# Security Management System Release Notes

Version 4.6.0

Release date: May 2017

This document contains release-specific information for the TippingPoint Security Management System (SMS). The release notes describe new features and changes included in this release.

To ensure that you have the latest product documentation, go to the Threat Management Center (TMC) at *https://tmc.tippingpoint.com* or contact your TippingPoint representative.

This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint SMS appliances and associated devices.

This document contains the following important information:



## New and changed in this release

This release includes the following new features:

- *Renaming of deployment modes in the DV* on page 6

## SMS web management console

The SMS provides a new web-based interface in this release. The SMS web management console provides at-a-glance insight into your network security status with data that reflects the health, status, and security events for your system.

The SMS web management console enables you to install or upgrade SMS client software, monitor the TippingPoint devices installed on your network, and access Threat Insights.

You can review any available SMS system logs, exported and archived files, and saved reports.

You can access certain SMS web management console features from your mobile devices and tablets. For more information, see "SMS web management console" and "Desktop versus mobile experience – feature availability" in the *Security Management System User Guide*.

The SMS web management console provides a convenient way to:

- **Montior all devices** – View all devices, device groups, clusters, and stacks managed on the SMS.

  For more information, see "Monitor all devices" in the *Security Management System User Guide*.

- **Identify devices that require your attention** – Quickly identify devices that might have health or performance issues. Devices Requiring Attention on the web management console provides a list of managed devices that might have health or performance issues so that you can quickly identify and respond to device status.

  For more information, see "Identify devices that require your attention" in the *Security Management System User Guide*.

- **Switch a device into Layer-2 Fallback mode** – In the event of a server outage, or if you detect a system failure, you can also use the web management console to put a device into Layer-2 Fallback mode, monitor which devices are in Layer-2 Fallback mode, and take a device out of Layer-2 Fallback mode.

  For more information, see "Switch a device into Layer-2 Fallback mode" in the *Security Management System User Guide*.

## Threat Insights

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

Threat Insights include **Breached Hosts**, **Attacked Vulnerable Hosts**, **Suspicious Objects**, and **Zero Day Initiative (ZDI) Filter Hits**.

### Breached Hosts

Breached Hosts identify hosts in your network that might be compromised based on intelligence gathered from your Advanced Threat Protection (ATP) devices and your TippingPoint Intrusion Prevention System (IPS) and Threat Protection System (TPS) devices.

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

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

For more information, see "Breached Hosts" in the *Security Management System User Guide*.

### Attacked Vulnerable Hosts

Attacked Vulnerable Hosts identify vulnerabilities in your network. Third-party scans generate the vulnerability data, which you can import on the SMS. This enhanced visibility into your network allows you to highlight blocked or permitted attacks targeted to vulnerable assets.

You can use this information to make immediate updates to your security policy to protect your network. With the vulnerability insights provided by the Attacked Vulnerable Hosts, you can run updates on your assets.

For more information, see "Attacked Vulnerable Hosts" and "Enterprise Vulnerability Remediation (eVR)" in the *Security Management System User Guide*.

### Suspicious Objects

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

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

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

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

**Note:** You must have predefined tag categories configured in order for any data to be displayed for Suspicious Objects.

For more information, see "Suspicious Objects" in the *Security Management System User Guide*.

### ZDI Filter Hits

ZDI Filter Hits identify the number of blocked or permitted hits for pre-disclosed and disclosed filters.

The DV filter protection covers the time between when a vulnerability is discovered and when a software patch is made available. In addition, DV filters provide added protection for legacy, out-of-support software. The DV packages are delivered weekly, or immediately when critical vulnerabilities emerge, and can be deployed automatically.

ZDI Filter Hits include:

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

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

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

For more information, see "ZDI Filter Hits" and "Digital Vaccines" in the *Security Management System User Guide*.

## Predefined tag categories

In this release, the SMS incorporates predefined tag categories from ATP devices. You no longer need to manually create these tag categories when you augment your IPS deployment with your ATP devices.

The advanced threat intelligence provided in these categories keeps the Reputation database updated and enables robust reputation filters for enhanced protection of your system. The *Reputation database* is a collection of IP addresses and DNS names on an SMS that represents potential risks to network security. The entries in the Reputation database are used to create reputation filters that target specific network security needs.

