account with sufficient rights to read all the desired data from the SMS database.
   - **Password** – Provide the password for the user account. Retype the password in the Confirm Password field.
6. If you changed the replication settings, click **Reboot** to restart the SMS server and initialize the service.

Note

Follow your company's server downtime policies, including notification to SMS clients of a pending reboot. Before you reboot the SMS, gracefully stop other client connections to the server.

7. Click **Create Snapshot**, and select **Include Events in Snapshot** if you want the snapshot to include event data.

Note

The snapshot is saved locally on the SMS server. You must copy the snapshot to the target replication system and import it into a new or existing MariaDB database before the SMS server can replicate its data to the target system.

8. Click **OK**.

Note

External database replication and the SMS High Availability (HA) features both leverage the same functionality in the underlying MariaDB database. The SMS database does not support replication to multiple destinations; therefore, we do not recommend using SMS HA and external database replication at the same time.

Configure the SMS to enable restricted access

This service allows access to the external database to be restricted to a set of IP addresses.

Procedure

1. In the SMS, go to **Admin** > **Database**.
2. On the External Database Settings panel, click **Edit**.
3. In the Edit External Database Settings wizard, select **Access Restrictions**.
4. Select **Enable restricted access** to enable the service. (To disable the service, clear the check box.)
5. Provide the following:
   - **Named IP Address Group** – To restrict a set of IP addresses, click the arrow, and either select a Named IP Address Group or create a new one.

6. Click **OK**.

Backup and restore

The SMS server maintains important data in both its database and its configuration files. The database contains data from current and historical events and operations as well as devices the SMS manages. Configuration files contain such data as SMTP server, NAT configuration, and user data. This data is critical to the operation of the SMS Server; you should back up the data periodically to assist in recovery from any unexpected failures.

Backup

The backup process backs up both the database and the configuration files. By default, event-related and statistics-related database tables are not backed up due to their size, but you can choose to include these tables as well as other, optional configuration files.

Note

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

Backing up the SMS database is a resource-intensive process, particularly if the server is under heavy load conditions and the database is large. Take this into consideration when scheduling a regular backup or initiating an immediate backup.

Backup the SMS database

Procedure

1. Go to **Admin** > **Database** > **Backup**.
2. Do one of the following:
   - Click **New** on the Scheduled Backups panel to schedule a one-time or recurring backup.

- Click **Backup Now** on the Backup and Restore panel to initiate an immediate backup.

3. For an immediate backup, skip to the next step. For a one-time or recurring backup, provide a **Schedule Name** and select the recurrence options for your scheduled backup, and then click **Next**.

4. Configure your backup from the available options.

Setting	Description
Include... most recent Digital Vaccine(s)	Select the number (1–6) of Digital Vaccines to include in the backup. The most recent Digital Vaccine is always included in a backup.
Include... most recent Device TOS packages	Select up to the six most recent Device TOS packages to include in the backup.
Include... most recent Custom packages	Select up to the six most recent custom packages to include in the backup. The active DV Toolkit (if you have one) is always included in a backup.
Include contents of events table	Select this option to include data from the Events table in the backup.
Email the backup results	Select this option to send a copy of the backup results to members of the SMS notification list. The System Notification List is defined in the Server Properties.
Use timestamp as suffix of the backup file name	Select this option to append the current timestamp to the end of the backup filename.
Include SMS logs	Select this option to provide diagnostic information for troubleshooting backups. You can skip this option if space or RAM is limited.
Encrypt backup	Select this option to encrypt the backup file. If you select this option, you must provide an encryption password. Note that this password is not recoverable. You cannot restore the contents of an encrypted backup without this password.

5. Click **Next**.

6. Select the protocol the backup process is to use, and then click **Next**.

Note

If you choose **HTTPS**, the backup file is placed on the SMS server. Best practices imply that you move the file to other storage media. To do this, use a Web browser to connect to the SMS server and copy the file. (The backup location is provided in the backup configuration summary.) SMS local backups should be offloaded from the SMS as any subsequent backup attempts will remove the current backup file.

If you choose **NFS**, ensure the NFS share grants the SMS Server write permissions for the anonymous user.

7. If prompted, provide the appropriate access information, and click **Next**.

   Depending on the protocol you select, access information might include one or more of the following:

   - **Location** path, including hostname, directory structure, and backup file name.
   - **Username** and **Password** for account with sufficient access to write to the identified storage location.
   - **Domain** in which the storage location resides.
   - **Username** and **Password** for account with sufficient access to write to the identified storage location.

8. On the Summary screen, verify your backup configuration and then click **Finish**.

   The backup procedure validates access to the storage location and then proceeds to back up the data. Backup time varies according to amount of data, server performance, and the performance of the storage location/device.

Note

An SMS backup includes the web certificate (and its private key in encrypted form) configured for the system. If the SMS is configured to use a custom web certificate, and a backup (that was created before the custom web certificate was imported) is restored, the custom web certificate will be overwritten with the original web certificate (and its private key) from the backup. If this happens, you will need to re-import the custom web certificate. To secure the private key, you can encrypt the backup.

Note

If the backup version does not match the current SMS version, the vulnerability scan (eVR) converters are not restored. The vulnerability scan (eVR) converters are only restored during a backup if the backup version and the current version of the SMS are the same.

Edit a scheduled backup

Procedure

1. On the Backup and Restore screen, select a scheduled backup in the list, and click **Edit**.
2. In the **SMS Backup** wizard, edit the backup options as needed.
3. Click **Finish** to save your changes.

Delete a scheduled backup

Procedure

1. On the Backup and Restore screen, select a scheduled backup in the list, and click **Delete**.

2. In the Delete Confirmation dialog, click **Yes**.

Restore

The restore process restores the SMS database and configuration files from a backup file. Before restoring the database, the SMS validates the integrity of the backup file. If the file is invalid, the SMS console displays an error message. To ensure database integrity, the system automatically reboots after the restore operation.

The SMS supports restoring a backup taken from a previous version of SMS. For example, you can restore a backup taken with SMS 3.5 and restore it to an SMS 3.6 server. When you restore a backup file from a previous version, the database is not only restored, but the data is migrated and data structures conform to the version of SMS running on your SMS server.

Note

If you restore a backup to an SMS server on which SMS patches are installed, you might need to rollback and reapply an SMS patch. In this case, the restoration process displays a dialog that indicates if you need to perform this task.

Backup and restore processes require access to storage, either to back up data to storage or restore data from storage. The SMS backup and restore processes can perform their tasks using any of the following storage access protocols:

- Network File System (NFS) Protocol — Does not require local storage on the SMS.
- Server Message Block (SMB) Protocol — Microsoft-based shared-access file system. Does not require local storage on the SMS.
- Secure File Transfer Protocol (sFTP) — Does not require local storage on the SMS.
- Secure Copy Protocol (SCP) — Requires temporary local storage on the SMS.

- Secure Hypertext Transfer Protocol (HTTPS) — Data is stored locally on the SMS. HTTPS requires that the service be enabled on the SMS server.

During backup and restore processes, the SMS server performs the following tasks:

- Mount the storage destination, referred to in the SMS product as the location.
- Stop the SMS server database and SMS server application.
- Back up or restore the database files to/from the specified storage location.
- Unmount the storage destination.
- Restart the SMS server database and SMS Server application. If it is a restore operation the SMS server is restarted and rebooted, which stops client connections to the SMS server.

Some of the supported storage access protocols allow IPv6 addressing. When you specify a backup location in the SMS backup wizard with an IPv6 address, be sure to follow the following syntax requirements:

- **NFS** — Does NOT support IPv6
- **SMB** — IPv6 address MUST be surrounded by brackets
- **SCP** — IPv6 address with or without brackets
- **sFTP** — IPv6 address with or without brackets

If the restored SMS is a different platform or version than the SMS from which you backed up then the following configurations will not be restored and will remain unchanged:

- **Admin Server Properties** (Admin > Server Properties)
  - Management: System Information and Services
  - Network: Network Interface, Date/Time, and DNS
- **Auto DV Activation** (Profiles > Digital Vaccines > DV Inventory > Auto DV Activation)

- Automatic Download
- Automatic Activation
- Automatic Distribution

Restore the SMS database

Before you initiate the restore process, ensure there are no active client connections to the SMS server through the SMS client, command line interface, or Web browser. You can restore any database beginning with SMS v4.4.0.57192 on a system that runs the most current software.

Procedure

1. On the Backup and Restore screen, click **Restore**.
2. In the SMS Restore wizard, select the backup file you want to restore, and click **OK**.
3. Click **Import**.

   The **SMS Restore** wizard verifies the integrity of the chosen file and proceeds if the file is valid. If the file is invalid, the SMS displays an error message.
4. A summary page appears. If the information is correct, click **Finish**.

   Database restoration begins, with the restored data overwriting the existing data. When complete, the SMS Server reboots to finalize the restore process and ensure data integrity of the restored database.

Server Properties

Management

Update system information

You must have SuperUser privileges to use this feature. Learn more: *User roles and capabilities on page 8-39*.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Management** tab.
2. Update the following:
   - Name
   - Contact
   - Location
3. Select **Management Port Negotiation** to enable automatic negotiation on the management port.
4. Click **Apply**.

Enable FIPS Crypto Core mode

Only the cryptographic libraries used by SMS version 4.2.1 and later are FIPS 140-2 certified. Because of this, FIPS mode in SMS version 4.2.1 and later is called **FIPS Crypto Core**.

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. The FIPS 140-2 publication coordinates requirements and standards for cryptography modules that include both hardware and software components. Some United States federal agencies and departments require software, including the SMS, to comply with the 140-2 standards.

The SMS supports two levels of FIPS operation:

- **Disabled** — No FIPS compliance actions or restrictions are activated on the SMS server.
- **FIPS Crypto Core** — In this mode the SMS uses cryptographic libraries certified by the National Institute of Standards and Technology to be compliant with FIPS 140-2 publication. The SMS automatically reboots when placed into FIPS Crypto Core mode or when FIPS Crypto Core mode is disabled.

You must have SuperUser privileges to use this feature. Learn more: *User roles and capabilities on page 8-39*.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Management** tab.
2. Click **Edit** under FIPS Mode.
3. Review the current state. The current state radio button indicates if the SMS is in FIPS Crypto Core mode. If it is not, the radio button is unselected and the current state displays as Disabled.
   a. If the current state is Disabled, select the **FIPS Crypto Core** radio button to enter FIPS Crypto Core mode.
   b. If the current state is FIPS Crypto Core, select the **Disabled** radio button to turn that mode off.
4. Click **OK**.

   When you submit the request to enter FIPS Crypto Core mode, the SMS server reboots. This process, along with the reboot, also occurs when transitioning out of FIPS Crypto Core mode.

Note

If the SMS is currently running a 1K key, it will display a message about upgrading to a 2K key to be fully FIPS compliant. You can still enable FIPS mode on the SMS without installing the 2K key, but when the SMS is in FIPS mode, you cannot install the 2K key.

When this process is complete, the SMS operates in FIPS Crypto Core mode. The following restrictions apply in this mode:

- A 2048-bit certificate is required.
- If an SMS backup was taken while the SMS was in FIPS Crypto Core mode, the backup cannot be restored on an SMS that has a 1024-bit certificate.
- Upgrading the SMS certificate key will not be allowed. For more information, see *SMS certificate key on page 8-9*.

- SMS will not be able to communicate with the Identity Agent. For more information, see *User ID IP Correlation on page 8-132*
- SMS High Availability (HA) is available if both systems have the required 2K key.
- The SSH terminal will negotiate connections using only FIPS 140-2 approved algorithms.
- Custom Responder Actions cannot be imported or executed.
- To get logs from a managed SSL device, you must first set up SMS as the syslog destination in the SSL web client.
- External Database access is not permitted.
- External Database replication is not permitted.

Enable SMS services

You can enable or disable the services that run on the SMS server. Services listed on the panel are used to communicate with the SMS server.

You must have SuperUser privileges to use this feature. Learn more: *User roles and capabilities on page 8-39*.

Procedure

1. Select **Admin** > **Server Properties**, and then select the **Management** tab.
2. Select a service from the following.

SELECT:	TO ENABLE ...
HTTPS	Web services for the SMS.
Ping	The SMS to respond to an ICMP request.

SELECT:	TO ENABLE ...
SSH	Secure communication connection used for CLI. Requires SuperUser access. **SSH Login Grace Time** - Amount of time a user has to enter a password and establish a connection. The SMS disconnects after this time if the user has not successfully logged in. The default is 60 seconds, but you can set the time from 30 to 600 seconds. **SSH Max Authentication Attemps** - A limit of six invalid SSH connection attempts can now be configured.
TAXII	The SMS to receive Structured Threat Information eXpression (STIX™) 2.0 data using a TAXII service. STIX data is used for tag categories in the Reputation Database. For more information, see *View open threat intelligence - STIX/TAXII data on page 5-103*. This service is enabled by default. To enable the TAXII service, ensure that you have TLS v1.2 enabled. For more information, see *Edit TLS versions on page 8-120*.

3. Click **Apply**.

Network

Update network interface information

Procedure

1. Select **Admin** > **Server Properties**, and then select the **Network** tab.
2. Update the following.

SETTING	DESCRIPTION
Ethernet MAC ID(2)	Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv4 standard.

(2) read-only field

Setting	Description
Scope Link Address*	Unique identifier assigned by the manufacturer to network interface cards (NICs) capable of supporting the IPv6 standard.
IP Address	Internet protocol (IP) address of the SMS server used for management communication.
Subnet Mask	Subnet mask of the IP address.
Gateway	Network gateway through which SMS Server traffic flows.
IPv6 Address	IP version 6 address of the SMS Server.
Default Router	IP address of the default router through which SMS Server traffic is routed to/from the network.

3. Click **Apply**. If you change the management IP address, you must reboot the SMS server (**Admin** > **General** > **SMS Server** > **Reboot**).

Enable Network Time Protocol (NTP)

Configure how the SMS Server obtains its date and time. You can configure the SMS Server to obtain its date and time from a network-based network time protocol (NTP) server or you can set the date and time manually.

To keep date and time consistent between the SMS Server and the devices it manages, consider configuring your SMS Server as an NTP Server, and configure the managed devices to obtain their date and time from the SMS Server. You can then configure the SMS Server to obtain its time from another NTP Server.

Do not set the time backwards on the SMS server as it might cause inconsistencies in system services that depend tightly on time. The SMS will restart if the time zone is changed, or if the time change is greater than 1 minute.

Enable SMS Network Time Protocol authentication settings - You can only enable Network Time Protocol (NTP) authentication settings for the SMS from the SMS CLI. For details, see "ntp-auth" in the *CLI Reference*.

The SMS does not store NTP log messages or connection details. Review this information on the NTP Server.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Network** tab.
2. Select **Enable Time Protocol (NTP)** under Date/Time.
3. Provide the IP address or hostname of one or more NTP servers. If Enable Time Protocol (NTP) is selected, you must identify at least one NTP Server.
4. Click the **Time Zone** drop-down list, and select the correct time zone in which the SMS server operates.
5. Click **Apply**.

Manually set the date and time on the SMS server

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Network** tab.
2. Clear the **Enable Time Protocol (NTP)** check box under Date/Time.
3. Click the calendar icon next to the **New Date/Time** field.
4. Use the controls in the pop-up window to select the month, year, day, and time, and then click **OK**.
5. Click the **Time Zone** drop-down list, and select the correct time zone in which the SMS server operates.
6. Click **Apply**.

Edit SMTP server settings

Identify a Simple Mail Transfer Protocol (SMTP) server through which the SMS can send email messages, typically generated when critical operational states trigger email communications with system and network

administrators. The SMS sends email messages for specific events, including the following:

- SMS HA fail-over and activation
- SMS start and stop
- Critical device failures (device can no longer communicate)
- Critical or Error entries in the device syslog
- Database backup
- SMS migrate
- Auto DV download and activation
- Auto DV distribution including both success and failures
- Reports can be configured for scheduled runs where an email is sent

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Network** tab.
2. Click **Edit** under SMTP Server.
3. Enter the following.

Setting	Description
Server Address	IP address or hostname of the SMTP mail server through which the SMS can send email messages.
SMTP Port	Port on the mail server that listens for SMTP requests. If you enable SMTPS (see below), this defaults to 587. If SMTPS is disabled, this defaults to 25.

Setting	Description
Aggregation Period	Amount of time (in seconds) that the SMS aggregates the device email notifications before it sends the notifications in a single email. If you set the aggregation to zero (default), the SMS will immediately disable the email aggregation. The maximum number of emails the SMS can collect for a single aggregation period is 10,000. When the SMS reaches this limit, it will discard new device email notifications received. This setting only applies to device notifications. All other SMS emails are sent immediately.
System Notification List	List of email addresses or email address groups to which the SMS sends email notifications.
From	Email address or address group to appear as the sender for email notifications sent by the SMS.
Reply To	Email address or address group to receive replies to email notifications originally sent by the SMS.

4. If the mail server requires authentication, select **Authentication** and provide the required user name and password.
5. If you need to secure the mail transfer, select **Enable SMTPS**. Because SMTPS requires a certificate, select a previously imported certificate from the **Certificate** pull-down menu, or click **Import** to import another certificate.
6. Click **Test**.

   The SMS transmits a test email to the SMTP server, which should then send the email to the designated recipients. The test verifies whether the SMS can connect to the mail server using the server settings you configured; it does not verify that the designated recipients receive the email, which is the responsibility of the SMTP server.
7. Click **OK**.

Configure an HTTP proxy connection

Configure a proxy server for communication between the SMS and the destination website, such as the TMC. This feature supports basic HTTP authentication (with or without user authentication).

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Network** tab.
2. Select **Proxy Internet Connections** under HTTP Proxy.
3. Provide the IP address or hostname and the port number for the proxy server.
4. If the proxy server requires authentication, select **Use Proxy Authentication** and provide the user name and password in the appropriate fields.
5. Click **Apply**.

Configure DNS

Configure a DNS server that the SMS can use to locate other servers and to register its own identity. You are not required to identify a DNS server.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Network** tab.
2. Enter an IP address or hostname of up to three DNS servers under Domain Name Service (DNS).
3. Click **Apply**.

NAT

Enable SMS NAT

Configure an alternate IP addresses that a device can use to communicate with the SMS Server. You can manage a device when the IP address for the

SMS network interface is not available to the device because the SMS is behind a network address translation (NAT) boundary or a network address translation protocol translation (NAT-PT) boundary. Typically, when the SMS discovers a TippingPoint device, the SMS communicates with the device via the IP address of the SMS. When the SMS is behind a NAT boundary, it can provide devices with an alternate IP address that the device can reach. An alternate IP address can be defined as part of a global NAT, per network NAT, or both.

For basic NAT configuration, you can choose to use only the global NAT option. Global NAT is an alternate IP address that is made available across multiple networks that managed devices can use to connect with the SMS.

When you use the per network NAT option, you may want to configure a global NAT address that can be used if the system is unable to match a device network.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **NAT** tab.
2. Click **Edit** under SMS NAT.
3. Select **Enable Global NAT**.

   Global NAT is an alternate IP address that is made available across multiple networks that managed devices can use to connect with the SMS. If Global SMS NAT is enabled, the system uses the specified Global NAT Address as the SMS IP address. If the system cannot locate an SMS NAT address or a Global NAT address, it uses the configured IP address of the SMS network interface.
4. Enter an IP address that the device should use to communicate with the SMS.
5. Click **OK**.
6. Click **Apply**.

Enable SMS per network NAT

Specify a list of alternate IP addresses so that managed devices separated from the SMS Server by a NAT layer can connect to the SMS through an address that resides on the same network as each device.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **NAT** tab.
2. Click **Enable** under SMS Per Network NAT.

   If Per Network NAT is enabled, the system consults the list of SMS NAT Addresses and chooses the entry whose network matches that of the specified device address. In case of multiple matches, the system chooses the most specific match. If no network address matches, the system consults the Global SMS NAT settings.
3. Click **Add**.
4. Enter the IP address for the device network.
5. Enter the prefix length in bits. The Prefix Length is the number of bits that make up the network portion of the address. The maximum is 32 bits for an IPv4 address and 128 for an IPv6 address.
6. Enter an SMS NAT Address that the device can use to connect to the SMS.
7. Click **OK**.
8. Click **Apply**.

ID Resolver

Configure, enable, and query IDResolver (A10 Networks)

You can configure the SMS to retrieve user information from an A10 Networks appliance. This service provides information about a user based on a host association entry on the A10 Networks appliance.

To configure integration between the SMS and the A10 Networks appliance, the location and login credentials of the A10 Networks appliance must be identified on the SMS server.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Integration** tab.
2. Click **Edit**, and provide the following information:
   - **Address** and **Port**.
   - **User Name** and **Password**.
   - Select a value for **Password Encryption**.
   - Specify a numerical value for **Timeout**.
3. Click **OK**.
4. Click **Enable**.
5. To query IDResolver, right-click an entry that displays an IP address that is part of an A10 managed network, and select **Query IDResolver**.

SNMP

Enable SNMP requests

SNMP is an application-layer protocol that monitors network devices for conditions that warrant administrative attention. Items typically monitored include servers, workstations, routers, switches and hubs.

You can configure SMS to be a managed device that is monitored by an SNMP server. The SNMP server periodically requests information from the SMS server. You can also configure the SMS to send trap information to the SNMP server. The SNMP server is also referred to as a network management system (NMS). SNMP request settings determine how the SMS handles SNMP requests, they do not affect SMS communication with IPS devices.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **SNMP** tab.
2. Click **Edit** under Request Settings.
3. Select **Enable SNMP Requests**.
4. Select a version from the following:
   a. Select **v2**, and use the Community String field to restrict access. By default, the Community String is “public.”
   b. Select **v3**, and provide the following information:
      - Username required for the SNMP application
      - Protocols used for authentication and privacy
      - Keys used with the authentication and privacy protocols

   The Engine ID is a read-only, SMS-generated identifier for the SNMP application. If no protocol is selected, the **Key** field is disabled.
5. Click **OK**.
6. Click **Apply**.

Configure an NMS trap destination

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **SNMP** tab.
2. Click **Add** under NMS Trap Destinations.
3. Enter the IP address and port number.
4. Select a version from the following:
   a. Select **v2**, and use the Community String field to restrict access. By default, the Community String is “public.”
   b. Select **v3**, and provide the following information:

- Username required for the SNMP application
- Protocols used for authentication and privacy
- Keys used with the authentication and privacy protocols

The Engine ID is a read-only, SMS-generated identifier for the SNMP application. If no protocol is selected, the **Key** field is disabled.

5. Click **Test** to send a test trap to the specified destination.
6. Click **OK**.
7. Click **Apply**.

Syslog

Create or edit syslog notification settings

Configure syslog notification settings to set up the sending of events to a syslog server and to control the number of events that are sent to it.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Syslog** tab.
2. Under **Remote Syslog for Events**, click **New** to set up the sending of events to a syslog server, or select an existing configuration and click **Edit**.
3. Select **Enable** to turn on this feature.
4. Enter the host name or IP address in the **Syslog Server** field.
5. Select a transportation **Protocol**:
   - UDP
   - TCP
   - Encrypted TCP, and import or select the x509 certificate that is generated on the syslog server.

Note

When URI information that includes URI strings is sent using the UDP protocol, data loss can result. When logging URI string information, use either the TCP or Encrypted TCP protocol.

6. Enter the **Port** number (for the listener port on the syslog server).
7. Select a **Log Type** format. *Learn more on page 8-101*.
8. Select an **Event Query** to send all events or a select set of events to the syslog server.
9. Select a **Facility** option to limit the events sent to a specific facility level. Facilities are defined by the BSD Syslog Protocol. Refer to `RFC 3164`. The default setting is Security/Authorization.
10. Specify the **Severity** of the syslog messages sent to this server.
11. Select a **Delimiter** to determine the character the SMS uses as a delimiter for event data in the syslog message. The default setting is TAB.
12. Select a **Timestamp in Header** option:
    - None
    - SMS current timestamp – when the SMS sends the message to the syslog server.
    - Event timestamp – original timestamp of the event.
13. Select **Include SMS Hostname in Header** to include the hostname of the SMS.
14. Select **Send New Events/Log Only** to determine whether the SMS will send only new events and log entries, not those already received by the SMS. Select this when you initially configure the connection to a syslog server to exclude what could be a sizable number of historical events.
15. Click **OK**.
16. Under **Remote Syslog for Events**, click **Apply**.

Create or edit a syslog format

The SMS server generates and gathers syslog events, which log information about a variety of conditions and operational state changes from monitored devices. You can define a custom message format that will be sent to a syslog server. The maximum size of a syslog message is 9K.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **Syslog** tab.
2. Under **Syslog Formats**, click **New** to define a new syslog format, or select an existing format and click **Copy** to save as a new format. You can also edit an existing syslog format.
3. Select a type from the Log Type drop-down list. *Learn more on page 8-101*.
4. Enter a name in the **Name** field.
5. Click **Insert Field** to insert a syslog field. *Learn more on page 8-113*.
6. Edit the pattern for the syslog format as needed.
7. Select a protocol to truncate or split messages:
   - **RFC 3164 compliant** - messages are truncated
   - **RFC 5424 compliant** - messages are split into multiple messages
8. Click **OK**.
9. Click **Apply.**

Syslog log types

Use the following log types for SMS message logging.