Predefined tag categories include:

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

To configure this integration from your ATP device, refer to the ATP device documentation on the Trend Micro documentation site.

**After you upgrade to SMS v4.6.0**

- You can continue to use your user-defined tag categories for ATP integration provided you have not yet upgraded your Advanced Threat Protection for Networks device to version 3.85.1002 or later.
- After you upgrade your Advanced Threat Protection for Networks device to version 3.85.1002 or later, edit your existing profiles to add the reputation filters that use these new predefined tag categories.

For information on how to migrate reputation entries defined in previous SMS releases, contact support.

## URL Threat Analysis

URL Threat Analysis enables the SMS to automatically use the ATP Analyzer device. The ATP device analyzes suspicious content in HTTP traffic to detect malware threats to browsing clients in your network.

Configure URL Threat Analysis in the Event workspace to send inspection event URLs from the SMS to the ATP device. The ATP 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 in the SMS and indicate which event URLs might pose a threat. Based on the results, you can make security policy configuration adjustments, such as modifying profile action sets or creating a manual response to quarantine an infected host.

For more information, see "URL Threat Analysis" in the *Security Management System User Guide*.

## Configurable CVE ID field

A new configurable field option, CVE ID, is available when you create or edit a custom syslog format in the SMS. This field allows you to send CVE IDs to your remote syslog server.

To use this new setting:

1. In the SMS, navigate to **Admin** > **Server Properties**, and then click the **Syslog** tab.
2. Under **Syslog Formats**, create a new or edit an existing custom syslog format.
3. Click **Insert Field**.
4. Select `cveIds`.

For more information about custom syslog formats, see "Create or edit a custom syslog format" in the *Security Management System User Guide*.

**When you create a custom syslog format, note the following information:**

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 different custom fields can be parsed correctly by the receiving server.

**Note:** If necessary, adjust the settings for your syslog server so that it recognizes the defined escape character.

The following example shows a custom syslog format pattern:

```
${signatureName} ${_delimiter} ${actionType}
```

The following example shows another custom syslog format pattern that includes the CVE ID field with double-quotes (") used as escape characters. The double-quotes are manually inserted around the CVE ID field:

```
${signatureName} ${_delimiter} ${actionType} ${_delimiter} "${cveIds}"
```

## Automatic cleanup of unnamed, unused named resources

The SMS now performs scheduled, automatic cleanups of the following unnamed, unused named resources: IP addresses and IP address groups. Because the SMS sometimes creates multiple unnamed named IP addresses when performing various tasks, these objects could accumulate and affect SMS performance. This feature mitigates the impact of these auto-created objects by deleting resources that are no longer in use.

Cleanup happens automatically after you upgrade to SMS v4.6.0. It does not affect SMS functionality or your ability to create new named resources.

## Delete Reputation entries using the SMS web API

In this release, a new management API allows you to delete Reputation entries using a CSV file. For more information, see the *Security Management System External Interface Guide*.

## DV version for SMS v4.6.0

We recommend that you use DV 8952 or later packages in SMS v4.6.0. For more information, see "Digital Vaccines" in the *Security Management System User Guide*

## Renaming of deployment modes in the DV

In this release, note the following changes to the deployment modes:

- Two deployment modes were renamed to better reflect their intended usage.
- Three deployment modes were deprecated. These deployment modes will remain in the DV, marked as "Deprecated".

| Deployment mode | Description |
|---|---|
| Default | Provides a balance between high quality security and appliance performance and are suitable for most deployments. |

| Deployment mode | Description |
|---|---|
| Security-Optimized (previously named Aggressive) | Favors additional security over network performance or application adherence to protocol standards and is a subset of the Hyper-Aggressive deployment mode. Enables more Zero Day Initiative (ZDI) protection than other deployment modes. |
| Performance-Optimized (previously name Hyper-Aggressive) | Provides an ideal way to enforce an aggressive policy with filters designed to detect anomalies, application deviations, coding practices, and protocols.<br>**Note:** This deployment mode emphasizes network performance over security and is not recommended for use in a production environment. It 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. |
| Perimeter [Deprecated][1] | Offers optimal security for devices deployed on the perimeter of a network and protects the network from Internet traffic. |

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

# Installation

See the detailed installation instructions for your product on the TMC at *https://tmc.tippingpoint.com/*.