SMS System

Field	Type	Max size	Description
facility	integer	11	Appears to always be 0

Field	Type	Max size	Description
formattedTime	date string	15	MMM dd HH:mm:ss, ex. Mar 20 02:02:48
logID	long	20	SMS system log entry identifier
message	string	1024	System log message
severity	integer	4	Severity of the entry: 1,2 – Info 3 - Warn 4 – Error 5 - Critical
time	long	20	System log entry timestamp in milliseconds

SMS Audit

Field	Type	Max size	Description
clientIpAddress	String	39	Source address of the client that generated the audit entry.
clientPort	Integer	11	Port of the client that generated the audit entry.
description	String	1024	Audit message.
index	Long	20	SMS audit log entry identifier.
sessionID	Integer	11	SMS identifier for the user session that generated the audit entry.
status	String	300	Success, fail
time	Long	20	Audit log entry timestamp in milliseconds.
userName	String	150	Name of the user.

Device System

Field	Type	Max size	Description
component	String	12	Component area of the device that generated the system log entry.
deviceID	Integer	10	SMS identifier for the device.
deviceName	String	63	User-provided name of the device that system log entry was received from.
index	Long	20	SMS device system log entry identifier.
message	String	65.535	System message.
messageCode	Long	10	
sequence	Long	20	Device system log entry identifier.
severity	String	32	INFO, WARN, ERR
time	Long	20	System log entry timestamp in milliseconds.

Device Audit

Field	Type	Max size	Description
accessLevel	string	13	Unknown, Operator, Administrator, Super User, SMS
component	string	12	Component area of the device that generated the audit entry
deviceID	integer	10	SMS identifier for the device
deviceName	string	63	User-provided name of the device that audit entry was received from
index	Long	20	SMS device audit entry identifier
interface	string	7	Device interface type that initiated the audit entry
ipAddress	IP Address	39	Source address of the interface that generated the audit entry

Field	Type	Max size	Description
message	string	65,535	Audit message
result	String	4	PASS, FAIL
sequence	Long	20	Device audit entry identifier
time	Long	20	Audit entry timestamp in milliseconds
user	String	128	Name of the user

Snort Syslog Format MARS [Deprecated]

Column	Description
0	Date (timestamp)
1	Device identifier
2	SID
3	Filter name
4	Classification
5	Priority
6	Protocol (`TCP`, `UDP`, `ICMP`, and `IP`)
7	Source address
8	–> (indicates direction of traffic flow: source –> destination)
9	Destination address

Snort Syslog Format V2 [Deprecated]

Column	Description
0	Device identifier
1	SID
2	Filter name

Column	Description
3	Classification
4	Priority
5	Protocol
6	Source address
7	–>
8	Destination address

SMS 2.0/2.1 Syslog Format

Column	Description
`0`	Syslog category — "`<32>`" — defined facility and severity
`1`	Action type — `7` is `Permit`, `8` is `Block`, `9` is `P2P`
`2`	Severity — `0` is `Normal`, `1` is `Low`, `2` is `Minor`, `4` is `Critical`
`3`	Policy UUID — TippingPoint UUID for policy
`4`	Signature UUID — TippingPoint UUID for signature
`5`	Signature name — user-friendly name for signature and policy
`6`	Signature number
`7`	Signature protocol — protocol of signature (`IP`, `UDP`, `TCP`, `HTTP`, etc.)
`8`	Source address
`9`	Source port
`10`	Destination address
`11`	Destination port
`12`	Hit count — number of attacks during aggregation period
`13`	Device slot — this slot can be `3,5,7,8`

Column	Description
14	Device segment — device segment of above slot that got event
15	Device name — user-friendly name of the device event was received
16	TippingPoint Taxonomy ID — category ID assigned to the signature
17	Event timestamp in milliseconds
18	Additional comments about the event
19	Sequence number of the event in the SMS

SMS 2.5 Syslog Format

Column	Description
0	Syslog category — "<32>" — defined facility, and the severity
1	Action type — 7 is Permit, 8 is Block, 9 is P2P
2	Severity — 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical
3	Policy UUID — TippingPoint UUID for policy
4	Signature UUID — TippingPoint UUID for signature
5	Signature name — user-friendly name for signature and policy
6	Signature number
7	Signature protocol — protocol of signature (IP, UDP, TCP, HTTP, etc.)
8	Source address
9	Source port
10	Destination address
11	Destination port
12	Hit count
13	Source zone name

Column	Description
14	Destination zone name
15	Incoming physical port
16	VLAN ID
17	Device name — user-friendly name of the device event was received
18	TippingPoint taxonomy ID — category ID assigned to signature
19	Event timestamp in milliseconds
20	Additional comments about the event
21	Sequence number of the event in the SMS

ArcSight CEF Format v3.5 [Deprecated]

Use this format type to send events to an ArcSight connector. This format type does not support IPv6.

Column	CEF key name	Description
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|)
1	app	Application protocol
2	cnt	Base event count
3	dst	Destination address
4	dpt	Destination port
5	act	Device action
6	cn1	Device custom number 1: VLAN tag
7	cn1Label	Device custom number 1 label
8	cn2	Device custom Number 2: taxonomy ID

Column	CEF key name	Description
9	cn2Label	Device custom number 2 label
10	cn3	Device custom number 3: packet trace
11	cn3Label	Device custom number 3 label
12	cs1	Device custom string 1: profile name
13	cs1Label	Device custom string 1 label
14	cs2	Device custom string 2: policy UUID
15	cs2Label	Device custom string 2 label
16	cs3	Device custom string 3: signature UUID
17	cs3Label	Device custom string 3 label
18	cs4	Device custom string 4: zone names
19	cs4Label	Device custom string 4 label
20	cs5	Device custom string 5: device name
21	cs5Label	Device custom string 5 label
22	cs6	Device custom String 6: message parameters (IP address of Reputation filter matches)
23	cs6Label	Device custom string 6 label
24	src	Source address
25	spt	Source port
26	externalID	External ID (event ID)
27	rt	Event time
28	cat	Device event category
29	proto	Transport protocol
30	deviceInboundInterface	Device inbound interface (physical port in)

ArcSight CEF Format v4.1 [Deprecated]

Use this format type to send events to an ArcSight connector. This format type includes HTTP context information and supports IPv6.

Column	CEF key name	Description
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|)
1	app	Application protocol
2	cnt	Base event count
3	dst	Destination IPv4 address
4	dpt	Destination port
5	act	Device action
6	cn1	Device custom number 1: VLAN tag
7	cn1Label	Device custom number 1 label
8	cn2	Device custom number 2: taxonomy ID
9	cn2Label	Device custom number 2 label
10	cn3	Device custom number 3: packet trace
11	cn3Label	Device custom number 3 label
12	cs1	Device custom string 1: profile name
13	cs1Label	Device custom string 1 label
14	cs2	Device custom string 2: policy UUID
15	cs2Label	Device custom string 2 label
16	cs3	Device custom string 3: signature UUID
17	cs3Label	Device custom string 3 label

Column	CEF key name	Description
18	cs4	Device custom string 4: zone names
19	cs4Label	Device custom string 4 label
20	cs5	Device custom string 5: device name
21	cs5Label	Device custom string 5 label
22	cs6	Device custom string 6: message parameters (IP address of Reputation filter matches)
23	cs6Label	Device custom string 6 label
24	src	Source IPv4 address
25	spt	Source port
26	externalID	External ID (event ID)
27	rt	Event time
28	cat	Device event category
29	proto	Transport protocol
30	deviceInboundInterface	Device inbound interface (physical port in)
31	c6a2	Source IPv6 address
32	c6a3	Destination IPv6 address
33	request	URI string
34	requestMethod	URI method
35	dhost	URI host

ArcSight CEF Format v4.2

Use this recommended format type to send events to an ArcSight connector. This format type includes HTTP context information, TCIP/XFF client IP, and user information.

COLUMN	CEF KEY NAME	DESCRIPTION
0	CEF	CEF header (Version|Device Vendor|Device Product|Device Version|Signature ID|Name| Severity|)
1	app	Application protocol
2	act	Flow control of the filter
3	c6a1	Client IPv6 address
4	c6a1Label	Client IPv6 address field label
5	c6a2	Source IPv6 address
6	c6a2Label	Source IPv6 address field label
7	c6a3	Destination IPv6 address
8	c6a3Label	Destination IPv6 address field label
9	cat	Filter name category
10	cn1	Device custom number 1: VLAN ID
11	cn1Label	Device custom number 1 label
12	cn2	Device custom number 2: taxonomy ID
13	cn2Label	Device custom number 2 label
14	cn3	Device custom number 3: packet trace
15	cn3Label	Device custom number 3 label
16	cs1	Device custom string 1: profile name
17	cs1Label	Device custom string 1 label
18	cs2	Device custom string 2: profile UUID
19	cs2Label	Device custom string 2 label
20	cs3	Device custom string 3: filter signature UUID

Column	CEF key name	Description
21	cs3Label	Device custom string 3 label
22	cs4	Device custom string 4: zone names (source and destination)
23	cs4Label	Device custom string 4 label
24	cs5	Device custom string 5: device name
25	cs5Label	Device custom string 5 label
26	cs6	Device custom string 6: filter message parameters (IP address of Reputation filter matches)
27	cs6Label	Device custom string 6 label
28	cnt	Event hit count
29	deviceInboundInterface	Physical port in
30	dhost	Host name of the URI
31	dntdom	Destination domain name
32	dpt	Destination port
33	dst	Destination IPv4 address
34	duser	Destination username
35	dvchost	Device name
36	externalId	Event ID
37	proto	Network protocol
38	request	URI string
39	requestMethod	URI method
40	rt	Event time stamp
41	sntdom	Source domain name

Column	CEF key name	Description
42	sourceTranslatedAddress	Client IPv4 address
43	spt	Source port
44	src	Source IPv4 address
45	suser	Source user name

Syslog fields

The following syslog fields are available on the SMS.

Field	Type	Max size	Description
_delimiter			tab, comma, semi-colon, or pipe.
actionSetName	integer	56	Action set name.
actionType	integer	3	Action type on the filter associated with the syslog event. • 7 – IPS Alert • 8 – IPS Block • 9 – P2P • 12 – Quarantine • 37 – Reputation Alert • 38 – Reputation Block
arcSightFilterName	string	250	Name of the filter associated with the syslog event.
arcSightSeverity	integer	7	0 is Info, 1 is Low, 4 is Minor, 7 is Major, 10 is Critical

Field	Type	Max size	Description
categoryName	string	128	Name of the filter category.
clientAddress	IP address	39	TCIP/XFF client IP address in IPv4 or IPv6 format from HTTP traffic when configured in the profile settings. This field matches the srcAddress field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the event. This field will be empty in the following situations: • The profile configured on the segment does not have TCIP/XFF enabled • The IPS device is running a version of TOS that doesn't support the feature **Note** When you upgrade a TPS device, the SMS will start sending the client IP address (or source IP address if the client IP address is not available) to any remote syslog configured with this field.
clientAddressv4	IP address	15	TCIP/ XFF client IP address in IPv4 format from HTTP traffic when configured in the profile settings. This field matches the srcAddress field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the syslog event. This field will be empty in the following situations: • The profile configured on the segment does not have TCIP/XFF enabled • The IPS device is running a version of TOS that doesn't support the feature • An IPv6 address was captured

Field	Type	Max size	Description
clientAddressv6	IP address	39	TCIP/XFF client IPv6 address in IPv6 format (for example, 2001:db8:85a3::8a2e:370:7334) from HTTP traffic when configured in the profile settings. This field matches the srcAddress field when TCIP/XFF collection is enabled but TCIP/XFF is unavailable for the traffic flow associated with the event. This field will be empty in the following situations: • The profile configured on the segment does not have TCIP/XFF enabled • The IPS device is running a version of TOS that doesn't support the feature • An IPv4 address was captured
cveIds	string	1000	CVE ID **When creating a custom syslog format, note the following:** Because commas are used to separate multiple CVEs in a syslog entry, define and manually insert an escape character when you use comma delimiters in your custom syslog. These characters will properly separate the CVE ID field so that the receiving server can parse the custom fields. You might also need to adjust the settings for your syslog server so that it recognizes the defined escape character.
destAddress	IP address	39	Destination address of the syslog event.
destAddressv4	IP address	15	Destination IPv4 address. This field will be empty if the destAddress is an IPv6 address.
destAddressv6	IP address	39	Destination IPv6 address. This field will be empty if the destAddress is an IPv4 address.
destPort	integer	5	Destination port number.

Field	Type	Max size	Description
destUserDomain	string	255	Active Directory domain name of the user at the destination IP address. The Identity Agent must be configured for the SMS.
destUserMachine	string	1023	Computer name for the user at the destination IP address. The Identity Agent must be configured for the SMS.
destUserName	string	1023	Active Directory logged in username at the destination IP address. The Identity Agent must be configured for the SMS.
deviceName	string	63	User-provided name of the device event was received from.
deviceSegment	integer	11	Segment on the device where the event occurred.
deviceSlot	integer	11	Device slot.
deviceTimezone	string	50	Device time zone.
eventID	long	20	SMS event identifier. This is the **Event No** field, available on Inspection Event Details.
eventTimestamp	long	20	Event timestamp in milliseconds.
filterName	string	250	Name of the filter associated with the syslog event.
fiterNameV2	string	250	Name of the filter associated with the event and contains the same information as the `filterName` field except for the colon (:) and semi-colon (;) punctuation.
flowControl	string	20	Flow control of the filter.
hitCount	integer	10	Number of times this event occurred during aggregation period.

Field	Type	Max size	Description
msgParameters	string	255	Message parameters used for certain filters, such as DDoS filters and Reputation filters. Each parameter is separated by pipes (for example, 10.1.4.80/32|exceeds|1|3) **Example**: If a signature has a message (e.g., 7202 is 7202: SYN flood against [1] [2] [3] SYNs/sec (current rate = [4], the numbers in brackets refer to the data in the message parameters. The complete message results when the signature message is combined with the message parameters. For example: 7202: SYN flood against 10.1.4.80/32 exceeds 1 SYNs/sec (current rate = 3)
originalFilterName	string	250	Name of the original filter associated with the event.
originalSignatureNumber	integer	50	Original filter number (for example, 1000730).
packetTrace	boolean	3	Packet trace associated with the event — 0 is if there is no packet trace, 1 is if there is a packet trace. This field will not be available from TPS devices.
physicalPortIn	integer	5	Physical port in.
policyUUID	string	36	UUID for the policy (for example, c6da0827-798b-49ad-85e8-bb8e0ae531b5). You can also use this field in conjunction with the SMS Web Services API.
profileName	string	127	Name of the profile on the device segment/interface where the event occurred.
protocol	string	30	Name of the protocol.
protocolLower	string	30	Name of the protocol in lowercase letters.

Field	Type	Max size	Description
severity	integer	3	0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical
severityType	string	8	Severity type (Low, Minor, Major, etc.)
signatureName	string	250	User-friendly name for the filter. Use this field with the SMS Web Services API.
signatureNumber	integer	11	Filter number. Use this field in conjunction with the SMS Web Services API.
signatureUUID	string	36	UUID for the filter. Use this field in conjunction with the SMS Web Services API.
smsName	string	63	User-provided name of the SMS.
snortClass [deprecated]	string	64	Snort Classification.
snortDate [deprecated]	date	15	Event timestamp.
snortDestAddress [deprecated]	IP address : Port	45	Destination address and port of the event.
snortName [deprecated]	string	255	Name of the filter associated with the event.
snortNameV2 [deprecated]	string	255	Name of the filter associated with the event.
snortPriority [deprecated]	integer	6	0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical
snortProtocol [deprecated]	string	36	Name of the protocol.

Field	Type	Max size	Description
snortProtocolV2 [deprecated]	string	36	Name of the protocol.
snortSid [deprecated]	string	25	Snort rule identifier (for example, [1:0:1]).
snortSrcAddress [deprecated]	IP address : Port	45	Source address and port of the event (for example, 10.0.0.3:80).
srcAddress	IP address	39	Source address of the event (for example, 10.0.0.3).
srcAddressv4	IP address	15	Source IPv4 address. (for example, 10.0.0.3). This field will be empty if the srcAddress is an IPv6 address.
srcAddressv6	IP address	39	Source IPv6 address (for example, 2001:db8:85a3::8a2e:370:7336). This field will be empty if the srcAddress is an IPv4 address.
srcPort	integer	5	Source port number.
srcUserDomain	string	255	Active Directory domain name of the user at the source IP address. The Identity Agent must be configured for the SMS.
srcUserMachine	string	1023	Computer name for the user at the source IP address. The Identity Agent must be configured for the SMS.
srcUserName	string	1023	Name for the user at the source IP address. The Identity Agent must be configured for the SMS.
taxonomyID	long	11	Category ID assigned to the signature.
uriHost	string	255	HTTP hostname from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, example.com).

Field	Type	Max size	Description
uriMethod	string	15	HTTP method from the HTTP header when HTTP context is configured for the profile and reported by the IPS device (for example, GET).
uriString	string	284	URI from the HTTP header when HTTP context is configured for the profile and reported by the IPs device (for example, /path/to/resource/resource.txt).
vlanTag	integer	5	Vlan ID.

Trend Micro TippingPoint app for Splunk

The Trend Micro TippingPoint app for Splunk contains action set logic, distribution history, and dashboards for monitoring SMS data in Splunk.

SMS configuration includes creating a Splunk syslog format and configuring a syslog exporter to send events and messages to Splunk. For more information, see the *Splunk Getting Started Guide*.

TLS

Edit TLS versions

Configure which TLS versions is enabled for the various SMS communication categories.

- **Web Server**— allows access to the SMS web server using a Web browser or the SMS Web API. The TLS version on your client (e.g., Web browser) must be compatible with the TLS versions enabled in this section.
- **IPS Remote Authentication** — used by the IPS devices when the SMS is used as the authentication source. If the device doesn't support the TLS version, the SMS will not be able to communicate with the device.
- **SMS Client Communication** — used for communication between the SMS client and the SMS server.

- **SMS connecting to Devices/TMC/LDAP**— used for communication between the SMS and remote servers, such as LDAP, TMC, Identity Agent, and managed devices. You can enable SSLv3.0 if your remote server requires this protocol.

SMS connecting to Devices/TMC/LDAP

If the SSLv3.0 protocol is not required in your network environment, we recommend that you disable it as it is the least secure TLS version.

The TLS versions enabled on a TPS device must be compatible with the TLS versions enabled in this section. To review the TLS settings on the TPS device, go to the TPS device, and then select **Device Configuration** > **Services**.

If TLS v1.2 is enabled and you are using the Identity Agent with TLS v1.2 enabled, the SMS must be running with the 2K key. For more information, see *SMS certificate key on page 8-9*.

If you have trouble managing a TippingPoint SSL appliance 1500S, set the TLS version to 1.0 only.

Before you edit the TLS versions, note the following caveats:

- You must select at least one TLS version for each communication category. Due to security reasons, we recommend that you disable TLS v1.0 and SSLv3.0 if they are not required in your network environment.
- The TLS versions for some devices are incompatible with the SMS. Before you configure the TLS versions settings, review the list of unsupported devices available on the TMC.
- Editing the TLS versions requires a restart of the SMS.

For more information on the supported cipher suites for the TLS versions, see *SMS encryption protocols, algorithms, and cipher support on page 4-9*.

Procedure

1. Go to **Admin** > **Server Properties**, and then select the **TLS** tab.

2. Review the current state for each communication type. A check mark indicates if a TLS version is enabled. If it is not, the radio button is unselected and the current state displays as Disabled.
3. Click **Edit** to edit the TLS versions.
4. Select one or more TLS versions for the communication categories:

Note

You must select at least one TLS version for each communication category.

   - Click **Select All Settings** to quickly select all versions for all communication categories. Clear the check box to quickly remove all version selections for the communication categories.
   - Click **All TLS v1.0** to quickly select all v1.0 versions for all communication categories.
   - Click **All TLS v1.1** to quickly select all v1.1 versions for all communication categories.
   - Click **All TLS v1.2** to quickly select all v1.2 versions for all communication categories.
   - Click **All SSL v2Hello** to quickly select the SSL v2Hello versions for the Web Server and IPS Remote Authentication communication categories.
5. If there are incompatibilities between the SMS TLS versions and the managed device TLS versions, the SMS will display warnings and/or errors. Click **Details** to review the severity and descriptions. If there are any errors, you cannot save your changes until you select compatible TLS versions.
6. Click **OK**. Editing the TLS versions requires a restart of the SMS. Click **Yes** to immediately reboot the SMS and commit the TLS versions.

Named resources

To help you to group and manage the unique identification of resources, the SMS uses *named resources*. You can define and use named resources within the system for:

- **Devices** — Exception Rules, Servers, Management Routes
- **Events** — Inspection Events (Source and Destination Addresses)
- **Profiles** — Restrictions and Exceptions (Source and Destination Addresses)
- **Responder** — Policies (Inclusions and Exclusions)

Named resources are similar to aliases, and named resource groups are similar to groups of aliases. The SMS supports, and in some cases requires the creation of, named IP addresses, VLAN IDs, and named email addresses. For example, when you configure the SMS to deliver SMTP messages, you must create a named email address group for the recipient list. In another example, if you allow the creation of an external SMS database, you can restrict access to that database instance to only those members included in a specific named IP address group.

Important

Access to named resources functionality is based on user roles. Users with SuperUser capabilities can create or edit named resources; users with SuperUser or Admin capabilities can view named resources; users with Operator capabilities do not have access to named resources.

Resource types

The SMS uses three types of resources: unnamed, named, and permanent.

Locked resource	Description	User Capabilities	
		Edit	Delete
Unnamed resources	Automatically assigned and used for autocomplete when you enter a value in a field that supports named resources. Select the **Show Unnamed Items** check box to show or hide these values. If you create a filter exception without assigning the source or destination IP address to a named IP address group, then you have created an unnamed IP address group. The IP address group exists on the SMS, but the SMS does not have a way to identify the name of the group.	No	Yes
Named resources	Created by the user.	Yes	Yes
Permanent resources	Created by the SMS and not by the user.	No	No

Note

Named resources are used only on the SMS. In its communication with the device, the SMS sends only the constituent parts of a named resource (IP addresses, CIDR, and email address) to the device. The named resource itself is not sent.

View whether a named resource is in use

Click **Show References** to view whether the named resource is currently in use. If it is in use, the SMS displays the respective settings for the named resource.

Save a copy of a named resource

Click **Save As** to create a copy of the named resource or named resource group with a different name.

Delete a named resource

You cannot delete a named resource if it is currently in use on the SMS. When you click **Delete**, the SMS displays the respective settings for the named resource. You must first remove the named resource from these associated items before the named resource itself can be deleted.

Create or edit a named resource

A named resource is an individual resource, typically created to be included in a named resource group.

Procedure

1. Select **Admin** > **Named Resources**.
2. Depending on the named resource you want to create (or edit), select either the **Named IP Addresses** tab, the **Named VLAN IDs** tab, or the **Named Email Addresses** tab.
3. Below the named resource table (located at the bottom of the screen), do one of the following:
   - Click **New** to create a new named resource.
   - Select an existing named resource, and click **Edit**. You cannot edit unnamed or permanent named resources. See *Named resources on page 8-123*.

   Select the **Show Unnamed Items** check box to show or hide any unnamed resources that exist on the SMS.
4. Enter a **Name** for the named resource.

Note

You cannot use special characters or spaces.

---

5. (Optional) To create a named IP Address:
   a. Select **IP Host**, and enter the single IP address.

b. Select **IP Subnet**, and enter the IP address in CIDR notation.

c. Select **IP Range**, and enter the range of IP addresses.

6. (Optional) To create a named VLAN ID:

a. Select **VLAN ID**, and enter a numeric tag, assumed to be 802.1Q compatible, and has a max value of 4094. IDs must between 1 and 4094 inclusive.

b. Select **VLAN ID Range**, and enter the range of VLAN IDs.

7. (Optional) To create a named email address, enter an Email Address.

8. Click **OK**.

Create or edit named resource groups

You can use named resource groups to simplify assigning actions or notifications to multiple resources on the SMS.

Procedure

1. Select **Admin** > **Named Resources**.

2. Depending on the named resource group you want to create (or edit), select either the **Named IP Addresses** tab, the **Named VLAN IDs** tab, or the **Named Email Addresses** tab.

3. Below the Groups area (located at the top of the screen), do one of the following:

- Click **New** to create a new named resource group.
- Select an existing named resource group, and click **Edit**. You cannot edit unnamed or permanent named resource groups. See *Named resources on page 8-123*.

Select the **Show Unnamed Items** check box to show or hide any unnamed resource groups that exist on the SMS.

4. Enter a **Name** for the named resource group.

Note

You cannot use special characters or spaces.

5. To include a resource in the named resources group, select it in the left (Available) list panel, and click the right arrow to move it to the right (Selected) list panel.

Note

If the Available list panel is empty, then no named resources of this type have been defined. Click **New** to create an individual named resource. See *Create or edit a named resource on page 8-125*.

6. (Optional) To remove a resource from the named resource group, select it in the right (Selected) list panel, and then click the left arrow to move it to the left (Available) list panel.
7. (Optional) Select the **Show Unnamed Items** check box to show or hide any unnamed resources that exist on the SMS.
8. Click **OK**.

Import or export named resources

Procedure

1. Select **Admin** > **Named Resources**.
2. Depending on the named resource you want to import (or export), select either the **Named IP Addresses** tab, the **Named VLAN IDs** tab, or the **Named Email Addresses** tab.
3. Below the named resource table (located at the bottom of the screen), do one of the following:
   - Click **Import**, browse to and select the file, and then click **Open**. If the file format is valid, the **Finish** button is enabled.

Note

The imported file must contain only comma-separated values (CSV) or tab-separated values (TXT), without column headings or spaces in the names.

- Select an existing named resource, and click **Export**. Browse to the directory in which you want to save the file, enter a filename, and click **Save**.

Exports and archives

The Export and Archives screen provides a convenient location to store files on the SMS. In the Admin workspace, select Exports and Archives in the navigation pane to display this screen.

When you back up the SMS database or create a snapshot, the SMS client displays these files on the Export and Archives screen. This screen shows the following information for each file:

- Filename – File name, including the file extension.
- Size – File size in bytes.
- Last Modified – Date and time the file was last changed.

Export a file from the SMS exports and archives directory

Procedure

1. On the Exports and Archives screen, select a file, and then click **Export**.
2. In the dialog, click **Save**.

Delete a file from the SMS exports and archives directory

Procedure

1. On the Exports and Archives screen, select a file, and then click **Delete**.
2. In the Delete File dialog, click **Yes**.

   To refresh the Exports and Archives list, click **Refresh**.

IP address identifier

The IP Address Identifier screen allows you to define address groups, enable event monitoring for IP addresses and address groups, and activate lookup services for a specified set of IP addresses. By default, all IP addresses in the network are monitored. You can modify the settings for any IP Address group that is configured for IP Address Identifier, or create new IP address groups containing one or more specific IP addresses to target for monitoring.

The IP Lookup Services enable you to specify and view selected metadata for monitored events associated with a given IP address or host. The IP Address Identifier screen lists address groups that the SMS is configured to monitor, which consists of the information described in the following table.

Column	Description
Order	Order of priority.
Icon	Icon that distinguishes the event when viewed.
Name	Name or identifier of the IP address group.
Address(es)	Addresses included in the IP address group; an asterisk (*) indicates all addresses.
Geo	Indicates whether Geo Locator lookup service is enabled for the address group.
NR	Indicates whether Named Resources lookup service is enabled for the address group.

Column	Description
DNS	Indicates whether DNS lookup service is enabled for the address group.
User ID	Indicates whether User ID lookup service is enabled for the address group.
Rep	Indicates whether reputation filter lookup service is enabled for the address group.
End Point	Indicates whether End Point Attributes lookup service is enabled for the address group.

Add or edit an IP address ID

Procedure

1. On the IP Address Identifier screen, click **New**, or select a row, and then click **Edit.**
2. In the New/Edit Ip Addr Id Entry dialog, provide a name for this entry.
3. Leave the **All Addresses** option selected, or select **Specified Addresses**, and then do the following:
   a. Click **Add**, and then select one of the following options:
      - Host/Subnet/Range – add one or more IP addresses, subnets, or ranges.
      - Named IP Address Groups – select one or more named IP address groups.
      - Named IP Addresses – select one or more named IP addresses.

   b. In the dialog, provide the required information, and then click **OK**.
4. Click **Next**, and then provide any custom metadata to be applied to the specified addresses.

   You can select the following options:

   - **End Point Attributes** – Specify operating system and manufacturer.
   - **Network Location** – Specify network location to apply end-point network location metadata.

- **Custom Attributes** – Specify one or two custom attributes that you describe.

5. Click **Next**, and then choose from the following Decoration options:
   - Select **No Icon**, or click **Apply Icon** and select or import an icon.
   - Select **No Color**, or click **Apply Color** and choose a color.

Note

By default, no color and no icon is applied to the entry.

6. Click **Next**, and then select lookup services to activate for the specified addresses. See *Look up an IP address or hostname on page 10-2*.
7. Click **Finish**.
8. Click **OK**.

Note

You can access all the IP Lookup services from the Tools menu. See *Tools on page 10-1*. You can also use the WhoIs utility to perform a WhoIs query from the Tools menu.

Delete an IP address ID

Procedure

1. On the IP Address Identifier screen, select an entry in the list.
2. Click **Delete**.
3. In the Confirm Delete dialog, click **Yes**.

Change the priority order for IP address groups

Procedure

1. On the IP Address Identifier screen, select an entry in the list.
2. Click **Move Up** or **Move Down** to change the order of priority.

   The list changes dynamically to show the new position of the entry in the IP Address Identifier table. The priority order helps you manage the Address Groups.

User ID IP Correlation

Once an Identity Agent is added to the SMS, the SMS will automatically poll the agent and will display the User ID to User IP correlation and security login events. With this data, you can search an IP address to view all historical information. When you first connect the Identity Agent in the SMS, the SMS will automatically poll the domain controller to get the last 15 minutes of historical information.

Note

When the SMS is in FIPS mode, it will not be able to communicate with the Identity Agent.

Polling times

The following table defines the polling times for the security login events and metadata and diagnostics.

Item	Polling time
Security login events	Every 4-5 seconds
Metadata and diagnostics	Every 15 minutes

Note

These are the default times. You can update the polling settings in the Identity Agent.

Note

You can manage the User ID IP Correlation data maintained by the SMS when you perform Database Maintenance and specify retention parameters for the data. See *Database maintenance on page 8-71*.

High level SMS and Identity Agent configuration process

There are four steps to configure the Identity Agent in the SMS in order to retrieve User Id IP correlation.

1. *Add the Identity Agents on page 8-133*.
2. *Create an Agent Group on page 8-134*.
3. *Select an Identity Agent to be in a group on page 8-135*.
4. *Enable the Agent Group on page 8-135* that will be actively used by the SMS to poll the Identity Agent for User ID IP correlation data.

Add the Identity Agent

Procedure

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **Identity Agent Groups**.
3. Create an agent by opening the **Identity Agents** tab and clicking **New**.
4. Specify the following information of the Identity Agent:
   - IP address of the hostname
   - Port. The default port is 8443.

- (Optional) Description or comments about the agent.

5. Click **OK**.

   The agent is added to the Identity Agent table.

Create an Identity Agent Group

Each Identity Agent must be added to a group before the SMS can retrieve events. Agents in a group can also be used for redundancy.

Procedure

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **Identity Agent Groups**.
3. Create an agent group by opening the **Identity Agents Groups** tab and clicking **New**.
4. Specify the following information of the Identity Agent group:
   - Name of the agent group.
   - Domain name. This information gets automatically retrieved from the identity agent. All agents in a single group must belong to the same domain.
   - (Optional) Description or comments about the agent group.
   - Number of retries before the SMS attempts to contact the next agent in the group.
   - Number of seconds the SMS waits for a connection to the agent.
   - Number of seconds the SMS waits for a failed connection.
5. In the Identity Agents area, select from the available Identity Agents to add to the group.

   Up to four agents can be added to a group. Use the Up and Down arrows to reorder the priority of the agents. The SMS attempts a connection to only one agent at a time, beginning with the first one in the list.

6. Click **OK**.

   The Identity Agent group is added to the Identity Agent Group table. Click **Show References** to see which devices reference the group.

Select an Identity Agent to be in a group

Select an Identity Agent group to use for the User ID IP Correlation.

Procedure

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **User Id IP Configuration**.
3. Select an agent group by clicking **Add**.
4. In the User Id IP Configuration area, select from the available Identity Agent groups. Use the Right and Left arrows to add or remove a group. Alternatively, click **New Identity Agent Group** to create a new group.
5. Click **OK**.

   The Identity Agent group is added to the Identity Agent Groups table.

Enable Identity Agent group

Enable the Agent Group that will be actively used by the SMS to poll the Identity Agent for User ID IP correlation data.

Procedure

1. Click **Admin** on the SMS toolbar, and then expand **User Id IP Correlation** in the navigation pane.
2. Click **User Id IP Configuration**.
3. Right-click on an agent group, and then click **Enable**. To disable an Identity Agent group, click **Disable**.

A checkmark appears in the Enabled column.

User ID IP Correlation events

Once the SMS is configured with the Identity Agent, the SMS automatically polls the agent, and the user login and group information displays in the User ID IP Correlation table. You can use this data to correlate events to user information. This data is used for SMS reports.

You can also search an IP address to view historical information.

Column	Description
Time	Specifies the date and time that the event was retrieved by the SMS.
IP Address	Specifies the IP address of the security login event.
User Name	Specifies the user name.
Domain	Specifies the user domains.
Machine	Specifies the user machines.
Member of Groups	Specifies all of the groups for the user.

Note

You can manage the User ID IP Correlation data maintained by the SMS when you perform Database Maintenance and specify retention parameters for the data. See *Database maintenance on page 8-71*.

Unknown user

The SMS may display "unknown" for the following reasons:

- Any security event that happened before the Identity Agent was installed.
- The user is not logged into a domain that is monitored by an agent which SMS is using.

- The user is logged on a non Windows system
- The user is logged on a system that uses something other than Active Directory for authentication
- Any IPs that are listed in the **Unmapped IPs** area in the Identity Agent.
- A remote IP address outside of your corporate network that cannot be correlated by the Identity Agent.

Configure a user resolver filter

Procedure

1. On the User Resolver panel, click **Configure a User Name Filter**.
2. In the Configure User Names dialog, select the check box to filter out all user names that end with a *$* character.

   Note

   The user name filter option is a convenient way to filter out recurring system events, such as Windows system service events. To filter out all system logons that end with "$" select the associated check box.

3. Click **Add**.
4. In the Add User Name dialog, specify a User Name and Domain. When the specified user logs on or off, the associated events are ignored for Active Directory monitoring purposes.
5. Click **OK**.

Geo Locator Database

The SMS uses geolocation databases to retrieve geographical information associated with IP addresses to:

- Correlate the country of origin for host IP addresses associated with events.

- Query the database to view the country location for a specified host name or IP address.
- Display a map showing the country of origin for all IP addresses generating events.
- Display event details, reporting information, and *IP Lookup results on page 10-2*.

You can import the Geo Locator Database from the TMC. You can also import Geo IP files from MaxMind. The SMS supports certain GeoLite Legacy and GeoLite2 databases (GeoLite2 City). Zipped database files must be in CSV format. To download the GeoIP database, go to https://dev.maxmind.com/geoip/geoip2/geolite2/.

Automatically download a Geo Locator package

Enable the SMS to automatically download a Geo Locator Database package file from the TMC.

Procedure

1. Select **Edit** > **Preferences** > **TMC Information share**, and select **Enable TMC Polling for DV, OS, GEO DB, and License Package updates**.
2. Go to **Admin** > **Geo Locator Database**, and click **Enable**.

   The SMS periodically checks the TMC for the latest version. If available, the SMS will automatically download and import the database package.
3. (Optional) Click **Disable** to stop the automatic Geo Locator Database download.

Download latest Geo Locator package from the TMC

Procedure

1. Go to **Admin** > **Geo Locator Database**.

2. Click **Check Now** to download the latest version of the Geo Locator package from the TMC, if available.

Import a Geo Locator database file

Procedure

1. On the Geo Locator Database screen, click **Import**.
2. In the dialog, locate the database file you downloaded.
3. Select the file, and click **OK**.

   If the Automatic Geo Download is disabled, the SMS displays a dialog box when the import is complete. If the Automatic Geo Download is enabled, the SMS displays a dialog box asking if you want to disable automatic Geo Locator package updates.

Licensing

The Licensing page contains information about the status and the availability of Trend TippingPoint products and services for licensed devices. If your SMS has TMC connectivity, you can configure the System Preferences to poll for license entitlement package updates. See *TMC information share on page 11-4* for more information.

The TippingPoint License Package panel displays the following license information:

- **Status** – Top-level indicator of the status of your license entitlement package
- **Version** – License entitlement package version
- **Package Timestamp** – Day and time that the current license entitlement package was created
- **Notification Settings** – Current notification options for receiving results of the SMS daily check for license entitlement package issues. Options include email notifications and SMS system log notifications.

Note

If you receive license status errors, log in to your TMC account and check for a license entitlement package update. See *Licensing details on page 8-143* and *Import a license entitlement package on page 8-142*.

Trend TippingPoint License Manager

The license manager, which is accessible from the TMC by navigating to **My Account** > **License Manager**, allows you to manage the licenses and certificates for your TPS products. This licensing model enables you to attach and detach speed and feature licenses for your TPS devices.

For more information, see the *License Manager User Guide* available from the license manager.

Default and licensed inspection throughput for TPS devices

Before a license entitlement package is installed on a device, each device has a limited, default inspection throughput. Contact your sales representative to purchase an inspection throughput license compatible with your device to increase the inspection rate.

Any TPS device inspection throughput license can be assigned to a compatible TPS device. For instance, a 1 Gbps inspection throughput license can be assigned to a 440T, 2200T, or vTPS device. The following table displays both the default inspection throughput and the inspection throughput options available for purchase for each device.

Device	Default inspection throughput	Purchasable inspection throughput
440T	100 Mbps	250 Mbps, 500 Mbps, 1 Gbps
2200T	200 Mbps	1 Gbps, 2 Gbps
1100TX	100 Mbps	250 Mbps, 500 Mbps, 1 Gbps
5500TX	100 Mbps	1 Gbps, 2 Gbps, 3 Gbps, 5 Gbps

Device	Default inspection throughput	Purchasable inspection throughput
8200TX	1 Gbps	3 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps, 30 Gbps, 40 Gbps
8400TX	1 Gbps	3 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps, 30 Gbps, 40 Gbps
9200TXE	1 Gbps	40 Gbps, 60 Gbps, 80 Gbps, 100 Gbps
vTPS	100 Mbps	250 Mbps, 500 Mbps, 1 Gbps, 2 Gbps

Note

You must install a vTPS certificate package on a vTPS to activate the capabilities purchased with the vTPS device license package.

SSL inspection licenses

With TOS v5.0.0 and later, SSL inspection is supported on TPS 2200T, 5500TX, 8200TX, 8400TX, and Virtual TPS (vTPS) security devices. With TOS v6.0.0 and later, SSL inspection is supported on TPS TXE-Series devices. SSL inspection is not supported on the 440T or 1100TX TPS security device.

Edit notification settings

The SMS runs a daily check for licensed capability expiration and other license entitlement package issues.

Procedure

1. Select **Admin** > **Licensing**.
2. Under TippingPoint Licensing Package, click **Edit**.
3. Select notification settings to specify whether to receive the results of this check by email or by an entry in the SMS system log. You can specify one, both, or none of these options.

4. Click **OK**.

Import a license entitlement package

Complete the following steps to manually import a device license entitlement package.

If your SMS is connected to the TMC, you do not need to manually import the entitlement file. The SMS automatically downloads the entitlement files from the TMC any time there is an update. See *TMC information share on page 11-4* for more information.

Note

It might take up to 30 minutes for a new license entitlement package to automatically update on the TMC database and for the SMS to reflect the change on the managed devices. Changes to the software, DV, and ThreatDV licenses are made automatically, but changes to the license-designated throughput speed require a device reboot to take effect.

To manually import a device license entitlement package

Procedure

1. Download the entitlement package from the TMC.
   a. Log on to the TMC at https://tmc.tippingpoint.com.
   b. From the TMC, navigate to **My Account** > **TippingPoint License Package**.
   c. Download and save the appropriate license entitlement package file to your local system.
2. On the SMS, select **Admin** > **Licensing**.
3. Under Capacity Licensing Package, click **Import**.
4. Select the license entitlement package file to import, and then click **Open**.

Note

You can only import license entitlement files that match a valid device managed by the SMS and visible in the Licensing Details panel. An error message appears if you try to import an invalid entitlement package.

5. Click **OK**.

Licensing details

The Licensing Details panel displays status and information for the license on each managed device.

Column	Description
Device/Capability	Displays the device serial number. Expand to view capabilities including maintenance, TOS updates, Digital Vaccine updates, Threat DV updates, and SSL Inspection throughput.
Device Name	Device name and IP address.
Type	Device type: IPS or SMS.
Model	Device model.
Contract End	License expiration date for each device.
Activation Code	Unique identification number assigned to the hardware, inspection throughput speed, Threat DV, and SSL license components.
Action	Displays the action for your license contract: Allow or Deny.

Column	Description
Details	Displays a color-coded status for your license contract: • Green - You **are** receiving updates. • Yellow - You **are** receiving updates. You are within 14 days of the contract end date. • Red - You **are not** receiving updates because you are past the contract end date and your license package has expired. • Grey - You **are not** receiving updates.
Hardware Serial Number	The device hardware serial number.

Expires within

Use the Expires Within field to sort the results in the Licensing Details panel by the expiration dates of the device licenses. Select the drop-down list to choose a time range from **One Week** to **Never** or select the start and end time to manually sort the table information by specific dates and times.

Export license details

You can export licensing details to a .csv (comma delimited, with or without column headings) or text file (tab delimited, with or without column headings). The device identifier appears on each line.

Procedure

1. Select **Admin** > **Licensing**.
2. Select one or rows on the Licensing Details table, right-click, and then select **Export to file**.
3. Select **Selected Rows** or **All Rows**.
4. Enter a file name, select a file type, and then click **Save**.

SMS High Availability

You can configure the SMS to operate in an active-passive, high availability (HA) cluster, increasing availability of the SMS when an unexpected event causes the primary SMS to fail or become inaccessible. The SMS HA cluster consists of two nodes, a primary and a secondary. If the primary SMS becomes unavailable, the secondary SMS becomes active.

In the Admin workspace, select **High Availability** in the navigation pane to display the Admin (High Availability) screen. From this screen you can configure and adjust the SMS HA settings, synchronize the two nodes, and monitor the HA cluster status. *Learn more on page 8-147*.

Synchronization

During initial configuration, the SMS synchronizes the database from the active SMS to the passive SMS. To keep the passive SMS current, the active SMS replicates critical SMS data to the passive SMS.

Failover

The process of promoting a passive SMS server to an active SMS server is called failover. A failover occurs when the primary SMS server experiences a fault or is taken offline for maintenance. You can also manually failover the cluster and swap roles between the active and passive SMS servers. *Learn more on page 8-154*.

Heartbeat

When the cluster is operating in a normal state, the passive server periodically sends a heartbeat signal to the active server.

If the passive server is unable to obtain a response from the active server, the passive server assumes the active server is unavailable and initiates a failover process. The total heartbeat timeout and the mitigation timeout are configurable fields that determine the total time the passive SMS spends to recover from a heartbeat failure. *Learn more on page 8-151*.

Network configuration

You can configure SMS HA to send the heartbeat over one of two possible network configurations. SMS HA can send the heartbeat over the same public network that the SMS uses to communicate to its clients and managed devices. Alternatively, you can instruct the SMS to send the heartbeat over a private, intra-cluster Ethernet network. If you use an intra-cluster network, the replication activity occurs over this private network, removing the traffic from the public network.

If you configure SMS HA to use the private network, your configuration also has built-in redundancy. If the heartbeat signal does not make it through the private network, the SMS attempts to communicate the heartbeat through the public network before initiating a failover. To make use of an intra-cluster network, connect an Ethernet crossover cable between the two cluster nodes and configure SMS HA to use a primary and secondary network configuration.

Cluster requirements

Compatibility requirements

- **System resources** – Both systems must have similar memory, CPU, and disk space. Both systems must also have the same disk partitions, which are set during initial install and are identified internally by a partition number.
- **FIPS mode** – Both systems must have the same FIPS mode configured. FIPS mode cannot be changed when HA is configured.
- **SMS certificate key** – Both systems must have compatible SMS certificate key sizes. For example, the active SMS cannot be running a 1K key and the passive SMS be running a 2K key. You cannot install the 2K key in either SMS while the SMS is running in HA. To install a 2K key, disable the cluster, install the 2K key on each SMS, and then reconfigure the cluster. A 2K key is required on both systems if HA is configured in FIPS mode.
- **SNMP** – You cannot modify SNMP settings for the passive SMS server after you configure SMS HA. If you use SNMP to monitor and manage your SMS servers, you must configure the SMS's connectivity to an

SNMP server before you configure the SMS HA cluster. To modify SNMP settings, disable the cluster, modify the SNMP settings on both servers separately, and then reconfigure the cluster.

Unsupported features

- **IPv6** – SMS HA is not supported with IPv6. If the SMS is IPv6 only, the HA configuration button shows an error when selected.
- **External database replication** – External database replication and SMS HA features both leverage the same functionality in the underlying database. The SMS database does not support replication to multiple destinations; therefore, Trend does not recommend using SMS HA and external database replication at the same time.

Replication bandwidth requirements

The SMS has replication bandwidth requirements for heartbeat, event traffic, and downloads for digital vaccines (DVs) and upgrade packages.

- Less than 10 Kb/s bandwidth is required for heartbeat and system usage/ administration operations, such as policy management.
- A minimum of 1 Mb/s bandwidth is recommended to download DVs and upgrade packages. These operations consume as much bandwidth as is available between the two systems, but headroom of about 1 Mb/s keeps the two systems reasonably synchronized.
- Event traffic requires approximately 1.5 Mb/s per 1,000 events/second.

Configure the cluster

Configure an SMS HA cluster from the primary SMS server. The active SMS server must manage all of your devices. After you configure SMS HA, the SMS client can no longer log in to the passive SMS.

Procedure

1. In the Admin workspace, select **High Availability** in the navigation pane.

2. Click **Configure** on the HA Cluster Status panel.
3. In the SMS High Availability wizard, click **Next**.
4. Select replication options:
   - **Enable Event Data Replication** – Replicates event data from the active SMS to the passive SMS. This option is already selected by default.
   - **Enable Encrypted Replication** – Encrypts replicated data. This option does not affect data replication during synchronization, which automatically occurs over a secure channel.

Note

If you clear the **Enable Event Data Replication** check box, the new events are not replicated from the active server to the passive server. Only turn this off when the SMS is already configured to use an external log process server like the Reporting Server and SIEM.

5. Click **Next**, and specify the parameters that the SMS server uses to determine the timeout values:
   - **Total Heartbeat Timeout** – Indicates the total time the passive SMS uses to recover from a heartbeat failure. This option is set to three minutes by default but can be adjusted from two to four minutes.
   - **Mitigation Timeout** – Indicates the total time the passive SMS spends on mitigation. This option is set to five minutes by default but can be adjusted from four to six minutes.

   When the passive SMS detects a health check failure, the maximum time the SMS spends on the recovery process is the sum of the total heartbeat and mitigation timeouts. *Learn more on page 8-151*.
6. Click **Next**, and then choose the appropriate network configuration:
   - **Primary Only** – All communications occur over a single network interface.
   - **Primary and Secondary** – Replication and heartbeat signals occur over a secondary, intra-cluster, network path.

7. Click **Next**, and then do the following:

   - To use a Shared Virtual Management IP address, select the check box and enter the IP address.

Note

The Shared Virtual Management IP address and the Maintenance IP addresses of the active and passive SMS servers must be in the same subnet.

   - Provide the maintenance IP address for the passive SMS server.

8. Click **Next**, and then do the following if you specified a primary and secondary network configuration:

   a. Provide the secondary IP addresses for the active and passive SMS.

   b. If you do not require the IP addresses to reside in the same subnet, clear the check box and provide gateway IP addresses for the active and passive SMS servers.

   c. Click **Next**.

9. Enter the login credentials for the passive SMS server. The credentials must be those of a user with SuperUser permissions.

10. Click **Configure**.

    The Configuration Status dialog box displays ongoing status. When the configuration finishes, the HA Cluster Synchronization dialog box opens.

11. Select **Synchronize the HA cluster**. To include all historical event data, select **Include historical event data**.

Note

If you include historical event data, depending on the size of your event database, it can take several hours to synchronize the cluster.

12. Click **Finish**.

    All client connections are disconnected because access to the SMS database is prohibited during the synchronization process. To monitor progress, click **More**. The HA Synchronization Status dialog displays a progress bar, time elapsed, and more.

    When synchronization finishes, the SMS client automatically attempts to re-establish a connection with the active SMS server. When the connection is re-established, the SMS client opens to the Admin (High Availability) screen.

Note

Powering off the SMS while HA is enabled could result in unrecoverable file systems and database corruption. If an SMS node is inaccessible, SSH to it from its peer node and manually restart the SMS database and server services. If necessary, perform a shutdown or restart of the cluster from the primary SMS cluster using a CLI command.

13. Verify the operational state of the cluster.

    The active SMS status displays Active, and the passive SMS status displays Passive.
    If you chose the primary and secondary network configuration, verify that the Heartbeat IP addresses for each SMS cluster node are performing as expected. The SMS monitors the needs to synchronize the cluster nodes. In typical operation, you do not need to initiate another synchronization. However, if you manually failover a cluster node or take one of the nodes offline, you need to re-synchronize the SMS cluster.

Configure servers in different locations

You can configure the SMS server for HA while the servers are located in different geographic locations. With this configuration, it is important to maintain the link between both SMS servers to make sure the network provides enough bandwidth for the heartbeat signal and the database replication.

By default, each node sends a heartbeat signal to its peer node every minute. If network issues prevent both nodes from receiving three consecutive heartbeat signals, the passive node initiates automatic failover even though it is possible for both server nodes to be functional. This can result in two active SMS servers in the same node configuration. To avoid unnecessary SMS HA server failover, ensure that the network has a reliable link between the SMS servers with a bandwidth delay of less than 300 ms. Monitor the primary SMS server to make sure it is not overloaded and has adequate resources including memory, file systems, and threads.

Adjust the timeout values

After you configure the SMS HA cluster, you can adjust its timeout values. For example, if the primary and secondary servers are located in different geographic regions or if you experience intermittent connectivity issues, you can increase the HA timeout values to prevent a heartbeat failover. However, if the two SMS servers are co-located or are on a low latency network, use the default timeout configuration values (three minutes for the total heartbeat timeout and five minutes for the mitigation timeout).

If the passive and active server-to-server communication is lost, the passive SMS initiates a mitigation process, which may include restarting the SMS. Set the time the passive SMS spends on mitigation in the Mitigation Timeout field.

When the passive SMS detects a health check failure, the maximum time the SMS spends on the recovery process is the sum of the Total Heartbeat Timeout and Mitigation Timeout fields.

Procedure

1. Click **Timeouts**.
2. In the dialog box, adjust the total heartbeat and mitigation timeout values as needed.

View the cluster status

The HA Cluster Status panel displays the current status of the SMS HA cluster and configuration settings, which include the management IP address and network, and event replication status data.

The nodes transition through these states. If a transition failure occurs, the node reverts to the previous state.

1. Un-configured
2. Configured
3. Primary: synchronization-source, Secondary: synchronization-target (synchronization state is transitional state).
4. Restart
5. Primary node is active and the secondary node is passive.

HA Cluster Status and HA Replication Delay metrics are displayed in graphs to help you track the status of the SMS HA cluster. The HA Replication Delay metrics show how many seconds the passive SMS is behind the active SMS in data replication.

The SMS displays information for the active and passive SMS.

From within the passive SMS area, you can manually activate the passive SMS server, which in turn deactivates the current active SMS server by invoking a failover. You can also swap roles of the active and passive SMS servers. *Learn more on page 8-154*.

Synchronize the cluster

Synchronize the SMS HA cluster to restore the cluster to a fully-functional state. Synchronizing the cluster synchronizes the database and configuration files to the passive server and restores the primary SMS to active status. When you synchronize the SMS HA cluster, the SMS client is temporarily disconnected while the SMS server on each node in the cluster automatically restarts.

Before you begin

Before performing a synchronization, investigate and resolve any server-related issues on the primary SMS server that may have resulted in an automatic failover to the secondary node.

When investigating SMS server issues, consider the following:

- The number of managed devices
- The rate at which the SMS server receives device events
- Profile distribution
- DV distribution

Procedure

1. On the HA Cluster Status panel, click **Synchronize**.

   If the **Synchronize** button is disabled, it is not necessary to perform a synchronization.

2. Choose to include, or not include, historical event data in the synchronization.

   Note

   If you include historical event data, depending on the size of your event database, it can take hours to synchronize the cluster.

3. Select the synchronization source, either the default source which is the most recent active SMS server or specify another source from the drop-down list.

4. Click **OK**.

   When the synchronization completes, the IP address of the original primary SMS appears under the Active SMS group with a status of Active.

Swap the cluster node roles

On the High Availability screen, you can swap the roles of the SMS HA cluster nodes to promote the passive SMS to the active SMS, and reconfigure the active SMS to the passive SMS.

This process can take several minutes, during which time the SMS HA cluster is re-synchronized, nodes are restarted, and the SMS client is temporarily disconnected to re-establish the SMS HA cluster to a fully functional active-passive state. The operational state of the cluster is shown as Configured for the active SMS server and for the passive SMS server until the synchronization process finishes.

Invoke a failover

Invoke a failover to activate the secondary SMS server and deactivate the primary SMS. Failover the cluster when you want to verify that the initial configuration of the HA cluster works properly or to perform maintenance on the primary SMS.

To reactivate your primary node and reinstate the SMS HA cluster to a fully functioning high-availability state, make sure that the primary node is online and then synchronize the SMS HA cluster. *Learn more on page 8-152*.

Deactivate the active server

The most important aspects of the SMS HA cluster are the heartbeat connection and database replication. Periodically, verify that both activities are performing as expected.

Two methods are available in the Admin - High Availability screen to deactivate the active SMS server:

- **Swap** – Swaps the roles of the SMS HA cluster nodes. This process re-synchronizes and restarts the nodes to ensure that HA status of the cluster is maintained. This process involves a temporary disconnect of the client and is temporarily more disruptive than failover. For more information, see *Swap the cluster node roles on page 8-154*.
- **Failover** – Invokes a failover of the active node in the SMS HA cluster, thereby activating the passive SMS server. To bring the failed-over node

back online and reinstate a fully functioning HA cluster, you must manually synchronize and restart the deactivated node. For more information, see *Invoke a failover on page 8-154*.

If you need to perform maintenance on the active SMS server, for example to swap out a network card, you can invoke a failover on the active node, which deactivates it and activates the passive SMS server. When it is deactivated you can take the node offline, power it off, and perform maintenance.

Disable the cluster

Disable the HA cluster before you apply software upgrades, patches, or hotfixes that include database updates.

SMS clients use an IP address or a hostname to connect to an SMS server. When an SMS client first connects to an SMS HA cluster, it obtains and caches the IP addresses of each cluster node. When you disable the cluster, you break the cluster into separate, independent systems with identical configurations. Ensure one of the SMS servers is rendered inaccessible to SMS clients and devices so that the two servers do not compete with each other. To avoid device management conflicts after you disable SMS HA, you can either power off the SMS that is not being used or perform a factory reset.

Because only one SMS can manage a device, the device always records the IP address and the certificate of the SMS in the HA cluster that manages it. This also prevents another SMS from taking control of the same device.

Under normal HA failover conditions, the certificate from the active SMS is copied to the passive SMS and used to manage the devices. If the cluster fails-over or is swapped, then the devices are still seamlessly managed with the same certificate.

If the original passive SMS server becomes the active SMS server and you disable HA, then the SMS displays a dialog with two list panels.

- The left panel identifies devices that will continue to be managed by the currently active (original secondary) SMS.

- The right panel identifies devices that will be unmanaged by the currently active SMS. The devices in this right panel will be managed by the currently passive (original primary) SMS unless you unmanage them and remanage them on the currently active SMS.

Apply software updates to a cluster

Upgrades: Disable the HA cluster before you apply software upgrades. To upgrade an HA cluster, upgrade each SMS server separately, and then re-establish the cluster. You cannot upgrade the passive SMS server while HA is enabled because the low-level services that are running on the passive node do not perform software upgrades or database updates, and because database updates on the passive node break database replication and as a result, data integrity.

Patches or hotfixes: Before applying a patch to an SMS HA cluster, determine whether the patch includes database updates:

- If the patch contains database changes, be sure to disable the SMS HA cluster, apply the patch to each SMS server separately, and then re-establish the cluster. Applying a database patch while under SMS HA breaks database replication and as a result, data integrity. The patch process does not prevent you from applying a database patch while under SMS HA.
- If the patch does not contain database changes, initiate the patch process from the active SMS server. The active SMS server automatically propagates the patch to the passive SMS server. If the patch requires a restart of the SMS software or a reboot of the SMS server, the action takes place on both the active and passive SMS servers.

Troubleshooting

This section discusses common troubleshooting techniques.

Collect logs

Collect SMS logs from both the primary and secondary SMS HA servers with these commands:

- Primary SMS server:

```
set logs.create=yes
```

- Secondary SMS server:

```
set logs.create-peer=yes
```

If this command is unsuccessful, SSH to the secondary SMS server and run the primary SMS command.

SMS out of Java Heap memory

A Java Heap memory error occurs when there is not enough Heap memory left for the application to operate correctly.

Run one of the following commands to check for out-of-memory errors:

- `grep "java.lang.OutOfMemoryError" tpt_sms.txt`
- `grep "java.lang.OutOfMemoryError" sms-info.log*`

Database errors

Check the following log file for database corruption or crash entries:

- `/var/lib/mysql/dbdatadir/mysqld.err`

Service mode

After you enable SMS HA, the SMS client cannot log in to the secondary (passive) server. Use service mode to access an otherwise inaccessible SMS server.

Note

To access service mode, you must contact product support.

Chapter 9

SMS client dashboard

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

Note

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

Dashboard palette

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

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

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

For more information about adding gadgets to your dashboard, see *Customize the SMS dashboard on page 9-9*.

Default dashboard configuration

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

- Top 5 Attacks (Last Hour)
- Top 5 Applications (Last Hour)
- Attacks (Last 24 Hours)
- Application Events (Last 24 Hours)
- Top 5 Attack Destinations (Last Hour)
- Top 5 Application Destinations (Last Hour)
- Top 5 App Users (Last Hour)
- Top 5 Attack Users (Last Hour)
- Device Health
- Device Status

- SMS Health
- SMS Client Health
- Distribution Status
- Top 5 Attack Geographic Sources (Last Hour)

See *Customize the SMS dashboard on page 9-9* for information on how to customize your dashboard and *Dashboard gadgets on page 9-3* for an overview of available gadgets.

Dashboard gadgets

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

- *Health and Status gadgets on page 9-4* — System health and status of managed devices
- *Task Status gadgets on page 9-5* — Distribution status and software update status
- *Inspection Event gadgets on page 9-5* — Information about events that trigger security or application filters on your system, as well as trends such as the top events and top events by IP address or geographic location
    - *Event Rate gadget on page 9-6* — Overall number of filter-triggered events that the SMS is processing over a specified period of time.
    - *Security gadgets on page 9-6* — Information based on SMS Security filters, and can display various aspects of related events including number of instances, IP addresses, and geographic locations.
    - *Reputation gadgets on page 9-7* — Information based on the security filters and are further refined by the Reputation filter category.
    - *Application gadgets on page 9-8* — Information based on application filters and can display various aspects of related events

including number of instances, IP addresses, and geographic locations.

- *User gadgets on page 9-9* — Information based on user and user group query criteria including login names, and source and destination IP addresses of domains and machines.

Health and Status gadgets

Health and Status gadgets monitor characteristics of system health and report on the basic health and status of managed devices. These dashboard gadgets provide a high-level warning system for potential health and performance problems with your system and devices. Main focal points of the Health and Status gadgets include:

- System Health — SMS health status for CPU, memory, temperature, file system, and system log. Select gadget to display the General – System Health screen
- SMS Client Health — Health of the SMS client memory and CPU usage.
- Device Health — Number of devices in each condition of system health:
  - Green – Normal
  - Yellow – Major
  - Red – Critical

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

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

- Rebooting

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

Note

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

Task Status gadgets

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

- **Distribution Status** shows the status of the most recent profile and Digital Vaccine (DV) distributions. You can specify how many status entries to show for each distribution category:
  - Inspection Profile
  - Digital Vaccine
  - Reputation
- **Software Update Status** shows the current (active) and available TippingPoint software versions, including SMS software, SMS patches, Digital Vaccines, and TOS software.

Click anywhere in the Software Update gadget to display the Admin (General) workspace in the SMS client.

Inspection Event gadgets

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

Event Rate gadget

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

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

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

Security gadgets

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

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

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

Security gadget	Description
Attacks	Number of attacks observed over a specific period of time, based on the Security filter type. You can specify the Time Period in the gadget options. Click in this gadget to display Security events in the SMS client.
Top Attack Destinations	Top attack destination IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.

Security gadget	Description
Top Attack Geographic Destinations	Map or table view of the top geography (city, region, country) based on top hit count for destination IP addresses in attack events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.
Top Attack Geographic Sources	Map or table view of the top geography (city, region, country) based on top hit count for source IP addresses in attack events. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and whether to display information in a map or a table.
Top Attack Sources	Top attack source IP addresses displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display the filter events in the SMS client.
Top Attacks	Top attacks displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display security events in the SMS client.

Reputation gadgets

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

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

to display (1–10), and choose the type of chart to use for display in the gadget options.

Application gadgets

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

The following table provides a description of dashboard application gadgets.

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

Application gadget	Description
Top Applications	Top applications displayed in table, bar graph, or pie chart format, and sorted by hit count. In addition to Event Criteria, you can configure the Time Period, the number of top events to display, and the chart type. Click an entry in this gadget to display application events in the SMS client.

User gadgets

The SMS dashboard includes two gadgets that you can use to monitor Active Directory information, such as user and user group query criteria, login names, and source and destination IP addresses of domains and machines.

The following table provides a description of dashboard user gadgets.

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

Customize the SMS dashboard

Customize your dashboard to provide the information you need to monitor for issues and react quickly:

- *Select a dashboard theme on page 9-10* – Select the color and contrast of the visual elements of the dashboard
- *Change the dashboard layout on page 9-10* – Change the column widths or move gadgets around

- *Add or remove a gadget on page 9-11* – Choose which gadget you want to see on the dashboard
- *Configure a gadget on page 9-11* – Change the gadget to show items

Note

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

Select a dashboard theme

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

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

Change the dashboard layout

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

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

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

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

Restore dashboard defaults

Click **Restore Defaults** (360° arrow) to remove all customizations to the dashboard. This removes all gadgets added that are not part of the default

configuration. It also removes any customizations made to the gadgets included in the default configuration.

Add or remove a gadget

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

Procedure

1. Click the **Show Palette** button (paint brush) in the top right hand corner of the dashboard. To change the location of the palette, click the **Location** button (compass needle) in the dashboard toolbar, and select top, bottom, right, or left.
2. Hover over the palette and use the scroll button on your mouse to scroll through the available gadgets. See *Dashboard gadgets on page 9-3* for information on the different types of gadgets available.
3. Either double-click or drag and drop the gadget from the dashboard palette to the display area.
4. To remove a gadget from your dashboard, hover the mouse over the gadget title and click the close button in the top-right corner of the gadget

---

Configure a gadget

Procedure

1. Hover the mouse over the top right of the gadget title bar to display the configuration tools.
2. Click the **Configure** button (wrench) to display configuration options.

3. In the Options wizard, select a category in the navigation pane to display related options. Depending on the gadget, option categories might include:
   - **General** – Change the title and other general settings, such as time period. Description is a read-only field.
   - **Event Criteria** – Change what the events the gadget will track, such as filter criteria, filter taxonomy criteria, device or segment criteria. You can also build a custom query. For background information about editing Event Criteria, see *Search for Inspection events on page 6-3*
   - **Display** – Choose how you want the information displayed. Some options are Top N Events or whether you want it to be a bar chart, pie chart, or a table.
4. Use controls on each screen to configure the gadget.
5. Click **OK** to save your changes and close the Options wizard.

Chapter 10

Tools

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

Look up an IP address or hostname

Use the IP Lookup utility tool to find the geographical location, domain name server, and registration information for a domain or IP address.

You can run these services manually on the SMS client, or you can configure the SMS to run many of these services automatically. Learn more: *IP address identifier on page 8-129*.

Procedure

1. Select **Tools** > **IP Lookup**, and then select a lookup service from the following options.

SELECT:	TO ...
Geo Locator	Perform a lookup in the Geo Locator database. Learn more: *Geo Locator Database on page 8-137*
Named Resource	Search for an IP address from the list of named resources on the SMS. If found, the most specific match displays. Learn more: *Named resources on page 8-123*
DNS	Perform a reverse DNS lookup.
User Id	Perform a lookup in the User ID database. If found, results show the user associated with the specified address. Learn more: *User ID IP Correlation on page 8-132*
Who Is	View registration information, based on the American Registry for Internet Numbers (ARIN). You can also look up domain registration information (source, destination, or client IP address) for SMS events. Right-click an event, and select **IP Lookup**.
Reputation	View reputation properties for the IP address, based on entries in the Reputation Database. This service is available whether or not you have a subscription for Threat DV.
End Point Attributes	View the end point attributes, if provided.

Select:	To ...
Multiple Lookups	Select every service listed above for the look up.

2. Enter an IP address or hostname.
3. Click **Lookup**.
4. Click **Copy All to Clipboard** to copy the text for all lookup services.

Access the TMC

The TMC is a service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters. The TMC also includes various documentation, the TippingPoint knowledge base, and how to contact support.

To access the TMC from the SMS, select **Tools** > **TMC**.

Access ThreatLinQ

ThreatLinQ works with the TMC to collect and analyze information about the security posture of the Internet. You can view globally aggregated information about filters, source IP addresses, and source or destination ports.

Because ThreatLinQ data is sensitive, you must enable ThreatLinQ event sharing to use this feature. Learn more: *TMC information share on page 11-4*.

To access ThreatLinQ from the SMS:

- Select **Tools** > **ThreatLinQ**.
- Right-click an event, and select **ThreatLinQ**.
- Select a filter, and then select **Filter Details**.

Create a Logs Zip file for the SMS client or SMS server

The Logs Zip file is a collection of log-related attributes used for troubleshooting. Create this file before you contact support.

Procedure

1. Select **Tools** > **Diagnostics** > **Log Utils**.
2. Select a tab: one is for the SMS client logs, and the other is for the SMS server logs.
3. Click **Create Logs Zip File**.

Edit logging levels

Procedure

1. Select **Tools** > **Diagnostics** > **Log Utils**.
2. Select a tab: one is for the SMS client loggers, and the other is for the SMS server loggers.
3. Click **Edit Loggers**.
4. Select a logger name, and then specify a **Logger Level** from the following options.

Select:	To ...
All	Include all levels.
Trace	Designate more details than the Debug level.
Debug	Designate informational events useful to debug the log file.
Info	Designate informational messages.
Warn	Designate potentially harmful situations.

Select:	To ...
Error	Designate errors that might still allow the application to continue running.
Fatal	Designate severe errors.
Off	Turn off logging.

5. Click **OK**.

Install or roll back a hotfix

Procedure

1. Select **Tools** > **Diagnostics** > **Hotfixes**.
2. Click **Install** to install a single SMS software hotfix. Verify that there is enough free space before you install a hotfix.
3. Click **Install Bulk** > **Add** to batch install multiple software hotfixes.
4. Select a hotfix, and click **Rollback** to roll back to a previous version. The SMS retains system settings and configurations. Depending on the version you rollback to, not all functionality will be available.

Generate bookmark string

You can generate a bookmark string for use on the SMS client or the Command Line Interface (CLI).

Procedure

1. Select **Tools** > **Diagnostics** > **Bookmarks**.
2. Click **Generate Bookmark String**.

Look up users on LDAP

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

Procedure

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

Chapter 11

System preferences

You can configure the following system preferences on the SMS:

- Security
- TMC information share
- Device SNMP
- Device communication
- Dashboard
- SSH client configuration
- Banner message
- PCAP download
- Reports
- Events

Security

Edit security preferences for the SMS.

Procedure

1. Select **Edit** > **Preferences** > **Security**.
2. Specify the level of security required when creating a username and password.

Level	Description
0 - None	• Usernames cannot contain a space or a backslash. • Password length and complexity are not restricted. • Passwords cannot contain a space.
1 - Low	Passwords must meet Level 0 (None) restrictions and the following: • Usernames must be at least six characters. • Passwords must be at least eight characters. • New password must be different from the previous password.
2 - Medium (default)	Passwords must meet Level 1 (Low) restrictions and the following: • Must contain at least two alphabetic characters. • Must contain at least one numeric characters. • Must contain at least one non-alphanumeric character (examples include `! ? $ * #`).

Level	Description
3 - High	Passwords must meet Level 2 (Medium) restrictions and the following: • Must contain at least 15 characters. • Must contain at least one uppercase character. • Must contain at least one lowercase character. • Must be different from the previous password in at least half of the corresponding character positions.

3. Select password preferences from the following options:

   - **Require password to be different from user ID**
   - **Lock user after failed login attempts**, and enter a threshold to set the number of unsuccessful consecutive attempts.
   - **Require new password to be different from previous passwords**, and enter the number of previous passwords the SMS will check.
   - **Show previous login details when a user logs in**, and enter the number of days as the count period. The SMS displays information for:
     - Last successful login including date, timestamp, and IP address.
     - Number of successful logins in the last number of days.
     - Last failed login attempt including date, timestamp, and IP address.
     - Number of failed login attempts since the last successful login.
     - Any group or role changes to the user account since the last login.
   - **Disable inactive user accounts**, and enter the number of days the user account must be inactive before it is disabled on the SMS.
   - **Require user to re-authenticate**, and set a time.

- **Enforce a minimum password lifetime**. Passwords cannot be changed again until the minimum time has passed.

4. Select **Limit number of total and user sessions** to determine whether the SMS limits the number of active sessions allowed on the SMS, or for a user, and enter a maximum number.
5. Select SMS client preferences from the following options:
   - **Allow storing the username and server used to login to this SMS**
   - **Timeout client session after inactivity**, and enter the number of minutes a user can be inactive.
   - **Lock client session after inactivity**, and enter the number of minutes a user can be inactive.
   - **Auto reconnect client to server after a disconnect occurs**

Note

When the SMS is configured to use two-factor authentication, a user account might be locked out if there are network interruptions. Learn more: *Configure authentication on page 8-17*

6. Click **OK**. If you update a user's security level, the SMS forces a password change at the next login if the security level restrictions set for the user requires it.

TMC information share

Share SMS information with the TMC

Procedure

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

Select:	To ...
Enable update tracking on TMC	By default, every SMS sends information to the TMC including version, model, and managed device information. Select this checkbox to send additional information to the TMC, such as configuration metadata and which SMS features are being used.
Enable TMC Polling for DV, OS, and License Package updates	Enable the SMS to periodically poll the TMC for updates.
Enable ThreatLinQ Event Sharing	Determine whether the SMS can upload aggregated events to the TMC in an effort to collect and analyze the security posture of the Internet. Enabled by default. You can choose one of the following options: • **Hide All IP Addresses in ThreatLinQ** - Hide the IP address for the event. (Default) • **Don't Hide IP Addresses in ThreatLinQ** - Send the IP address for when the event happened. • **Hide the Following Addresses in ThreatLinQ** - Determine which IP addresses to send to the TMC. When enabled, the SMS uploads the aggregated events during the last calendar day. Learn more: *Access ThreatLinQ on page 10-3*
Enable sharing CVE coverage gaps to help TippingPoint improve DV coverage	Enable the SMS to upload CVE IDs to the TMC including CVE IDs found in a vulnerability scan that are not yet associated to a filter. Learn more: *Vulnerability Scans (eVR) on page 5-111*

3. Click **OK**.

Device SNMP

Set the SNMP preferences used to communicate with N/NX Series devices.

Procedure

1. Select **Edit** > **Preferences** > **Device SNMP**.
2. Configure device SNMP preferences from the following options:
   - **Use SNMP v3 when possible**
   - **v2**, and enter and verify the SNMPv2 community.
   - **v3**, and enter or select the user name, authentication protocol, key, and privacy protocol.
3. Click **OK**.

Device communication

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

Procedure

1. Select **Edit** > **Preferences** > **Device Communication**.
2. Select **Enable Device Communication Check** to enable the SMS to perform communication checks with managed devices. If selected, specify values for the following options:
   - **Failure threshold**, and set the maximum number of failures. This only applies to IPS devices that are using SNMP traps to send alert logs.
   - **Comm check interval**, and set the time between communication checks. This does not apply to IPS devices using the Encrypted Alert Channel.

3. Specify **Data Retrieval Polling Intervals** from the following options:
   - **Device history stats**
   - **Device health and performance**
   - **Device port stats**
   - **SMS Health and performance**
4. Click **OK**.

Dashboard

You must have SuperUser privileges to use this feature. Learn more: *User roles and capabilities on page 8-39*.

Procedure

1. Select **Edit** > **Preferences** > **Dashboard**.
2. Select **Enable Dashboard** to determine whether the dashboard automatically displays when a user logs in to the SMS client. If you disable this option, a user can still access the dashboard (**View** > **Dashboard**), but the SMS will not update the dashboard information.
3. Specify the time at which the dashboard is updated, from 5–60 minutes.
4. Specify the font name, style, and size used on all dashboard gadgets.
5. Click **OK**.

SSH client configuration

Specify which external SSH client application to use for the SSH client terminal from the SMS client. Select **Edit** > **Preferences** > **SSH Client Configuration**

Banner message

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

Select **Edit** > **Preferences** > **Banner Message**.

PCAP download

Configure PCAP download preferences to provide remote storage information (directory and server name) for packet capture (PCAP) files.

Note

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

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

- User role that enables you to edit preferences. Learn more: *Administration on page 8-1*
- Sufficient storage space for the PCAP files. Learn more: *Packet trace on page 6-20*
- PCAP management application

Note

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

Procedure

1. Select **Edit** > **Preferences** > **PCAP Download**.
2. Select an external source.
3. Enter the following information for the selected external source:
   - Remote directory
   - Server
   - Domain
   - Username and password
4. Click **OK**.

Reports

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

Select **Edit** > **Preferences** > **Reports**.

Click **Run ETL Process Now** to prepare the data on the SMS for report generation.

Events

You can edit settings to determine the visibility of events. When selected, users will not be able to view events that occur on segments they do not have access to. These segments will display *<Unknown>* on the SMS.

This setting affects event visibility in the following areas on the SMS:

- Events
- SMS client dashboard
- Reports

Select **Edit** > **Preferences** > **Events** > **Enforce strict access control for event views**.

Chapter 12

Responder

Responder provides security mitigation to block infected or malicious traffic, inform you of possible threats, and place the host into remediation. Responder policies monitor all traffic according to devices, and use filters to enact another layer of protection. Filters include action sets with options to automatically redirect users and halt trigger traffic flows.

This chapter defines how to create actions and policies that perform expanded Responder actions beyond filter action sets. Triggered policies can make an entry to the event log, send email notification regarding the issue, send an SNMP trap, and add entries to the Reputation Database. You can also create switch-level policies and integrate with system management tools. The SMS provides manual actions for adding hosts to the Active Responder queue.

The Responder workspace provides a centralized environment for managing security response actions, policies, switches, and response history

Before you begin

Responder controls involve the use of policies, action sets, and filters that identify and possibly react to security violations. Therefore, you must fully implement an action before it can take effect. To use Responder, you must first:

- Manage devices.
- Define actions.
- Create an Active Responder policy to control how to trigger a response by setting initiation and timeout rules, selecting specific IP addresses, configuring a threshold period, executing and prioritizing responder actions, and selecting a device, if the policy contains an Intrusion Prevention System (IPS) action.
- Create a Profile Action Set to control the flow (permit, block, quarantine, rate limit, or trust) and to determine which notification types a filter hit will send (management console, SMS response, remote syslog, email, and SNMP) for the active responder policy.
- Select Profile Security and Application Filters to use that particular flow of traffic for the Action Set.

Learn more about these tasks in the *SMS User Guide*.

The SMS client defines the full implementation requirements for each action to ensure that your Responder policies are set up securely. All implementation requirements are located on the Implementation screen in the Response Action wizard.

Limitations

To ensure your continued success, note the following limitations when using Active Responder:

- **Actions** — The SMS can support a maximum of 250 actions per minute.
- **Response History** — There must be less than 20,000 active responses at any given time. The SMS does not have a limit on the number of closed responses.

Responder settings

Responder has a number of configurable settings. You can configure triggers for a response, set thresholds, supply the SMS with the URL where hosts that trigger responder policies can be redirected, control the criteria by which a host action is closed, and so on. When a response is triggered, the SMS uses an Active Responder policy to manage affected hosts and halted traffic streams. Each policy requires a set of actions and settings configured to respond to malicious traffic by using switches in the network topology.

Responder is a policy-based service that reacts to triggers and performs a set of actions. You configure and enable Responder policies in the SMS that determine how the service reacts and what actions it takes. A policy can be triggered in several ways: thresholding, manually, Web service, or escalation of an IPS Quarantine action. You can configure policies to include or exclude sets of IP addresses. A policy incorporates a dependency capability that allows actions in the list to execute conditionally, based on the success or failure of other actions.

You configure Responder by creating active responder policies, specifying or creating responder actions, configuring network equipment that will participate in the active responder system, and configuring server options.

Import or export an active responder action script

You can import, export, and delete action and device scripts with the SMS Active Responder Script Manager. Scripts are saved in XML format.

Procedure

1. Open Responder from the SMS navigation pane.
2. Click **Actions**.
3. Click **Import** and then browse and select a file. The file type defaults to Quarantine Action Package, which includes both XML and QDP file formats.
4. Click **Export** and navigate to the location you want to save the script and select **Quarantine Action Package** for the File type.

5. Click **Save**.

> **Note**
> If a previous version of the script exists, a warning dialog indicates it will overwrite an existing script file.

Writing Response action scripts

Action and device scripts, called packages, contain JavaScript code and metadata. XML comments are allowed and follow XML conventions.

DOCTYPE declaration

This declaration appears first in the package and instructs the JavaScript engine how to process the contents.

Action packages

```
<!DOCTYPE package PUBLIC "-//TippingPoint Inc//SMS Quarantine IEE Action Script
1.2//EN" "./iee-action-1_2.dtd">
```

Device packages

```
<!DOCTYPE package PUBLIC "-//TippingPoint Inc//SMS Quarantine Network Device Script
1.1//EN" "./iee-device-1_1.dtd">
```

Package element

Each XML package file contains one package element that contains all scripts and properties. Following are the child elements of the package element:

Description element

A description of the script package is displayed in the Script Manager for actions or devices. It is an element of both action and device packages. There are no attributes for the description element.

```
<description>Switch Package for 3Com 4400</description>
```

Migrate element

Contains XSL code to migrate the package from an earlier version. The migrate element requires the *fromVersion* attribute. This section must be present if any properties changed.

Example changes to packages

Following are examples of one way to address typical changes to a package.

Adding new properties

This example adds two properties, one (*snmp_version*) with a default value and one (*snmp_engine_id*) with no value.

```
<migrate fromVersion=”2”><![CDATA[
    <xsl:template match=”values”>
        <values>
            <xsl:apply-templates/>
            <value name=”snmp_version”>2</value>
            <value name=”snmp_engine_id”/>
        </values>
    </xsl:template>
]]></migrate>
```

Removing properties

This example removes the property *old_property_name*.

```
<migrate fromVersion=”2”><![CDATA[
    <xsl:template match=”values/value[@name=’old_property_name’]”/>
]]></migrate>
```

Renaming properties

This example renames the property *old_property_name* to *new_property_name* while retaining the currently specified value.

```
<migrate fromVersion=”2”><![CDATA[
    <xsl:template match=”values/value[@name=’old_property_name’]”>
        <value name=”new_property_name”><xsl:value-of select=”.”/></value>
    </xsl:template>
]]></migrate>
```

Converting values

This example converts the value of *property_name*.

```
<migrate fromVersion=”2”><![CDATA[
    <xsl:template match=”values/value[@name=’property_name’]”>
        <xsl:if test=”. = ‘MD5’”>
            <value name=”property_name”>HMAC-MD5</value>
        </xsl:if>
        <xsl:if test=”. = ‘SHA-1’”>
            <value name=”property_name”>HMAC-SHA</value>
        </xsl:if>
    </xsl:template>
]]></migrate>
```

Elements of both action and device packages

Properties element

A property is a value configured from SMS that is specific to a device instance. The *properties* element includes zero or more *pageGroup* elements.

pageGroup element

A *pageGroup* defines a property sheet in the SMS Client. The *pageGroup* element has one required attribute, *name*. This name is used as the title for the property sheet in the SMS Client.

The *pageGroup* element contains zero or more *propertyGroup* elements. A *propertyGroup* element defines a property grouping on a property sheet. The property grouping is boxed in the SMS Client and uses the *name* attribute for the title of the box.

Following is an example page group declaration:

```
<pageGroup title="Trap Destination">
  <description><![CDATA[
      Specify the destination agent for this SNMP trap:
      <ul>
          <li> Hostname or IP address to which this trap should be delivered.
          <li> UDP port the destination agent is listening on.
      </ul>
      By default a trap is sent when a host enters and leaves
      quarantine.  You may uncheck "Send trap on unquarantine" to
```

```
    disable the trap that is sent when a host leaves quarantine.
  ]]></description>
  <propertyGroup name="Trap Destination">
      <property name="sendto_host" displayName="Host" type="IpAddress" required="true"/>
      <property name="sendto_port" displayName="Port" type="Integer"
                    required="false" min="1" max="65535" default="162"/>
  </propertyGroup>
  <propertyGroup name="Trap Options">
      <property name="send_unq_trap"
                displayName="Send trap on unquarantine"
                type="boolean" default="true"/>
      <property name="snmp_test_oid" displayName="Test OID"
                type="string" regex="\d+(\.\d+)+" maxlen="100" required="true"
                default="1.3.6.1.4.1.10734.3.4.3.0.1">
      </property>
  </propertyGroup>
</pageGroup>
```

propertyGroup element

The *propertyGroup* element contains zero or more *property* elements. The *property* element describes a property in the SMS Client and available in scripts. The *property* element has many attributes. Only *name* and *type* are required.

Attribute	Type	Description
name	String	Name of the property that can be accessed in scripts through the device object.
displayName	String	Label for the property in the SMS Client.
type	String	Value type of the property.
required	boolean	Defines whether the user is forced to enter data in the SMS Client for this property.
min	integer	Minimum allowed value for this property
max	integer	Maximum allowed value for this property
default	String	Default value for this property. If not set, booleans default to false.
maxlen	integer	Maximum length of the property's value.
cols	integer	Size of the input field in the SMS Client

Attribute	Type	Description
rows	integer	Number of rows of the input field in the SMS Client
regex	String	Regular expression used to validate the entry in the SMS Client. See the Pattern object in the Java 1.6 documentation for more information.
dependsTarget dependsValue	String String	Specifies another property and its value(s) required for this property to be editable in the SMS Client.

Valid property types include the following:

Type	Description	SMS Client
string	Character string	Text area if rows > 1, otherwise Text field
password	Password string. This value is hidden in the SMS Client, but is stored in the database as plain text.	Password field
IpAddress	IP address	Text field with an IP Address validator
EmailAddress	Email address	Text field with an Email Address validator
Integer	A number	Text field
boolean	True or false value	Checkbox
enum	A list of values to choose from	Drop down (combo box)
array	Collects a list of values	List
blurb	A psuedo-property only used to display additional text in the SMS Client.	Text pane with HTML content. Uneditable.

Script element

JavaScript code is contained within *script* elements. A single package can contain multiple scripts. Trend recommends that you wrap the JavaScript code within a CDATA tag to avoid the need to escape special characters.

The *script* element has two attributes. The *name* attribute is required and is the name used to reference the script. The *depends* attribute is optional and refers to one or more names of scripts included in the same package that are referenced by the current script. This allows you to create common functions in one script and call them from multiple scripts.

For example, most of the device packages have scripts named *RADIUSFunctions, SNMPFunctions, SNMPActionFunctions,* and*SNMPDeviceFunctions. RADIUSFunctions* contains common functions that are available for RADIUS enforcement. *SNMPFunctions* contains common functions available for any SNMP use. *SNMPActionFunctions* contains common functions available for use by any action scripts. *SNMPDeviceFunctions* contains common functions available for use by any device scripts. The real difference between the last two are that certain objects are globally available for action scripts and a different set of objects are globally available for device scripts.

```
<script name="test "><![CDATA[
        var result = "Nothing to test";
        result += "<br>";
    ]]></script>
```

systemObjectID element

The systemObjectID element only appears in device packages and defines which systemObjectIDs this package supports. Currently, it is only used during SNMP discovery. If two device packages contain the same systemObjectID, it is not defined which package is selected during SNMP discovery.

The only attribute is *oid* and it is the systemObjectID returned by the device.

```
<!-- Supported devices -->
<systemObjectID oid="1.3.6.1.4.1.43.10.27.4.1.2.4">3Com Switch 4400</systemObjectID>
```

There can be multiple *systemObjectID* elements in a single device package.

Special scripts

Following are scripts used in special circumstances.

disconnect

The supported Switch Disconnect action package looks for and calls the *disconnect* script in the associated device package. Implement this script in your device package to support Switch Disconnect actions.

moveToVLAN

The supported Move To VLAN action package looks for and calls the *moveToVLAN* script in the associated device package. Implement this script in your device package to support Move To VLAN actions.

onBridgeUpdate

Implement this script in your device package to support Access Control. This script is called periodically by the SMS if the device is configured for Access Control. Specifically, if the property *use_radius_authentication* exists and is set to true OR if the property *use_for_access_control* exists and is set to false, *onBridgeUpdate* will not be called. Otherwise, it will be called whenever the device is added/updated and when the SMS starts and periodically after that.

It is important for new device scripts to use these property names. If these properties do not exist, it is assumed that the switch is used for Access Control.

This script should parse the bridge table of the device and use *device.storeBridgeInfo()* to store bridge table entries in the database.

onMACLookup

Implement this script in your device package to support IP Correlation. This script uses RFC-1213 to find the MAC address for an IP address. It is called during IP Correlation, which can be triggered a number of ways.

onPortLookup

Implement this script in your device package to support MAC lookups. This script uses the bridge table to determine if a MAC address is associated with

a port on the device. It is called primarily by the MACLOOKUP test feature and through the Web servlet.

onSubnetUpdate

Implement this script in your device package to support IP Correlation. This script reads in and stores the different IP subnets serviced by the Layer 3 device. It is called the same as *onBridgeUpdate*, including periodically. This information is used during IP Correlation to narrow down which devices might be able to correlate an IP address to a MAC.

QUARANTINED

An action package must have a *QUARANTINED* script defined that is called when a quarantine event occurs. The *QUARANTINED* script can register another script to be called when an *UNQUARANTINED* event occurs. In the supported action packages, this script is named "doUnquarantine". For example:

```
host.callbackOnState( "UNQUARANTINED", "doUnquarantine" );
```

reconnect

The supported Switch Disconnect action package looks for and calls the *reconnect* script in the associated device package. Implement this script in your device package to support Switch Disconnect actions. This script will undo the action performed by the *disconnect* script.

restoreDefaultVLAN

The supported Move To VLAN action package looks for and calls the *restoreDefaultVLAN* script in the associated device package. Implement this script in your device package to support Move To VLAN actions.

test

Implement this script in your device and action packages to support testing. Device scripts should test connectivity to the network device. Action scripts are dependent on the type of action.

Global functions

This function is available in all scripts.

Functions

Return Value	Name	Description
String	int2mac(long *mac* , int *numGroups* , String *separator*)	Converts a MAC address in long format to the string representation consisting of *numGroups* of digits separated by *separator* . Default is 6 groups and a separator of ':'

Sample usage

```
var macAddress = int2mac( host.macIfKnown );
```

Action object

The action scripts inherit access to specific Java objects. These object properties and methods enable scripts to use and communicate data to the RADIUS Proxy, database, and other quarantine elements. The action object represents an action script and contains dynamic properties defined for the current action. In user-created actions, these properties are defined in the scripts. These objects are treated as Global Objects and cannot be constructed, but are only available to action scripts.

Properties

There are no static properties for the action object. Dynamic properties defined in the action script file are available.

Methods

There are no static action methods available from JavaScript. Dynamic scripts defined in the action script file are available.

Sample usage

```
var msg = new Email();
msg.from = action.emailFrom;
```

```
msg.recipients = action.emailTo;
msg.body = action.userText;
msg.subject = “SMS Quarantine”;
msg.send();
```

Callback object

The callback object represents a registered callback from a quarantine. The intention is that the quarantine script registers different callbacks to run during state transitions or on the receipt of an event. Refer to host.callbackOnState() and host.callbackOnEvent().

This object has dynamic properties that can pass information from where the callback is registered to where the callback is invoked. See the NMS Trap action for an example of how this is used.

Properties

Name	Type	Description
callbackEvent	String	Returns the event name that caused this callback: Quarantine , Unquarantine , RADIUS Proxied , Trap Received , IPS Quarantine , Error , and Timer Expire . (read-only)
callbackState	String	Returns the state name that causes this callback: INITIAL , QUARANTINED , UNQUARANTINED , and ERROR . (read-only)
cause	Event	Returns the event that registered the callback. (read-only)

Methods

Return Value	Name	Description
boolean	invokeNow()	Invokes the callback immediately. This is not to be used on a callback that has been provided. It should only be used on callbacks that are searched. See host.searchCallbacks(). See the NMS Trap action for an example of how this is used.
boolean	isSatisfied()	Returns whether this callback has already been satisfied.

Return Value	Name	Description
void	satisfied()	Satisfies the callback.

Sample usage

```
var originalEvent = callback.cause;
callback.satisfied();
```

Event

The event object represents a trigger in SMS Quarantine. The types of triggers are:

Name	Description
Quarantine	An alert threshold has been crossed, a Manual Quarantine has been performed, or the Quarantine web servlet has been invoked.
Unquarantine	A manual unquarantine has been performed, or the Unquarantine web servlet has been invoked.
RADIUS Proxied	A RADIUS Access Request has been received on a host that is currently quarantined through SwitchDisconnect or MoveToVLAN actions.
Trap Received	An SmsTrapQuarantineRequestAck or SmsTrapUnquarantineRequestAck has been received.
Timer Expired	An SMS Quarantine has timed out.
Error	A non-recoverable error has occurred

This object has dynamic properties that can pass information. By default, the SMS populates the two dynamic properties *SWITCH_IP* and *SWITCH_PORT* if IP Correlation succeeded.

Properties

Name	Type	Description
alert	Alert	The alert that triggered this event.

Name	Type	Description
id	long	The event ID.
ingressSwitch	Device	The switch, if IP Correlation succeeded.
ip	String	The quarantined IP address.
macAsInt	long	The MAC address of the end station expressed as a long value. This property is provided, in conjunction with the method *int2mac()* to allow alternate formatting of the MAC address.
macIfKnown	String	The MAC address of the end station if IP correlation succeeded.
profileName	String	The name of the profile.
signature	Signature	The signature information for the filter.
triggerInfo	String	Who or what initiated the response event. This value depends on the trigger method used.
triggerMethod	String	How the response event was triggered.

Trigger methods

Method	Info	Description
SYSTEM	"system"	The system initiated the response event.
POLICY	Policy name	The response policy initiated the response event.
USER	User name	The user initiated the response event.
IPS	Device name	An IPS initiated the response event.
WEB	User Name	The web interface initiated the response event.

Methods

There are no Event methods accessible from JavaScript.

Sample usage

```
var switchIp = event.SWITCH_IP;
```

Alert

This object is only available through the Event object (i.e. event.alert). It represents the actual alert from the SMS.

Properties

Name	Type	Description
aggregrationPeriod	int	The amount of time over which the alerts were aggregated.
destAddress	String	The destination IP address
destPort	int	The destination port
deviceID	int	The ID of the device generating the alert. Most useful if you are using external DB access.
deviceTraceBeginSequence	int	
deviceTraceBucket	int	
deviceTraceEndSequence	int	
hitCount	long	Aggregated value for the number of filter hits represented by this alert
idx	long	Index value. Most useful if you are using external DB access
logEventType	int	
logVersion	short	
messageParameters	String	
noticeAction	short	
packetTrace	short	
physicalPortIn	int	

Name	Type	Description
policyUUID	String	The UUID of the policy triggering the filter hit.
segmentID	int	The ID of the segment that generated the alert.
sequenceNumber	long	
severity	short	The severity of the alert
signature	Signature	The signature information for the filter.
signatureUUID	String	The UUID of the signature. Most useful if you are using external DB access.
srcAddress	String	The source address of the alert
srcPort	int	The source port
time	long	
timeEnd	long	
vlanTag	int	

Methods

There are no Alert methods accessible from JavaScript.

Sample usage

```
var destAddr = event.alert.destAddress;
```

Signature

This object is only available through the Event or Alert objects (i.e. event.signature). It represents the signature information of the filter triggering the event.

Properties

Name	Type	Description
bugTraqId	String	

Name	Type	Description
cveId	String	
description	String	The signature description
id	String	The UUID of the signature
name	String	The signature name
nfAlarmId	int	
number	int	The signature number
protocol	String	
severity	int	
version	String	

Methods

There are no Signature methods accessible from JavaScript.

Sample usage

```
var name = event.signature.name;
```

Host

The host object represents a Quarantined Host entry in SMS Quarantine.

This object has dynamic properties that can pass information. The special dynamic property *EditRADIUS* allows the SMS RADIUS proxy to edit RADIUS responses for this host. This is how switch disconnect and move to VLAN actions operate with RADIUS enforcement. The host object also contains the dynamic properties *SWITCH_IP* and *SWITCH_PORT* if IP Correlation succeeded.

Properties

Name	Type	Description
id	long	The quarantined host ID.
ingressSwitch	Device	The switch, if IP Correlation succeeded.
ip	String	The quarantined IP address.
macAsInt	long	The MAC address of the end station expressed as a long value. This property is provided, in conjunction with the method *int2mac()* to allow alternate formatting of the MAC address.
macIfKnown	String	The MAC address of the end station if IP correlation succeeded.

Methods

Return Value	Name	Description
Callback	callbackOnEvent(String *eventType* , String *scriptName*)	Registers a script to invoke when an event occurs on this quarantined host. See Event for the valid values of *eventType* .
Callback	callbackOnState(String *stateName* , String *scriptName*)	Registers a script to invoke when this quarantined host transitions to the specified state. Since no script is invoked before the quarantined host is in the QUARANTINED state, the only effective values for *stateName* are UNQUARANTINED and ERROR.
boolean	isQuarantined()	Returns whether the quarantined host entry is currently in quarantine.
boolean	isUnquarantined()	Returns whether the quarantined host entry is currently unquarantined.
Callback[]	searchCallbacks(Integer *eventID*)	Returns an array of callbacks registered for this quarantined host entry. If *eventID* is not null, it will only return callbacks registered by that event.

Sample usage

```
host.callbackOnState( 'UNQUARANTINED', 'doUnquarantine' );
```

Device objects

The device scripts inherit access to a specific Java object. This object's properties and methods enable the scripts to use and communicate data to the database and other quarantine elements. This object is treated as a Global Object and cannot be constructed, but is only available to device scripts.

Correlation

The correlation object contains miscellaneous mapping information. This object is only available to the special scripts *onMACLookup* and *onPortLookup* in device packages.

Properties

Name	Type	Description
interfaceIndex	int	The interface index for the subnet
ipAddress	String	The IP address of the affected end station
macAddress	String	The MAC address of the affected end station

onMACLookup is called with only *interfaceIndex* and *ipAddress* initialized. *interfaceIndex* is the ifIndex of the interface to which the IP address belongs. These properties are added to ipNetToMediaPhysAddress in RFC-1213 to correlate the IP Address with a MAC Address.

onPortLookup is called with only *macAddress* initialized.

Methods

There are no Correlation methods accessible from JavaScript.

Sample usage

```
var ip = correlation.getIpAddress();
```

Device

The device object represents a device script and contains dynamic properties defined for the current device. In user-created devices, these properties are defined in the scripts.

Properties

Name	Type	Description
ipAddr	String	The IP address of the network device.
name	String	The name of the network device.

Methods

Return Value	Name	Description
void	addBridgePortMapping(String *index* , String *name*)	Adds an index/name mapping for bridge table ports.
void	addIfPortMapping(String *index* , String *name*)	Adds an index/name mapping for interface table ports.
void	addTrunkPort(String *portName*)	Registers *portName* as a trunk port. Trunk ports will not store bridge table information.
void	clearBridgePortMapping()	Removes all bridge port mappings.
void	clearIfPortMapping()	Removes all interface port mappings.
Map	getBridgePortMapping()	Returns the complete mapping of bridge ports.
String	getBridgePortMapping(String *index*)	Returns the port name for the bridge port index.
Map	getIfPortMapping()	Returns the complete mapping of interface ports.
String	getIfPortMapping(String *index*)	Returns the port name for the interface port index.

Return Value	Name	Description
void	storeBridgeInfo(String *macAddr* , String *switchIP* , String *port* , String *status* , Integer *portCount*)	Saves the bridge table information to the database.
void	storeRouteTable(List *ipAddressList* , List *interfaceList* , List *netmaskList*)	Saves the subnet routing information to the database.

Sample usage

```
var switchIP = device.ipAddr;
```

Global objects

A couple of Java classes are available for system level capabilities. These objects are singletons and cannot be constructed.

Environ

The Environ class provides special properties to JavaScript. This object is available to all scripts.

Properties

Name	Type	Description
debugging	boolean	Indicates whether the scripts are in debugging mode **(read-only)**
emailFrom	String	Returns the SMS Admin SMTP Server setting for *From* **(read-only)**
emailReplyTo	String	Returns the SMS Admin SMTP Server setting for *Reply To* **(read-only)**
hostIP	String	Returns the IP address of the SMS Server **(read-only)**
hostName	String	Returns the host name of the SMS Server **(read-only)**

Name	Type	Description
SMTPServer	String	Returns the SMS Admin SMTP Server address **(read-only)**

Methods

There are no Environ methods accessible from JavaScript.

Sample usage

```
var hostName = environ.hostName;
```

Logger

The Logger class provides the ability to log messages to the quarantine log. The log messages are preceded by "SCRIPT:", except for *trace*, which is preceded by "SCRIPT TRACE:". This object is available to all scripts.

Properties

There are no Logger properties accessible from JavaScript.

Methods

Return Value	Name	Description
void	debug(String *message*)	Sends a DEBUG level message to the log file.
void	error(String *message*)	Sends an ERROR level message to the log file.
void	info(String *message*)	Sends an INFO level message to the log file.
void	trace(String *message*)	Sends a DEBUG level message to the log file.
void	warn(String *message*)	Sends a WARNING level message to the log file.

Sample usage

```
logger.trace( “logging a message” );
```

Utility objects

A number of Java classes are available to enable connectivity to switches and other capabilities. These objects can be constructed and used from any script.

Email

The Email class provides the ability to send an email from a script.

Constructor

```
var email = new Email();
```

Properties

Name	Type	Description
body	String	The content of the email message.
from	String	The sender email address.
recipients	String	The email recipients, as a comma-separated list of email addresses.
replyTo	String	The reply-to email address.
subject	String	The subject line of the email.
smtpServer	String	The SMTP server to use for sending the email **(read-only).**

smtpServer defaults to the SMS Admin SMTP server settings.

Refer to the Email action for an example of how email is used.

Methods

Return Value	Name	Description
String	send()	Sends this email per its current configuration. On failure, a message is returned indicating the failure.

Sample usage

```
var email = new Email();
email.from = “test@tippingpoint.com”;
email.recipients = “user1@tippingpoint.com, user2@tippingpoint.com”;
email.subject = “Test”;
email.body = “Test Message”;
email.send();
```

SshClient

The SshClient class provides the ability to connect to a remote system using SSH2 or SSH3, but not SSH1. This class is very similar to the TelnetClient class.

Constructor

```
var client = new SshClient( String ip, String userName, String password, int port );
```

Specifying the *port* is optional. If the *port* is not specified, the default SSH port of 22 is used.

Properties

There are no SshClient properties accessible from JavaScript.

Methods

Return Value	Name	Description
String[]	expect(String *regex*)	Matches *regex* on incoming text, returns all capture groups.
String	get(String *regex*)	Blocks until *regex* is matched in returning text; returns everything up to that point or times out.

Return Value	Name	Description
String	getAll()	Returns all incoming text since the last 'get' oriented method was called. Imposes a 200ms wait for each invocation.
String	getAllToPrompt(String *prompt*)	Returns all input in the buffer up to prompt, since the last send.
int	getFlags()	Returns the flags used to compile the *regex* . Refer to the Java class *Pattern* for more information.
String	getPrompt()	Sends a newline and returns the results. Try to minimize the use of this method because it imposes a one second wait every time it is called.
String[]	grep(String *text* , String *regex*)	Performs basic grep functionality on *text* using *regex* .
String	replaceAll(String *regex* , String *replace* , String *text*)	Replaces all occurrences of *regex* in *text* with *replace*
String	replaceFirst(String *regex* , String *replace* , String *text*)	Replaces the first occurrence of *regex* in *text* with *replace*
void	send(String *value*)	Writes a string value to the SSH session
void	sendAsIs(String *value*)	Writes a string value to the SSH session without a trailing newline.
void	setCaseInsensitive(boolean *value*)	Enables/disables case insensitive pattern matching.
void	setCommandPrompt(String *prompt*)	Sets the command prompt to expect. Default is "\\$?"
void	setDotall(boolean *value*)	Enables/disables dotall mode. In dotall mode, the expression . matches any character, including a line terminator. By default this expression does not match line terminators. This allows matching patterns across multiple lines.

Return Value	Name	Description
void	setFlags(int *flags*)	Sets the flags used to compile the regex.
void	setMultiline(boolean *value*)	Enables multiline mode, in which the expressions ^ and $ match just after or just before, respectively, a line terminator or the end of the input sequence. By default these expressions only match at the beginning and the end of the entire input sequence.
void	setTimeout(int *seconds*)	Sets the timeout value of all 'get' type operations (get, expect, etc). Default is 10 seconds.
void	wait(int *milliseconds*)	Blocks for specified number of milliseconds

The following table lists the flag values and their meanings.

Value	Description
1	Enables Unix lines mode
2	Enables case-insensitive matching
4	Permits whitespace and comments in pattern
8	Enables multiline mode
16	Enables literal parsing of the pattern
32	Enables dotall mode
64	Enables Unicode-aware case folding
128	Enables canonical equivalence

Sample usage

```
var client = new SshClient( “1.2.3.4”, “root”, “password” );
client.setCommandPrompt( “Select menu option: “ );
client.getPrompt();
client.send( “logout” );
```

Syslogger

The Syslogger class provides the ability to send a syslog UDP packet from a script.

Constructor

```
var syslogger = new Syslogger();
```

Properties

There are no Syslogger properties accessible from JavaScript.

Methods

Return Value	Name	Description
boolean	syslog(String *ip* , int *port* , int *facility* , String *message*)	Sends a syslog message to the specified *ip* and *port* using *facility*

Sample usage

```
var syslogger = new Syslogger();
syslogger.syslog( “1.2.3.4”, 514, 1, “Syslog message” );
```

WebClient

The WebClient class is used to access web servers.

Constructor

```
var client = new WebClient();
```

Properties

There are no WebClient properties accessible from JavaScript.

Methods

Return Value	Name	Description
void	addParameter(String *name* , Object *value*)	Adds the name/value pair as a parameter to a GET or POST method. *value* is optional, but can only be missing for the first parameter of a GET method. Other parameters with no value specified result in *name=null* . This allows for a URL in a GET method. If you need more than one parameter with no value in a GET method, you must specify the parameters in the URL and encode the parameters manually.
void	clearParameters()	Clears all parameters.
int	doGetMethod(String *url*)	Creates and executes an HTTP GET method with the given *url* and any previously specified parameters. Returns the status of the GET method
int	doPostMethod(String *url*)	Creates and executes an HTTP POST method with the given *url* and any previously specified parameters. Returns the status of the POST method.
String	getResponseBody( )	Returns the response body of the last executed method. If the response body is not available or cannot be read, returns null.
int	getStatusCode()	Returns the response status code of the last executed method
String	getStatusText()	Returns the status text (or "reason phrase") associated with the latest response.
void	releaseConnection()	Releases the connection being used by the last executed HTTP method. In particular the connection is used to read the response (if there is one) and will be held until the response has been read. If the connection can be reused by other HTTP methods, it is NOT closed at this point
void	setConnectionTimeout(int *millis*)	Sets the timeout until a connection is established. A value of zero means the timeout is not used. The default value is zero.
void	setHost(String *host* , int *port* , String *protocol*)	Sets the given host, port and protocol needed to describe an HTTP connection to a host. *port* and *protocol* are optional.

Return Value	Name	Description
void	setProxy(String *host* , int *port*)	Sets the proxy settings. *port* is optional and defaults to http (80).
void	setProxyCredentials(String *username* , String *password*)	Sets the user credentials for the proxy host used for both BASIC and DIGEST authentication schemes. *setProxy* must be called before calling this method since the credentials are given an authentication scope of the *host* and *port* of the proxy.
void	setRetries(int *retries*)	Sets the number of times an HTTP method will be retried. This is the default value used for all methods associated with this client.
void	setUserCredentials(String *username* , String *password*)	Sets the user credentials used for both BASIC and DIGEST authentication schemes. *setHost* must be called before calling this method since the credentials are given an authentication scopr of the *host* and *port* .

Sample usage

```
var client = new WebClient();
client.setHostConfiguration( action.server, action.prot, action.protocol );
if ( action.use_auth == 'true' ) {
    client.setUserCredentials( action.username, action.password );
}
var resultCode = client.doGetMethod( action.url );
if ( resultCode == 200 ) {
    logger.info( "URL succeeded: " + action.url );
}
else if ( resultCode == -1 ) {
    logger.error( "URL failed: " + resultCode + ": Check logfile for errors" );
}
else {
    logger.error( "URL failed: " + resultCode + ": " + client.getStatusText() );
}
var body = client.getResponseBody();
```

SNMP objects

SNMP objects are available from either device or action scripts and must be constructed before use.

SnmpContext

The SnmpContext class specifies a "context" for SNMP traffic. SNMP objects start with SnmpContext because all of the other SNMP classes need the context to perform their function.

Constructor

```
var context = SnmpContext( int protocolVersion, String ipAddress, String port )
protocolVersion must be 1, 2, or 3. If no port is specified, 161 is used by default.
```

Properties

Name	Type	Description
community	String	The community string for v1 or v2 SNMP
userName	String	The v3 user name
engineId	String	The v3 engine ID as a string

Methods

Return Value	Name	Description
void	authinfo(String *protocol* , String *password*)	Specifies the encryption protocol (HMAC-MD5, HMAC-SHA) and password for v3 authorization
void	privacy(String *password*)	Sets the privacy password for v3 encryption. Currently only CBC-DES is supported.

Sample usage

```
var context = new SnmpContext( 2, “1.2.3.4”, 161 );
context.community = “public”;
```

SnmpGet

The SnmpGet class gets values from a remote SNMP agent.

Constructor

```
var request = new SnmpGet( context );
context is an object of type SnmpContext.
```

Properties

Name	Type	Description
retries	int	The number of retries before failure.
timeout	int	The timeout in seconds before a particular 'get' attempt is assumed to have failed.

Methods

Return Value	Name	Description
void	addOid(String *oid*)	Adds an OID to this GET Request.
void	destroy()	Frees up any resources used by this GET request.
String	getValue(String *oid*)	Returns the oid:named value from this result (if sendRequest was successful).
boolean	isDestroyed()	Returns true if this request has been destroyed.
boolean	sendRequest()	Performs the GET operation, returning true if successful.

Sample usage

```
var request = new SnmpGet( context );
var oid = “1.2.3.6.1.2.1.1.1.0”;
request.addOid( oid );
if ( request.sendRequest() ) {
    var value = request.getValue( oid );
}
```

SnmpGetNext

The SnmpGetNext class gets the next value from a remote agent.

Constructor

```
var request = new SnmpGetNext( context );
context is an object of type SnmpContext.
```

Properties

Name	Type	Description
retries	int	The number of retries before failure
timeout	int	The timeout in seconds before a particular 'getnext' attempt is assumed to have failed

Methods

Return Value	Name	Description
void	addOid(String *oid*)	Adds an OID to the GETNEXT Request.
void	destroy()	Frees any resources used by this GETNEXT request.
String	getInstance(String *oid*)	Returns the oid from the results of this GETNEXT request.
String	getValue(String *oid*)	Returns the oid:named value from this result (if sendRequest was successful).
boolean	isDestroyed()	Returns true if this request has been destroyed.
boolean	sendRequest()	Performs the GETNEXT operation, returning true if successful.

Sample usage

```
var request = new SnmpGetNext( context );
var oid = “1.2.3.6.1.2.1.1.1”;
request.addOid( oid );
if ( request.sendRequest() ) {
    var value = request.getValue( oid );
```

SnmpInform

A type of *SnmpV2or3Trap* that does an 'inform' instead of a simple trap.

Constructor

```
var trap = new SnmpInform();
```

Properties

Name	Type	Descriptions
trapOID	String	Describes the event being reported

Methods

Return Value	Name	Description
void	addInteger(String *oid* , int *value*)	Adds an oid:integer pair to this trap.
void	addOid(String *oid*)	Adds an oid:null value pair to this trap.
void	addString(String *oid* , String *value*)	Adds an oid:string pair to this trap.
void	destroy()	Frees any resources used by this INFORM request.
boolean	isDestroyed()	Returns true if this inform has been destroyed.
boolean	send(SnmpContext *context*)	Sends this trap to the specified SNMP context.

Sample usage

```
var trap = new SnmpInform();
trap.trapOID = ‘1.3.6.1.4.1.10734.3.4.3.0.1’;
trap.addInteger( ‘1.3.6.1.4.1.10734.3.4.3.1.1’, 101 );
trap.send( context );
```

SnmpSet

The SnmpSet class sets values on a remote agent.

Constructor

```
var request = new SnmpSet( context );
```

Properties

Name	Type	Description
retries	int	The number of retries before failure.
timeout	int	The timeout in seconds before a particular 'set' attempt is assumed to have failed.

Methods

Return Value	Name	Description
void	addInteger(String *oid* , int *value*)	Adds an oid:integer pair to this SET request.
void	addOid(String *oid*)	Adds an oid:null value pair to this SET request.
void	addString(String *oid* , String *value*)	Adds an oid:string pair to this SET request.
void	addUnsigned(String *oid* , String *value*)	Adds an oid:unsigned pair to this SET request.
void	destroy()	Frees up any resources used by this SET request.
boolean	isDestroyed()	Returns true if this request has been destroyed.
boolean	sendRequest()	Performs the SET request, returning true if successful.

Sample usage

```
var setter = new SnmpSet( context );
setter.addString( “1.2.3.4.5.6.7.8.9”, “value” );
setter.sendRequest();
```

SnmpV1Trap

The SnmpV1Trap class sends a trap to an SNMP V1 agent.

Constructor

```
var trap = new SnmpV1Trap();
```

Properties

Name	Type	Description
enterprise	String	Identifies the management enterprise under whose registration authority the trap was defined
genericTrap	int	Describes the event being reported. Refer to RFC 1157 for specific values
specificTrap	int	Identifies a non-generic trap when the Generic Trap Type is enterprise specific.

Methods

Return Value	Name	Description
void	addInteger(String *oid* , int *value*)	Adds an oid:integer pair to this trap.
void	addOid(String *oid*)	Adds an oid:null value pair to this trap.
void	addString(String *oid* , String *value*)	Adds an oid:string pair to this trap.
void	destroy()	Frees up any resources used by this trap request
boolean	isDestroyed()	Returns true if this trap has been destroyed.

Return Value	Name	Description
boolean	send(SnmpContext *context*)	Sends this trap to the specified SNMP context.

Sample usage

```
var trap = new SnmpV1Trap();
trap.enterprise = '1.3.6.1.4.1.42';
trap.genericTrap = 0;
trap.send( context );
```

SnmpV2or3Trap

The SnmpV2or3Trap class sends a trap to an SNMP V2 or V3 agent.

Constructor

```
var trap = new SnmpV2or3Trap();
```

Properties

Name	Type	Description
trapOID	String	Describes the event being reported.

Methods

Return Value	Name	Description
void	addInteger(String *oid* , int *value*)	Adds an oid:integer pair to this trap.
void	addOid(String *oid*)	Adds an oid:null value pair to this trap.
void	addString(String *oid* , String *value*)	Adds an oid:string pair to this trap.
void	destroy()	Frees up any resources used by this trap request.

Return Value	Name	Description
boolean	isDestroyed()	Returns true if this trap has been destroyed.
boolean	send(SnmpContext *context*)	Sends this trap to the specified SNMP context.

Sample usage

```
var trap = new SnmpV2or3Trap();
trap.trapOID = '1.3.6.1.4.1.10734.3.4.3.0.1';
trap.addInteger( '1.3.6.1.4.1.10734.3.4.3.1.1', 101 );
trap.send( context );
```

SnmpWalk

This is a convenience class for doing repeated GETNEXT requests when reading in a table.

Constructor

```
var request = new SnmpWalk( context );
```

Properties

There are no SnmpList properties accessible to JavaScript.

Methods

Return Value	Name	Description
String	get(int *index*)	Returns the element at the specified position in the list.
String	getIndex(int *index*)	Returns the instance OID as a suffix of the requested OID. For example, if the requested OID is '1.3.6.1.2.1.1' and the instance OID for an entry is '1.3.6.1.2.1.1.1.2', then *getIndex* on that entry would return '2'.

Return Value	Name	Description
boolean	isEmpty()	Returns true if the list contains no elements.
int	size()	Returns the number of elements in the list.
List<String>	walk(String *oid*)	Performs GETNEXT requests with the specified OID until the response OID is no longer under the specified OID. Returns the complete list of results.

Sample usage

```
var request = new SnmpWalk( context );
var list = request.walk( “1.2.3.4.5” );
```

Manage manual response policies

You can manually respond to hosts from the Active Response screen. When you manually respond to a host, the SMS enacts the Manual Response policy on the traffic flow.

To edit and enhance a Manual Response:

Procedure

1. Add policy actions.
2. Edit the Manual Response policy.
3. Manually respond to hosts.

   You will need the IP address and any information about the devices you want to specifically act upon.

You can also perform a manual response by right-clicking IP addresses in generated event lists on the Events screen. Or, you can use the **File** > **Create Manual Response** menu option on the Active Response screen.

Manage Responder through an external or third-party interface

For information about using an external or third-party interface to manage Responder, see the *Active Response* area in the *SMS Web API Guide*.

Responder actions

When host traffic triggers an Active Responder policy, the SMS performs the response actions associated with that policy.

The SMS client provides nine pre-defined action types that you can use to create response actions for Active Responder policies. The SMS provides hidden default actions (IPS Quarantine and Switch Disconnect) that you can implement in a response policy, and add flexibility to specific filters. You can also import scripts that define response actions. *Learn more on page 12-4*.

Important

The SMS defines the full implementation requirements for each action to ensure that your Responder policies are set up securely. To review the specific requirements for a particular action, click **Implementation** on the Response Action wizard.

Notification actions

You can specify a notification action that occurs when a response policy is triggered. SMS initiates these notifications when they are enabled in a policy that is enabled in an action set. You can implement one or more of these notification actions in a policy.

- **Syslog** — Sends an event to a syslog server when the response policy is triggered.
- **Email** — Sends an email to specified recipients when the policy is triggered.
- **Web** — Sends a Web request. Performs an HTTP GET on a URL.

- **SNMP Trap** — Enacts an SNMP Trap for the host traffic when the policy is triggered.

These notification actions apply to Active Responder policy notification, as opposed to IPS Profiles notifications settings that specify how SMS notification of filter events is handled.

Reputation entry actions

This action enables you to automatically enter offending IP addresses that the Active Responder service identifies into the Reputation Database.

Reputation entry actions have the following characteristics:

- The Reputation Database entry is only used by profiles that have a Reputation Filter defined with matching tag category values and has been distributed to one or more devices.
- You can specify tagged or untagged entries.
- You can assign tag values with any tag category currently defined in the Reputation Database and user-defined tags created in the **Add Tag Category** editor. Any changes to the tag definitions in the database can invalidate an action.
- You can aggregate entries and add them to the database every 60 minutes (recommended).
- You can control the total number of entries added to the database.
- Tag categories defined in Reputation Entry actions can conflict with Reputation filters that match the tag categories and have defined exceptions that can pre-empt triggering of the Reputation Entry action.

Add these actions to a policy and add the policy to an action set enabled for SMS Response.

IPS quarantine actions

A hard-coded IPS Quarantine action performs traffic management and reradiates Web requests as block actions or redirects them to a web page detailing issues they may have about their system. You can also add

accessible web sites allowed to the host while blocking all other access, such as to a virus detection company or software update web site.

The default IPS Quarantine action is set to block all traffic from hosts identified for quarantine, but you can modify these settings. For example, you may want to redirect suspect Web requests to a specified Web server. Incorporating this action in a policy with notification actions can provide an effective defense.

When the SMS has an IPS escalation policy with the IPS Quarantine action, it sends the unquarantine command to ALL managed devices, including the originator.

IPS Quarantine Response (Hidden) Action describes how the IPS behaves when the SMS adds an IP to its list of responded to IP addresses. You can edit this action to better meet the needs of your environment.

The IPS Quarantine action configured on an IPS device provides a first layer of defense. Using the SMS Quarantine response action provides greater flexibility in targeting quarantine behavior. Before you set up this action, you must configure a Profile action set for Active Responder.

Switch actions

A default Switch Disconnect action works with Active Responder policies for switches. This action works dynamically based on IP correlation. You can edit the name of this action, but cannot make any other changes. Specific instructions are required to implement this action.

Other actions are available to enact on switches or other network devices that have been defined in the Network Devices screen in Responder. Use these actions to effect remediation by directing targeted hosts to network devices or systems for remediation. The switch actions include the following:

- **Switch Disconnect** — Instructs the switch to momentarily disable the port, which causes the host to reauthenticate. On reauthentication, the RADIUS server rejects access. A default Switch Disconnect action works with Active Responder policies that apply to switches and works dynamically based on IP correlation. You can edit the name of this action, but you cannot make any other changes.

- **NMS Trap** — Integration with a network management system (NMS) to use an NMS Trap for a response action. An NMS Trap action sends an SNMP Trap to an NMS and performs other Response actions. NMS-type programs include: 3Com Transcend, 3Com Enterprise Management Suite, 3Com Network Supervisor, OpenNMS, Unicenter, OpenView, SunNet Manager, Traffic Director, eHealth, VitalSuite, and nGenius. Most functions of NMS Trap require access to switches and the associated IP correlation functions.
- **Move Quarantine Host onto a VLAN** — Moves a host triggered for a response action onto a VLAN. Switch policies can use all of the other available action types including the default actions and other switch actions.

Create or edit response actions

You can create action-based-response action types (SMS-defined and imported actions). In addition, you can edit or delete an existing action.

Procedure

1. On the Responder navigation pane, click **Actions**.
2. On the Response Actions screen, do one of the following:
   - To create a new response action, click **New**.
   - To edit an existing response action, select a response from the Response Actions list, and then click **Edit**. The Response Action wizard opens.
3. On the Action Name and Type screen, provide the following information:
   - **Action Name** — Specify or edit the name for the action. Use a name that is meaningful in describing the purpose of the action.
   - **Action Type** — Select a type from the Action Type list, if enabled.

Note

When you edit an existing action, you cannot modify the selected action type. You cannot edit a Switch Disconnect action; you can only change the name of this default action.

4. Click **Next** or select the next item from the wizard navigation menu and begin entering the values required for the action.
5. (Optional) To test a connection, click **Test**.
6. (Optional) Read the Implementation instructions. The implementation instructions describe what is required to use the action.
7. Click **Finish** to create the new action, or click **OK** if editing an existing action.

Create an email response action

The email response action specifies recipients to which the SMS sends email notifications when a response is triggered.

Note

Before you set up an Email action, the system SMTP Server must be configured under the **Admin** > **Server Properties** > **Network** section of the SMS. The system reply-to and from fields will be used if none are configured in this Email action.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **Email** from the Action Type list.
3. Click **Email Settings** (or click **Next**), and then enter the following:
   - **From** — Enter the email address where the notifying email originates (generally an SMS-specific email alias).

- **Reply To** — Enter the email address where replies are to be sent.
- **To** — Click the **Add** button, and then enter the email address where syslog email notices will be sent. To enter multiple email addresses, separate entries with a comma.
- **User Text** — Enter the email message.

Important

To implement this action, it must be listed in the **Actions** section of one or more Active Responder policies. *Learn more on page 12-39*.

Move a quarantined host onto a VLAN response action

The action to move a quarantined host onto a VLAN specifies a VLAN to quarantine suspect hosts.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **Move Quarantined Host onto a VLAN** from the Action Type list.
3. Click **VLAN Name** (or click **Next**), and then enter the following:
   - **VLAN Name** — Specify the name of the VLAN. Use a name that is meaningful in describing the network equipment that recognizes names. The actual interpretation of the name is configured on each device.
   - **VLAN ID** — Numeric tag, assumed to be 802.1Q compatible, that has a maximum value of 4094.

Create a NMS trap response action

The NMS trap response action specifies a network management system to use for quarantine enforcement at the switch-level.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **NMS Trap** from the Action Type list.
3. Click **NMS Trap Destination and Settings** (or click **Next**), and then enter the following:
   - **NMS IP address** — Specify the IP address of the NMS system.
   - **Destination Port** — Type a Destination Port (any value from 1-65535) or accept the default port (162).
4. Click **SNMP Settings** (or click **Next**), and then enter the following:
   - **SNMP Version** — Select the version of the SNMP agent to use for traps (version 2 or 3).
   - **Test OID** — Specifies the object identifier (OID) used for the trap.
   - **Community-based Security Model** — If using SNMPv2, specify the community string (for example: "public") to use when sending trap messages.
   - **User-based Security Model** — If using SNMPv3, specify the username and the authentication method and information required in your security model.
5. Click **Primary Action Settings** (or click **Next**), and then enter the following:
   - **Primary Action type** — Select RADIUS Reauthentication (default), VLAN isolation, or disable port to specify the action.
   - **NAM rule** — Specify the NAM rule if the NMS requires it.
   - **Active Directory Group** — Specify the active directory group to use for lookup.
   - **Quarantine VLAN** — Specify the quarantine VLAN address.
   - **Perform VLAN check** — Specify whether to check for VLAN preconditions before attempting this action.

- **Drop Port Link** — Drops the port link for 10 seconds if this action is successful. In some configurations, such as 802.1x with an XP client, this causes a DHCP lease renewal.

Note

This is the criteria used to enact the SMS response action. It is attempted first if you configure secondary and final settings for the action.

6. (Optional) Click **Secondary Action Settings** (or click **Next**) to specify the secondary action settings.

   These options are the same as what is described for primary action settings.

Create a Reputation entry response action

The Reputation entry response action specifies an entry that is automatically added to the Reputation database when targeted.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **Reputation Entry** from the Action Type list.
3. Click **Reputation Entry** (or click **Next**), and then enter the following information:
   - **Aggregate Entry Creation** — Select this checkbox to aggregate and save reputation entry requests to the database every 60 minutes. To add new reputation entries immediately, clear this checkbox.
   - **Maximum Reputation Entries** — Enter the maximum number (1-2000000) of reputation entries allowed by this action based on the capacity of your Reputation database.
   - **Tag Values** — Specify the tags and tag values that apply to the reputation entries created by this action by selecting the checkbox of those tags you want to apply.

4. (Optional) Click **Add Tag Category** to add a tag category that you define for the entries.

Create an SNMP trap response action

With the SNMP trap response action you can use SNMP trap notification for Active Responder events. This action sends an SNMP Trap to an SNMP agent (SNMP version 2 or 3).

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **SNMPTrap** from the Action Type list.
3. Click **Trap Destination** (or click **Next**), and then enter the following information:

   Note

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

   - Specify the trap destination Host and Port settings.
   - Select whether you want the SMS to send a trap when the action is closed.
4. Click **SNMP Settings** (or click **Next**), and then enter the following information:
   - **SNMP Version** — Version of SNMP to use when sending this trap.
   - **Community** — Group to which the destination host belongs. Only valid for SNMP v2.
   - **Engine ID** — Numeric ID that identifies this trap.
   - **User Name** — User login name to use for authentication. Defaults to *private* for a v3 trap. Value is only used for SNMP v3.

- **Authentication Protocol** — Protocol to use for authentication. Only valid for SNMP v3.
- **Authentication Key** — User login password to use for authentication. Only valid for SNMP v3.
- **Privacy Protocol** — Protocol to use for data protection. Only valid for SNMP v3.
- **Privacy Key** — Password to use for encrypting the trap. If no value is specified, the trap is not encrypted. Only valid for SNMP v3.

Important

To implement this action, add it to the **Actions** section of an Active Responder policy that is added to an action set enabled for SMS Response.

Create a syslog response action

The syslog response action enables you to specify a Syslog server where Active Responder sends events when a response is triggered.

Note: Before you set up a Syslog action, a UDP Syslog agent must be running on the Syslog destination IP and port configured for this action.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **Syslog** from the Action Type list.
3. Click **Syslog Settings** (or click **Next**), and then enter the following information:
   - **IP Address of Server (UDP)** — IP address of the syslog server.
   - **Port** — Listening port on the syslog server (0-65535). The default setting is 514.
   - **Facility** — Choose the syslog facility that applies.

Important

To implement this action, you must add it to an Active Responder policy. *Learn more on page 12-39*.

Create a web response action

Use the web response action to elicit a Web server response.

Procedure

1. Review *Create or edit a response action on page 12-43*.
2. Select **Web** from the Action Type list.
3. Click **Host Configuration** (or click **Next**), and enter the following information to specify the destination for the HTTP/HTTPS message:

Note

If a server is not specified, the URL must be fully specified (for example, http://xyzzy.com/page).

- **IP Address of Server** — IP address of the server running the HTTP/HTTPS service.
- **Port** — TCP port on which the service is listening.
- **Protocol** — protocol used for communicating with the server.
- **URL** — page to GET.

Host Authentication section

- For Host Authentication, select the **Use Authentication** check box.
- Select Authentication Type (Basic or Digest).
- Enter Username.
- Enter Password.

4. Click **Proxy Settings** (or click **Next**), and provide the following information, if using a proxy service for the Web server:

   Proxy Host Settings section

   - Select the **Use Proxy Host** checkbox.
   - Enter the name or address of the Proxy Host.
   - Enter the **Proxy Port** number.

   Host Authentication section

   - Select the **Use Authentication** checkbox.
   - Enter the Username to use for login authentication on the proxy host.
   - Enter Password.

Important

To implement this action, you must list it in the **Actions** section of one or more Active Responder policies and add it to an action set that is enabled for SMS Response. An HTTP Server must be running on the HTTP destination IP and port configured for this action.

Create an IPS quarantine response action

The IPS quarantine response action is the SMS default response action for IPS Quarantine. You can edit this action to specify how traffic is handled.

Procedure

1. On the Responder navigation pane, click **Actions**.
2. On the Response Actions screen, select **IPS Quarantine** on the Response Actions table.
3. Click **Quarantine Settings**, and enter the following information:

- **Web Requests** — Select one of the following actions: Block, Redirect to a Web server (an address is required), or Display quarantine Web page.
- **Other Traffic** — Select one of the following actions: Block or Permit.

4. To allow quarantined hosts to access specific sites, click **Quarantine Exceptions**, and then do one of the following:
   - Click **New** to create a new listing.
   - Select an existing listing, and then click **Edit**.
5. On the Quarantined Access Dialog, enter the following information:
   - **Name** — Specify or edit the name for the quarantined host. Use a name that is meaningful in describing the purpose of the quarantined action.
   - **Destination** — Type the IP Address.

Important

To implement this action, add it to a policy that specifies the values that trigger the response action.

Policies

An active responder policy defines the detection of a security event and the SMS response. Each policy may include the following:

- Segments from multiple managed devices
- One of each type of action you created
- IPS Quarantine action

The system provides a default response policy. This policy enacts when you manually respond to a host and the status is listed in the Response History table.

The method of configuring an active responder policy on an IPS segment is based on a response action set. You create an action set with the SMS action

equal to the Active Responder policy and then assign filters with the action set. Then you can distribute to the IPS segments or segment group where you want to enforce SMS Active Responder.

Policy setup options

The following policy setup options are available when setting up or editing an active responder policy:

- *Policy initiation on page 12-53*
- *Policy remediation communication (timeout) on page 12-54*
- *Inclusions and exclusions on page 12-54*
- *IP correlation and thresholding on page 12-55*
- *Actions on page 12-55*
- *IPS destinations on page 12-55*

Policy initiation

An active responder policy controls the security response state of a host. A policy defines a number of actions that occur during a response. These actions can potentially interact with a variety of networking equipment, including an NMS and ingress switches, to enforce a response. A policy also handles reversing these actions when a response is closed. You can initiate Active responder using these mechanisms:

- By correlating the event stream from a subset of managed IPS devices, and responding when threshold criteria are met.
- Manually, by choosing **File** > **Create Manual Response** and entering an IP address.
- Via a Web service call from an external NMS (Network Management System).
- By escalating an IPS Quarantine - which is local to that IPS - to a potentially network-wide SMS response.

Note

Limit SMS Policies that escalate the IPS Quarantine to one SMS active responder policy.

If there is already a host in SMS active responder and that host shares the same identity with an incoming IPS Quarantine escalation, the SMS does not escalate the IPS Quarantine into a new response event.

Policy remediation communication (timeout)

The response typically is ended when response actions are complete or the suspect host has had time for remediation to complete. This act must be communicated to the SMS using the same set of mechanisms that are used to initiate a response manually, by an external NMS, or other means. Optionally, you can configure a timeout to automatically close a response when a certain amount of time has passed since the last response request for a given end-station.

Inclusions and exclusions

An Active Responder policy also contains a list of hosts/networks with the following classifications:

- **Allow Active Responder** — Specifies the IP address ranges and subnets that are eligible for Active Response.
- **Never Respond** — Specifies the IP address ranges and subnets that will never trigger a response.

Typically, include IP addresses internal to your organization in the Allow List, with critical servers listed in the Never list.

Note

You can specify a multicast subnet or range in the inclusions and exclusions lists; however, you cannot specify a single multicast host.

IP correlation and thresholding

The SMS examines IPS alert logs from all managed IPS devices and correlates them using the attacker's IP address. Hit counts are qualified and accumulated within a sliding time window (the Threshold Period).

A response is automatically initiated when the accumulated hit count exceeds a threshold.

Hits are simply IPS events that meet these criteria:

- The attacking IP addresses are eligible for a response per the Inclusions and Exclusions lists.
- The attack was seen on one of the selected IPS Segments.
- The Filter that matched is one of the selected IPS Filters for this Policy.

Note

The IPS Profiles installed on any selected segments must have NOTIFY turned on for the selected filters in order for SMS to see the alerts.

Actions

When an end-station is acted on using this Policy, zero or more actions are executed to effect the response. The Policy itself lists configured actions, and incorporates a dependency capability that allows actions in the list to execute conditionally, based on the success or failure of earlier listed actions. *Learn more on page 12-40*.

IPS destinations

The SMS provides the option to distribute IPS actions to selected IPS devices. If an Active Responder policy contains an IPS action, you can select whether you want all the IPS devices or individual IPS devices to receive the Active Responder policy.

Default response policy

The default response policy is based on a special IPS action set. Every IPS contains this special hidden response action set that the SMS Active Responder application manages. This action set describes how the IPS behaves when the SMS adds an IP to its list of targeted IP addresses. You can make changes to the default response policy or create a new IPS quarantine with additional configuration options.

Edit the default response policy

You can modify the criteria defined in the policy and more finely-tune the default response.

Procedure

1. On the Responder navigation pane, click **Policies**.
2. On the Policies screen, select the Default Response entry from the Active Responder Policies list, and then click **Edit**.

   The Active Response Policy wizard opens.
3. On the Initiation and Timeout screen, enter the following information:
   - Specify the mechanism to use to initiate the policy. See *Policy initiation on page 12-53*.
   - To set a timeout option, select **Enable Automatic Timeout** and enter a time in minutes, hours, or days.

   Note

   Enabling automatic timeout automatically ends the continued application of Response Actions after the prescribed time limit even if remediation has not occurred.
4. Click **Inclusions and Exclusions**.
5. Specify the hosts/networks to **Allow Active Response** or **Never Respond**.

6. Click the arrow next to a field to add an existing Named Resource or to create a new Named Resource.

7. If it is enabled, select **Correlation and Thresholding**, and provide settings in the Automatic Response Configuration and Qualified Filter Hit Notifications sections.

Note

The Correlation and Thresholding screen is available only if you select **Enable Policy** on the Initiation and Timeout screen.

8. Select **Actions**, and then enter the following information:

   - **Priority** — The order in which the actions are to be performed.
   - **Action** — Name assigned to the action that you created.
   - **Condition** — Trigger for running the action. This option is set when you add a new action to the Response Policy. You can change it by editing a select action on this screen.
   - **Dependency** — Specify what other action must take place for this action to be triggered.

9. Click **Add** to add a Response Action, or select an existing action entry, and then click **Edit**.

10. In the Response Action dialog, enter the following information:

    - Select an Action from the menu, or click **New** to create a new Response Action.
    - Select an option under **Conditional Execution**. The selections available in the Action menu are Response Actions from the **Active Response (Actions)** area.

11. To create dependencies when you add an action:

    a. In the **Action** list, select an action to add.

    b. Under Conditional Execution, select either **Only on success of** or **Only on failure of**.

c. In the list, select the action to connect for dependency.

For example, if you add an action called Email Admin with an action type of Email, you have an existing action called Switch Down (Switch Disconnect type). For Email Admin, if you specify Only on success of Switch Down, then when the switch goes down, the email action sends a message informing the network administrator.

12. On the Actions screen, review the listed actions.

To change the priority of a selected action, use the up and down arrows to change the location of the selected action in the list.

13. In the IPS Destinations screen, select which devices will receive the Response Policy.

- To distribute to all IPS devices, select the **All Devices** checkbox.
- To distribute to selected IPS devices, expand the **All Devices** entry, and then select one or more IPS devices.

14. Click **OK**.

Manual response

You can manually respond to a targeted host by specifying the IP address of the host and the policy that you want to trigger for that host. When you initiate a manual response, if the Response policy includes an IPS action, you can select one or more devices to which to apply the response.

Initiate a manual response

Procedure

1. 1. On the Responder workspace, click **File**, and then click **Create Manual Response**.

2. Enter an IP Address of a host for which to trigger a response.

3. Select a Policy Name from the list.

The SMS enacts this policy against the targeted host.

4. (Optional) Select the **Enable Automatic Timeout** checkbox, and specify the number of minutes the system enforces the policy action or actions.

   Setting this option automatically ends the application of Response actions after the prescribed time limit even if remediation has not occurred.

5. Select **All devices** or individual devices if the policy you want to apply contains an IPS action.

6. Click **OK**.

New response policies

New response policies provide more configuration options than the default response policy and allow you to finely tune your response. Responder supports multiple action sets that you can add to a response policy.

You can initiate multiple IPS Quarantine actions from the SMS. For new response policies, you must set up a profile action set with IPS quarantine defined before you set up the response policy. *Learn more on page 12-43*.

Create or edit a new response policy

Procedure

1. 1. On the Responder navigation pane, click **Policies**.

2. On the Active Response Policies screen, click **New**, or select an existing policy from the **Active Response Policies** list, and then click **Edit**.

3. In the Active Response Policy wizard, specify the following on the Initiation and Timeout screen:

   a. Specify a **Policy Name**.

   b. Specify the mechanism to use to initiate the policy. *Learn more on page 12-53*.

   c. To set the timeout option, select the **Enable Automatic Timeout** checkbox and enter the number of minutes, hours, or days.

Setting this option automatically closes the response action for an end-station after the prescribed time limit even if remediation has not occurred.

d. Click **Next**, or select **Inclusions and Exclusions** from the wizard navigation tree.

4. On the **Inclusions and Exclusions** screen, specify the hosts or networks to **Allow Active Response** or **Never Respond**.

   Click the arrow next to a field to add an existing **Named Resource** or to create a new **Named Resource**. *Learn more on page 12-54*.

5. Click **Next**, or select **Correlation and Thresholding** from the wizard navigation pane.

6. For Correlation and Thresholding, enter the following settings:

   Automatic Response Configuration:

   - **Qualified filter hits** — The number of hits to enact the policy.
   - **Threshold period** — The period of time in seconds or minutes for the hit count threshold.
   - **Quiet period** — The Quiet Period begins when the automatic response action is initiated. A new Threshold Period will not begin until the Quiet Period is over.

   Qualified Filter Hit Notifications :

   - Select **Send Syslog Notification** to send a message to the syslog. Enter a server and select a port and facility for the syslog.
   - Select **Send SNMP Trap Notification** to send a message to the SNMP trap. Enter a destination and select a port.

7. Select **Actions** from the wizard navigation pane.

8. The **Actions** screen lists the actions that are associated with the policy and the following information:

   - **Priority** — The order in which the actions are to be performed.

- **Action** — Name assigned to the action that you created. *Learn more on page 12-43*.
- **Condition** — Trigger for running the action. This option is set when you add a new action to the Active Responder policy. You can change it by editing a select action through this screen.
- **Dependency** — Specify what other action must take place for this action to be triggered.

9. In the **Actions** screen, click **Add** to add a new Response action or select an existing action entry, and then click **Edit**.

Note

The SMS supports multiple IPS action sets. You must set up a Profile action set with IPS Quarantine defined before you set up an Active Responder policy.

10. On the Response Action screen, select an action to add from the menu.

    You created these actions in the **Actions** screen for Active Response. When adding additional actions, you can create dependencies between the actions:

    a. Select an action to add.

    b. Select an option: success on or failure on.

    c. Select the action to connect for dependency.

    For example, the added action called Email Admin (email type) could have a dependency on the previously added action of Switch Down (switch disconnect type). In this situation, when the switch went down, the email action sends a message informing the network administrator.

11. Click **OK** to return to the setup wizard.

12. On the **Actions** screen, review the listed actions.

    To change the priority of a selected action, use the up and down arrows to change the location of the selected action in the list.

13. Click **Next**.
14. In the **IPS Destinations** screen, you can select which devices will receive the Active Responder policy.
    a. To send an IPS action to all devices with qualified hits, select **Send IPS Action only to the device which triggered the threshold**.
    b. To send the IPS action to one or more devices, select one or more devices.

    When you configure an IPS Quarantine action for a stack, propagate the policy to the stack so that any stack member that inspects the traffic can also quarantine the traffic when necessary.
15. On the Active Response Policy setup wizard, click **Finish** to save your settings.

Responder network devices

Responder supports a number of hardware infrastructure elements. These elements use one or both of two separate authentication methods, RADA and 802.1x.

Note

If network devices are defined and you have not enabled the RADIUS proxy, Active Responder uses RFC 1493 (BRIDGE-MIB) to provide a MAC address to switch IP and port mapping. You must develop device scripts that perform the actual switch actions separately.

From the **Network Devices** screen in the Responder workspace you can add network devices that you want to configure for Responder. This page lists the supported network device types.

Auto discovery of switches

The SMS can automatically discover network devices for use by IP/MAC Correlation and Responder. This feature discovers the network devices on

your network and allows you to choose the devices you want to add. You can add a single device or multiple devices.

Because the discovery process uses SNMP to discover the devices, you must enable SNMP and use a common authorization method on the devices to be discovered. IP/MAC Correlation uses Layer 3 devices (routers) that support RFC 1213. Switch actions use Layer 2 devices (access switches) to disconnect access ports or change their VLAN.

Note

In order to initiate a switch level response, the SMS must know the MAC address of the target device and then match that to an IP address targeted for the Response action.

Configure auto discovery of network devices

Before you begin, you must enable SNMP and make sure all devices share the same SNMP credentials.

Procedure

1. On the Responder navigation pane, click **Network Devices**.
2. On the Network Devices screen, click **Discover**.
3. On the Discover Network Devices dialog, select options for the following:
   - **Search Method** — Select Subnet and enter an IP Range, or select Cisco Discovery Protocol and enter a router.
   - **SNMP** — Enter a port number, select a version, and then click **OK**.
4. Select the device or devices to include, and then click **Add**.
5. On the **Active Responder Options** tab, select options for the following:

   RADIUS Options

   - Use RADIUS Authentication

- Enforce switch actions using RADIUS
- Prefer VLAN symbolic name over ID

Device Usage

- Use this device for IP to MAC Correlation
- Use this device for Access Control

6. Click **Next**, or select **SNMP Settings**.
7. On the **SNMP Settings** tab, select the appropriate **SNMP Settings**:
   - Community-based Security Model
   - User-based Security Model
8. Click **Next**, or select **Telnet Settings**.
9. On the **Telnet Settings** tab under the User Authentication area, enter the administrative username and password for the selected access device(s).
10. On the **Telnet Settings** tab under the Connection Settings area, select the **Session Timeout** and the **Telnet Port** to use for the connection.
11. Click **Finish**. The selected device(s) are added to the Network Devices table.

Adding a switch

Some network architectures employ switches for managing and maintaining traffic. Typical equipment includes:

- **Network ingress switches** — Switches in your network to which end-stations that can be quarantined are directly connected.
- **Edge routers** — Those routers that are closest to end-stations that are able to be quarantined. Ensure that edge routers have no other layer-3 devices between them and end-stations, and that they can see the true MAC address of end-stations.

Responder supports the following device types:

- 3Com4400, 5500, and 7750
- Cisco 2950 IOS, 6500 IOS
- Generic Cisco Switch
- Generic Router
- Generic Switch

Add or edit a switch

Procedure

1. On the Responder navigation pane, click **Network Devices**.
2. On the **Network Devices** screen, click **New**, or select an existing entry in the Network Devices list, and then click **Edit**.

   The Network Equipment wizard displays.
3. On the **Device Address and Type** screen, enter an IP Address for the switch and select a Switch Type from the menu.
4. Click **SNMP Settings** (or click **Next**), and then provide the **SNMP Version** and the **SNMP Port** for the device.
5. In the **Community-based Security Model** section, provide the appropriate values for Read Community and Write Community.
6. In the user-based Security Model area, provide the appropriate information in the following fields:

   - Engine ID
   - User Name
   - Authentication Protocol
   - Authentication Key
   - Privacy Protocol
   - Privacy Key

Note

The 3Com 7750 and 3Com 5500 switches support RFC1213 IP Correlation. To use IP Correlation with these switches, be sure to select Use this device for IP to MAC Correlation (ARP, via RFC 1213) on the configuration screen for your particular 3Com switch. To test this action, click **Test**.

7. Click **Next**, or select **Implementation** in the wizard navigation pane.
8. Click **Finish**.

Chapter 13

SMS Web Management

The SMS web management console provides comprehensive visibility into your network with data that reflects the health, status, and security events related to your system. Operational, security, and performance contexts enable you to fine-tune your security policies for maximum effectiveness.

To log in to the SMS web management console, open a supported web browser (the most current version of Mozilla Firefox, Microsoft Edge, Apple Safari, or Google Chrome), and type `https://` followed by the IP address that you configured as the management address for the SMS server.

Integrate SMS with Trend Vision One™

You can maximize your protection by integrating your SMS web management console with Trend Vision One™. To learn more, refer to *Integrating SMS with Trend Vision One™ Software Guide*.

Logging in to the SMS web management console

After the SMS server is configured and your user account has been defined, you can connect to the SMS web management console.

Enter `https://<SMS IP address or host name>` in the web browser to display the SMS login page. After you log in, the SMS web management console Dashboard is displayed.

Threat Insights

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

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

Threat Insights include:

- *Compromised Hosts on page 13-3*
- *Attacked Vulnerable Hosts on page 13-5*
- *Suspicious Objects on page 13-7*
- *ZDI Filter Hits on page 13-9*

Filter by time period

The Threat Insights events list is refreshed approximately every minute with the most recent events listed at the top. When the maximum number of Threat Insights events that can be displayed is reached, the oldest event is

deleted to allow new events to be displayed. You can also reload the page to keep the list updated.

By default, the events from the last 30 days are displayed when you access Threat Insights from a laptop or desktop computer. You can further filter your results to events from the last seven days or the last 24 hours. Events from the last 24 hours are displayed when you access Threat Insights from a mobile device. To narrow larger sets of events to a specific time period, you can configure a custom date and time range.

To filter the number of Threat Insights events by time period or to adjust the time period, always return to the Dashboard and specify a time period from the **Time period** list at the upper right corner.

Note

Predisclosed filter event hits are displayed regardless of the time range you select. For example, if you narrow the ZDI Filter Hits to the last 7 days, an event from the last 30 days will still be displayed.

Compromised Hosts

Compromised Hosts identify hosts in your network that might be compromised based on intelligence gathered from your Deep Discovery devices, TPS devices, and IPS devices. Security intelligence is leveraged to identify:

- Domain generation algorithms (DGA) defense malware filters
- Reputation events that score hosts and provide context from policy and attack filters

ThreatDV delivers a weekly malware filter package to help protect against the latest advanced threats. It prevents and disrupts malware activity, secures sensitive data, and optimizes network performance. ThreatDV also includes reputation feeds that are updated multiple times a day. Entries are assigned a threat score between 1 to 100 based on a comprehensive analysis of the activity, source, category, and threat. Malware filters are designed to detect:

- Infiltration

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

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

To identify compromised hosts in your network environment, you must register your device for the ThreatDV service.

You can use newly discovered threats forwarded from your Deep Discovery devices to identify compromised hosts in your network. The Deep Discovery devices detect suspicious network traffic between hosts and discovered C&C servers.

To include the C&C Callback Address data from your Deep Discovery device, you must include the following predefined tag categories on the SMS (Learn more: *Tag Categories on page 5-84*):

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

To view, select **Threat Insights** > **Compromised Hosts Threat Insights**.

Heading	Description
IP Address	IP address (either source or destination) of the identified compromised host.
Host Name	Host name of the IP address, if available.
Last Compromised Filter	The name of the filter that either matches traffic from the compromised host or traffic to the compromised host.
Last Hit Time	The time on the device that the traffic was last encountered.
Blocked Hits	Number of times traffic was blocked by a filter and an event was generated.
Permitted Hits	Number of times traffic matched a filter and was permitted to flow through. If you see permitted hits, consider updating your security policy. You can change the action set to **Block** or **Block + Notify**. You can also associate your policy with a Responder Policy.

Attacked Vulnerable Hosts

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

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

Importing vulnerability scan data to the SMS — Before you can identify attacked vulnerable hosts in your network, you must first run a vulnerability scan using a third-party vendor and import this data to the SMS. Learn more: *Import vulnerability scans on page 5-112*.

To view Attacked Vulnerable Hosts on the SMS web management console select **Threat Insights** > **Attacked Vulnerable Hosts**. The following information displays.

Heading	Description
Expand/ Collapse	Controls visibility to the relevant filters associated with the vulnerable host identified in a vulnerability scan. Expand to view additional information including: • Relevant filter name • Vulnerabilities identified including the CVE ID • Last hit time • Number of blocked hits • Number of permitted hits
IP Address	Network IP address of the vulnerable host.
Host Name	Host name of the IP address, if available.
Last Scan	Name of the vulnerability scan file available on the SMS, and the number of days since it was imported to the SMS. Consider importing a new vulnerability scan file to replace files that are older than two weeks.
Relevant Filters	The number of filters identified. When you expand the table column, the name of the filter displays in addition to the vulnerabilities. The SMS establishes a correlation between the CVE IDs provided from a vulnerability scan and the CVE IDs included in the DV filters. Using this information, the relevant filters are displayed.
Vulnerabilities	When you expand the table column, the name of the filter is displayed along with any associated vulnerabilities. Expand an event to see the CVE ID identified in the DV filter.
Last Hit Time	Date and time when the relevant filter was processed by the inspection, and traffic was either blocked or permitted.
Blocked Hits	Number of times traffic was blocked by a filter and an event was generated.
Permitted Hits	Number of times traffic matched a filter and was permitted to flow through. If you see permitted hits, consider updating your security policy. Learn more: *Profile tuning on page 5-120*

Suspicious Objects

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

When your Deep Discovery device detects a threat, it alerts your TippingPoint IPS and TPS devices by forwarding threat intelligence to the SMS. To view the Suspicious Objects on the SMS, select **Profiles** > **Reputation Database** > **Search Entries** > **Tag Criteria** > **Trend Micro Detection Category** > **Tag value is any of Suspicious Object**, and then click **Search**.

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

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

Requirements

Note the following prerequisites before any data can be displayed for Suspicious Objects:

- Configure predefined tag categories. Learn more: *Tag Categories on page 5-84*
- Enable **HTTP Context** from the Reputation filter. Select the **Trend Micro Detection Category** check box, and then select a **Suspicious Object** value. Select the **Trend Micro Severity** check box, and then select a value. Learn more: *Create or edit a Reputation filter on page 5-43*
- Enable **HTTP Context** on the profile. Learn more: *Create a new profile on page 5-14*

To view Suspicious Objects on the SMS web management console, select **Threat Insights** > **Suspicious Objects**. The following information displays.

Heading	Description
Object	IP address, host name, or URL, if available, of the suspicious object.
Severity	Severity identified for the suspicious object, based on the **Trend Micro Severity** tag category. Learn more: *Tag Categories on page 5-84*

Action in Profiles	Every profile that is configured for Reputation has at least one reputation filter. For a profile to block or permit Suspicious Objects, its reputation filter must specify the following criteria:
	
	• Entry criteria that matches the predefined tag categories for Suspicious Objects. Learn more: *Tag Categories on page 5-84*
	• The filter is enabled.
	• The action is set to **block** or **permit**.
	
	Your security policy, as it relates to Suspicious Objects, is expressed using the following categories:
	
	• **Protected** – All profiles configured for reputation *block* Suspicious Objects.
	• **Partially protected** – Some profiles configured for reputation *block* Suspicious Objects, and other profiles *permit* Suspicious Objects.
	• **Monitored** – All profiles configured for reputation *permit* Suspicious Objects.
	• **Unprotected** – Displays for any of the following reasons:
	  • At least one profile is configured for reputation, but no filter is configured for Suspicious Objects on the SMS.
	  • A reputation filter matches but it is disabled.
	  • No profile is configured for reputation on the SMS.
	
	If you see **Unprotected**, consider updating your security policy.
	
	Learn more: *Action sets on page 5-3*

Last Hit Time	Date and time that the filter was processed by the inspection.

Heading	Description
Blocked Hits	Number of times traffic was blocked by a filter and an event was generated.
Permitted Hits	Number of times traffic matched a filter and was permitted to flow through. If you see permitted hits, consider updating your security policy. You can change the action set to **block** or **block + notify**. Learn more: *Action sets on page 5-3*

ZDI Filter Hits

Zero Day Initiative (ZDI) Filter Hits identify blocked and permitted hits for predisclosed and disclosed filters.

DV filter protection covers the time between when a vulnerability is discovered and when a patch is made available. In addition, DV filters provide added protection for legacy, unsupported software. DV packages are delivered weekly, or immediately when critical vulnerabilities emerge, and can be deployed automatically with no user interaction required. Learn more: *Digital Vaccines on page 5-53*.

ZDI Filter Hits include:

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

  Note

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

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

To view ZDI Filter Hits on the SMS web management console, select **Threat Insights** > **ZDI Filter Hits**. The following information displays.

Heading	Description
Filter	Name of the filter that generated the alert or block.
CVE	Unique tracking number used to identify a Common Vulnerabilities and Exposures (CVE). CVE IDs are publicly known security vulnerabilities.
Released	Date the filter was released by the TMC.
Filter Disclosed	Date the filter was publicly disclosed, if available.
Last Hit Time	Date and time that the filter was processed by the inspection.
Blocked Hits	Number of times traffic was blocked by a filter and an event was generated.
Permitted Hits	Number of times traffic matched a filter and was permitted to flow through. If you see permitted hits, consider updating your security policy. You can change the action set to **block** or **block + notify**. Learn more: *Action sets on page 5-3*. You can also associate your policy with a Responder Policy. Learn more:

Filters for Review

Use Filters for Review to make strategic changes to your security policy according to filter factors relevant to the policy.

By providing operational, security, and performance contexts, this interface enables you to target your filters to known active threats.

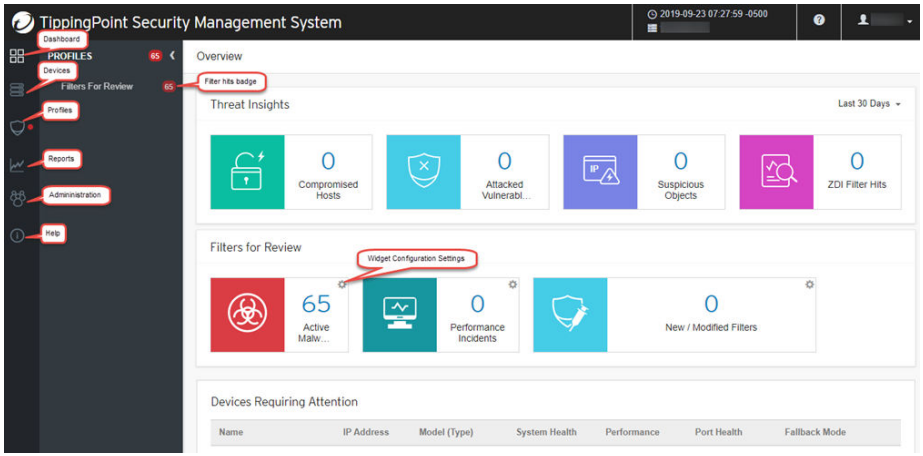
Using the detailed context provided for each filter, you can maximize the effectiveness of your security policy by:

- Fine-tuning your policies to enable only those filters that are relevant to your environment
- Negotiating the tradeoff between higher security and higher performance
- More efficiently blocking bad traffic without hampering good traffic

- Identifying the conditions surrounding congestion

A red badge next to the navigation panel's Profiles icon alerts you that you have profiles with filters that have been flagged for review. When you click the Profiles icon, the expanded navigation shows another badge next to Filters for Review that indicates how many filters have been flagged.

Refer to the following image of the Dashboard.



Filters are automatically flagged for review according to the criteria identified by the following Dashboard widgets:

- **Active Malware Threats** – Real-world malware that actively exploits network vulnerabilities.
- **Performance Incidents** – Traffic-based anomalies, such as Adaptive Filter Configuration (AFC) events.

Note

To display performance incidents, *configure your device for AFC on page 3-68* and distribute at least one profile to the device. Because the polling that associates distributed profiles with your device runs every five minutes, expect a corresponding delay before performance incidents are displayed.

- **New / Modified Filters** – New filters or enhancements to existing filters provided in a Digital Vaccine (DV) or Auxiliary DV package.

Note

A filter remains flagged until the malware threat gets demoted as a top threat or expires. For new and modified filters, there is no expiration.

When you click the Dashboard widget you want to review, a list of filters for that category is displayed. Active Malware filters are displayed in order of security importance; other filters are displayed sequentially by filter number. You can narrow the list by **Flag Type**, **Review Status**, and **Snooze Status** on the toolbar.

To determine a filter's security importance, the Trend SMART Protection Network (SPN) compiles security information from a conglomeration of sources. After it ranks the threats, SPN then combines the data with TippingPoint Digital Vaccine (DV) intelligence for the final output, which is provided to the SMS by the Threat Management Center (TMC). A filter's final ranking on the list depends on a number of factors. For example, a filter with a minor severity can be higher on the list than a filter with a critical severity if it has a higher prevalence.

From the list, click a filter to see an overview of it, including:

- Information about the filter's function
- Release/modification dates
- Severity
- Source

- Category
- CVE identifications

The context panel to the right of the console displays the following tabs with details of how the filter is used in your security policy:

- **Flags** – List of flags associated with the filter, and when that flag occurred. You can change the review status of this filter's flag by clicking the **Actions** drop-down menu. If you want to re-evaluate this flag later, set the action to **Snooze** and select a time period. If you have the required permissions, click the **Add Flag** button to add your own custom flag.

  Note

  You can edit filter settings only within the context of a profile using the SMS client. If you do edit a filter's settings, remember to also use the SMS client to redistribute all profiles that contain that filter.

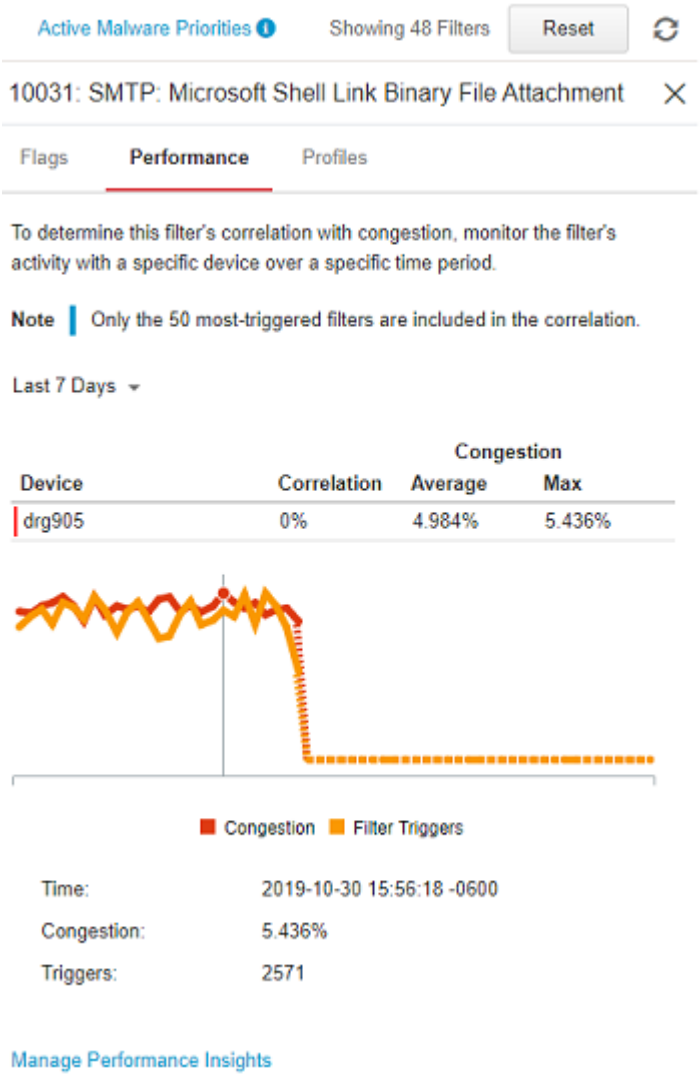
- **Performance** – An interactive graph is displayed showing filter activity in correlation to a device's CPU congestion over a period of time that you specify. Although you can configure this for up to 20 devices, only the top 10 devices with the highest correlation rates are used to calculate the data. To see this graph, configure Filter Performance Correlation on a device that has this filter enabled. *Learn more on page 13-17*. Hovering over different points in the graph presents congestion statistics, including:

  - The precise time reflected at that point on the graph.
  - The percentage of congestion reflected at that point.
  - The number of times the filter was triggered at that point.

  Note

  A trigger count of 0 (zero) indicates that this filter was not one of the 50 most-triggered filters for the specified time period. It does not reflect the actual number of filter triggers.



The performance table lists the device with the highest correlation at the top, and the graph you see is for that device. Because the data is

dynamic, you might see the graph for a different device each time you refresh the page. To see the correlation graph for any other device, click the device in the table.

Any portion of the graph showing a dashed line indicates that no data is available during the specified time period. Time, congestion, and trigger statistics will not be displayed.

- **Profiles** – A list of profiles that use this filter, and, if the filter is in an **Enabled** state, the action set your profile has configured for the filter. A label of **Recommended** indicates that the recommended settings for the filter are applied.

Take action on a filter

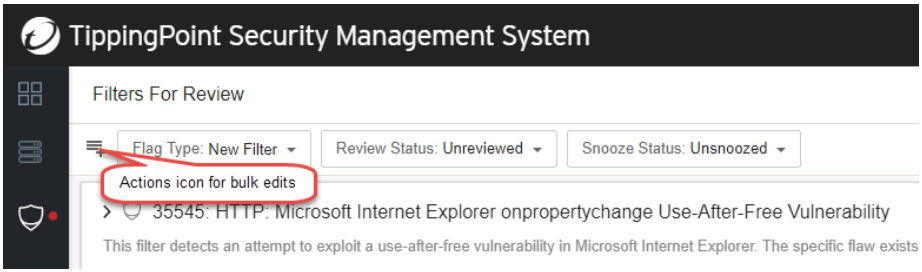
After reviewing a flagged filter, you can perform any of the following actions:

- Mark flagged filters as **Reviewed**, or change those you have already reviewed back to **Unreviewed**. This enables you to keep the Filters for Review page current and more manageable.
- Set a flagged filter to **Snoozed** for a specified time period so that you can follow up with it later. You can also set the filter back to **Unsnoozed** at anytime.
- Add or remove one of your own custom flags to the filter. For example, you can add a flag to the filter so that it is brought to the attention of a specific person. If you do not have the required permissions to manage profiles, the **Add Flag** button is not available. To enable the **Add Flag** button, you must configure a user role with that capability:
  1. Using the SMS client, create a user role by selecting **Admin** > **Authentication and Authorization** > **Roles**. *Learn more on page 8-49*.
  2. With **Capabilities** selected from the navigation tree, click **Profiles** and ensure that the **Manage filter flags** option is selected for your role.
  3. Assign the new role to a group. *Learn more on page 8-50*.
  4. Assign the group to your user account. *Learn more on page 8-37*.

Note

You can only remove custom flags. You cannot remove a system-generated flag. A filter with a system-generated flag remains flagged until the malware threat gets demoted as a top threat or expires. For new and modified filters, there is no expiration.

You can apply the action you select to an individual filter or to many filters at the same time. To apply your action to many or all filters, click the **Actions** icon at the far left of the Filters for Review toolbar to enter Bulk Action mode. To apply your action to all filters, select the topmost checkbox. To apply the action only to certain filters, select specific checkboxes on the list.



Configure auto-flagging

You can adjust auto-flagging according to your requirements. For example, you might decide to disable auto-flagging on filters that protect against vulnerabilities that are not relevant to your network environment. Alternatively, you can keep auto-flagging enabled on a filter while disabling it on specific profiles that you select.

Note

Auto-flagging is enabled by default. When you disable auto-flagging or specify profiles where it is to be excluded, all relevant existing flags will be removed.

To configure auto-flagging:

Procedure

1. Click the Configuration Settings cog of the filter widget (refer to the Dashboard image in *Filters for Review on page 13-10*).
2. Set auto-flagging for the filter to **Enable**.
3. To keep auto-flagging enabled but excluded from specific profiles, select the **Exclude Profile(s)** checkbox and specify which profiles you do not want auto-flagged for this filter.

Configure Filter Performance Correlation

When you have Filter Performance Correlation configured, the Performance tab displays an interactive graph that tracks filter activity in correlation to your device's traffic congestion over a specified period of time.

Procedure

1. From the left navigation panel, click the **Devices** icon and select **Performance Insights**.

   Alternatively, when reviewing a filter, you can select the Performance tab on the context panel to the right of the SMS web management console and click **Manage Performance Insights**.
2. On the Performance Insights screen, click **Configure Filter Performance Correlation** for your device. You can set this for up to 20 devices.

   Note

   Devices retain this setting even after you unmanage them. If your SMS already has 20 devices configured for Filter Performance Correlation, and you remanage a device on which you had previously enabled the setting, a notification informs you that the SMS has automatically disabled this setting for the remanaged device.
3. From the drop-down menu above the graph, specify the performance period that you want monitored.

Note

For a graph to be displayed, your device must have this filter enabled for the time range that you specify. If the query period you specify exceeds the period for which data is retained (60 days for SMS models prior to H4 and H4 XL; 90 days for SMS models beginning with H4 and H4 XL), an error message is displayed instead of the data. Data is collected every five minutes.

4. Optionally, share the Filter Performance Correlation data with the TMC by enabling ThreatLinQ Event Sharing (from the SMS client, select **Edit** > **Preferences** > **TMC Information Share**). *Learn more on page 10-3*.

Monitor all devices

You can view all devices, device groups, clusters, and stacks added on the SMS, whether the device is currently managed or unmanaged.

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

If the device is functioning properly, the System Health, Performance, and Port Health status indicators are green. If a device has issues with its health status, the status indicators change color, and the device is listed on the *Devices Requiring Attention on page 13-19* panel. If a device is unmanaged, a message is displayed under the System Health, Performance, and Port Health.

To monitor your devices, log in to the SMS web management console, and from the navigation panel click the Devices icon and select **All Devices**. The All Devices page displays the following information.

Heading	Description
Name	Name (and icon) of the device. If a device is included in a device group, select the name of the device group to drill down or expand the device information.

Heading	Description
IP Address	IP address used to connect to the device.
Model	Model and type of the device.
System Health	Indicator that provides information about the hardware components of the managed device. If the System Health indicator displays an error, you can view the error on the SMS System Log.
Performance	Indicator that provides top-level performance information of the managed device, such as packet statistics or CPU.
Port Health	Indicator that tracks key port statistics for the managed device.
Fallback Mode	Indicates current fallback status. Learn more: at *Switch a device into fallback mode on page 13-20*.

Identify devices that require your attention

You can quickly identify and respond to devices that might have health or performance issues.

To view devices that require your attention, scroll down to the **Devices Requiring Attention** panel of the Dashboard. The following information displays.

Heading	Description
Name	Name (and icon) of the device that has system health, performance, or port health issues.
IP Address	IP address used to connect to the device.
Model	Model and type of the device.
System Health	Indicates a potential issue with the hardware components of a device. If the System Health indicator displays an error, you can view the error on the SMS System Log.
Performance	Indicates top-level performance issues of a device, such as packet statistics or CPU.
Port Health	Indicates port health issues of a device.

Heading	Description
Fallback Mode	Indicates current fallback status of a device. If the device is in fallback mode, an explanation displays. To switch a device into fallback mode, see *Switch a device into fallback mode on page 13-20*.

Switch a device into fallback mode

In the event of a server outage, or if you detect a system failure, you can automatically switch to the fallback mode on a device. The fallback mode determines how a device manages traffic on each segment in the event of a system failure.

You can switch the fallback mode on the device from your mobile phone or tablet.

Procedure

1. Select a device on the SMS web management console.
2. Set the fallback mode to **On**.

   When a device is in fallback mode, it either permits or blocks all traffic on each segment, depending on the segment action setting. When a device is in fallback, any traffic allowed through the device is not inspected; it simply passes through the device.

   You cannot switch the fallback mode if the device is unable to communicate with the SMS.
3. Select **Confirm**.
4. To remove the fallback mode on a device, set the mode to **Off**.

View or download saved reports

You can view or download your saved reports from the SMS. Learn more: *Saved reports on page 7-22*.

Procedure

1. Select **Reports** on the SMS web management console.
2. Select **Saved Reports** and then select a report name.
3. To download a report, select a file type: **PDF**, **CSV**, **XML**, **DOCX**, or **XLS**.

Download exported or archived files

You can download exported or archived files from the SMS. Learn more: *Exports and Archives on page 8-128*.

Procedure

1. From the navigation panel of the SMS web management console Dashboard, select the Administration icon.
2. Select **Exports and Archives**.
3. To download a file, select the checkbox next to the filename, and click **Download**.
4. To delete one or more files, select the checkboxes next to the filenames, and click **Delete Selected**.
5. To delete all files, click **Delete All**.

View system logs

You can view system log messages sent from the SMS client. System logs are sent to the SMS web management console as they are generated with the most recent messages listed at the top. For each event, the system log displays the date and time, severity level and color-coded icon, and description.

To view the system logs, you must use a laptop or desktop workstation to access the SMS web management console.

Procedure

1. From the navigation panel of the SMS web management console Dashboard, click the Administration icon.
2. Select **System Logs**.
3. Select an option to filter the system logs by severity level.
4. To filter the system logs by date or time, select an option:
   - **Latest** to view the latest SMS system log messages.
   - **Custom Range** to filter the SMS system log messages by selecting or entering a start date (and time) and an end date (and time) from the calendar. This is helpful if your search has resulted in a large set and you want to narrow your results to a specific time range.

Install or upgrade the SMS client

- You must use a laptop or desktop computer to install the SMS client.
- To communicate with the SMS server, the SMS client must use TCP ports 9033 and 10042.
- Make sure your system meets TMC port requirements. Learn more: *Ports on page 4-1*.

Procedure

1. From the navigation panel of the SMS web management console Dashboard, select the Help icon.
2. Click **Client Installation**.
3. Download the installer appropriate for your system.
4. Complete the installation:
   - **For Windows workstations:** In the Download Complete dialog, click the **Open** button to start the SMS client installer.

- **For Linux workstations:**
  a. Ensure that the user installing the SMS client is also the user that will be running the client.
  b. From the directory containing the installer, run `chmod 755 SMSInstall.sh;./SMSInstall.sh`
- **For Mac workstations:**
  a. Install Java Runtime Environment (JRE) version 1.8.
  b. Open the `dmg` (disk image) file and run the installer application.
  c. For versions 1.8u71 and later, continue to step d. For versions prior to 1.8u71, continue to step e.
  d. Edit the `java.security` file located in the `/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security` directory:
     - Remove MD5 from the line `jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024` so that it is now `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024`.
     - Remove MD5withRSA from the line `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768` so that it is now `jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768ph`.
  e. Go to **System Preferences** > **Security & Privacy Settings** and configure the **Allow applications downloaded from** to **Anywhere**.

Note

If the **Anywhere** option is not available, enter the following command from your terminal (**System Preferences** > **Finder** > **Go** > **Utilities** > **Terminal**):

```
sudo spctl --master-disable
```

f. After you complete the SMS Client installation, reset your **Security & Privacy Settings** to their defaults.

Logging in to the SMS client

Log in to a single SMS client. For distributed management, you can log in to multiple SMS clients.

Procedure

1. Launch the SMS client.
2. Enter the IP address or fully qualified host name in the **SMS Server** field.
3. (Optional) To log into multiple SMS server clients:
   a. Click **More**.
   b. Select **Multiple SMS Servers**.
   c. Click **Add**.
   d. Specify the IP address or host name in the **SMS Servers** field, and click **Connect**.
   e. Repeat for each SMS server.
4. Click **Login**.

   You can also log in using the Command Line Interface (CLI).

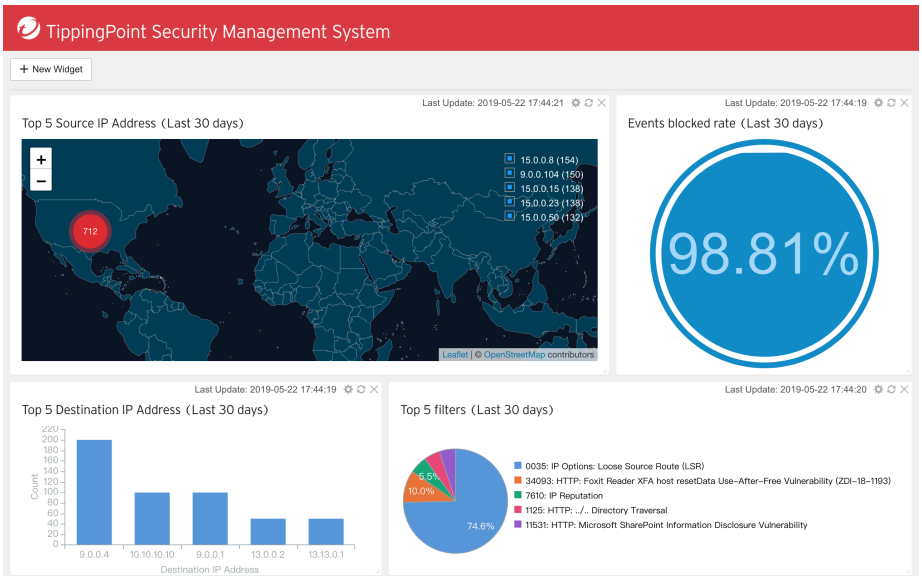
   If your password has expired, or if an administrator has set a forced password change, the Password Change Required dialog is displayed and you must enter your old password, a new password, and a confirmation.

To exit the SMS client, select **File** > **Logout**. The SMS client displays logout feedback information.

SMS Web Dashboard

You can use the SMS Web Dashboard to continuously display the information that is most important for mornitoring your network, such as the ability to monitor geographic locations of an attack on a map. The SMS Web Dashboard alerts you when there is an issue on your network. When you need to take action, you can drill down quickly to view the details of an alert.

The SMS Web Dashboard is configured with several widgets. You can customize the existing widgets or add additional widgets to display the information that you need to monitor. By default, the dashboard contains the following widgets: Top Attack Sources, Top Filters, and Events Blocked Rate.



To access this feature, open a supported browser (the most current version of Mozilla Firefox, Microsoft Edge, Apple Safari, or Google Chrome), and then enter `https://<SMS IP address or host name>/d/Dashboard`.

To refresh the widget, click the **Refresh** icon at the top of the widget. To edit a widget, click the **Gear** icon and then select parameters or visualization options. To remove the widget from the dashboard, click the **X** icon.

Create a new widget

You can create a widget by selecting a template or by using customized parameters.

Procedure

1. Open the SMS Web Dashboard.
2. Click **New Widget**.
3. Select a widget template, and then click **Next**.
4. Select whether to include the top three, top five, or top 10 data.
5. Select a filter from the **Aggregated Filters** drop-down list.

Aggregate Field	Name	Description
time_end	Event Time	Time at which the notification was logged and send to the SMS Web Management console.
src_ip_addr	Source IP Address	Source IP of the packet causing the notification.
src_port	Source Port Number	Source port of the packet.
dst_ip_addr	Destination IP Address	Destination IP of the packet.
dst_port	Destination Port Number	Destination port of the packet.
src_geography_id	Source Geography ID	Identifier for the geographic location of the source IP address.
src_country_code	Source Country Code	Country code for the geographic location of the source IP address.

Aggregate Field	Name	Description
src_country	Source Country	Country for the geographic location of the source IP address.
src_latitude	Source Latitude	Latitude for the geographic location of the source IP address.
src_longitude	Source Longitude	Longitude for the geographic location of the source IP address.
dst_geography_id	Destination Geography ID	Identifier for the geographic location of the destination IP address.
dst_country_code	Destination Country Code	Country code for the geographic location of the destination IP address.
dst_country	Destination Country	Country for the geographic location of the destination IP address.
dst_latitude	Destination Latitude	Latitude for the geographic location of the destination IP address.
dst_longitude	Destination Longitude	Longitude for the geographic location of the destination IP address.
signature_id	Signature ID	Identifier used to map this alert.
action_set_id	Action Set ID	Action set.
device_id	Device ID	Identifier for the device that sent the notification.
virtual_segment_id	Segment ID	Identifier for the device segment for the alert.
policy_id	Hit Count	Identifier used to map this alert.
severity_id	Severity ID	Severity ID of the event.
hit_count	Hit Count	Counter that displays the number of times the event triggered before the notification was sent to the SMS Web Management console.

Aggregate Field	Name	Description
xff_ip_addr	X-Forwarded-For IP Address	The X-Forwarded-For IP address. **Capture Additional Event Information** must be enabled on the profile.
tcip_ip_addr	True-Client-IP Address	The True-Client-IP address. **Capture Additional Event Information** must be enabled on the profile.
signature_name	Signature Name	Signature name.
action_set_name	Action Set Name	Name of the action set.
policy_name	Policy Name	Name of the policy for the event.
severity_name	Severity Name	Severity name.

6. If you select the **Events Blocked Rate** template, select field parameters from the drop-down lists.
7. Select the time used to aggregate data points over a specified time period.
8. Select a widget type.
9. Enter a name in the **Widget Title** field.
10. Click **Create**.

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: TPEM69835/230927