**Important:** You can upgrade the SMS client to v4.6.0 automatically from SMS v4.3.0 or later. However, if you upgrade directly to v4.6.0 from SMS v4.2.1 or earlier, you will need to download the client manually from the SMS web management console.

### Product version compatibility

The following table lists all compatible SMS versions with the TippingPoint Operating System (TOS) for TPS, vTPS, IPS, Next Generation Firewall (NGFW), and Identity Agent devices.

| | SMS v4.6.0 | SMS v4.5.0 | SMS v4.4.0 | SMS v4.3.0 | SMS v4.2.0 | SMS v4.1.0 |
|---|---|---|---|---|---|---|
| **TPS** | TOS v4.2.0 and earlier | TOS v4.2.0 and earlier | TOS v4.1.0 and earlier | TOS v4.0.0 | Not supported | Not supported |
| **vTPS** | TOS v4.2.0 | TOS v4.0.2 | TOS v4.0.2 | Not supported | Not supported | Not supported |
| **IPS** | TOS v3.9.2 and earlier | TOS v3.9.2 and earlier | TOS v3.8.4 and earlier | TOS v3.8.4 and earlier | TOS v3.8.4 and earlier | TOS v3.7.2 and earlier |
| **NGFW** | TOS v1.2.3 and earlier | TOS v1.2.3 and earlier | TOS v1.2.3 and earlier | TOS v1.2.3 and earlier | TOS v1.1.1 and earlier | TOS v1.1.1 and earlier |
| **Identity Agent** | v1.0.0 | v1.0.0 | v1.0.0 | v1.0.0 | v1.0.0 | Not supported |

### Software updates and migration

SMS and Virtual Security Management System (vSMS) upgrades are supported from v4.1.0. Install SMS v4.1.0 before you upgrade to SMS v4.6.0.

### Important information when you use Mac OS X to host an SMS client

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

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

If you cannot connect to the SMS using Mac OS X, you can choose to:

- Change the JRE temporarily on your local Mac OS X.
- Use a Windows SMS client to update the SMS to a 2K certificate key. You will no longer need to temporarily change to the JRE on your local Mac OS X.

**To change the JRE on your local Mac OS X**

1. Edit the `java.security` file located in the /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security directory.
2. Locate `jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024`, and then delete `MD5` from the line.

   The line should now be `jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024`.
3. Locate `jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768`, and then delete `MD5withRSA` from the line.

   The line should now be `jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768`.
4. Open the dmg (disk image) and run the installer application.

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

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

### SMS connecting to Identity Agent

In SMS v4.6.0, TLS v1.2 is enabled by default for SMS connecting to Devices/TMC/LDAP.

If the SMS has only a 1K certificate key (default), upgrade the SMS certificate key before you migrate to SMS v4.6.0. If you continue to use a 1K certificate key on the SMS, it will not be able to communicate with the Identity Agent.

If you choose not to upgrade the certificate key, you can disable TLS v1.2 after you upgrade to SMS v4.6.0. The SMS will be able to communicate with the Identity Agent again (117814).

### How to upgrade the SMS certificate key

To upgrade the SMS certificate key, log in to the SMS and under **Admin > General > SMS Certificate Key**, upgrade to a 2k certificate key.

For more information, see *SMS certificate key* in the *Security Management System User Guide*.

# Software updates and migration

An upgrade may require more time, depending on the quantity of data to migrate.

**Note:** The estimated times in the following table apply if you are upgrading from SMS v4.5.0. However, if you upgrade directly to v5.0.0 from SMS v4.4.0 Patch 1 or earlier, the upgrade will take more time. For more information on upgrading from releases prior to v4.4.0 Patch 1, refer to the release notes for those versions of your product on the TMC.

| Step | Task | Manual/automatic | Estimated time | SMS status |
|---|---|---|---|---|
| 1 | Download upgrade package. | Manual | Varies[1] | Available |
| 2 | Install upgrade package. | Manual | 2-10 minutes | Unavailable |
| 3 | Migrate data. | Automatic | Up to 4 hours[2] | Unavailable |
| 4 | Migrate report data. | Automatic | Up to 2 hours[3] | Available |

1) Network speed determines the time to download 800+ MB file.

2) Depends on the amount of event data to be migrated. The SMS automatically reboots after step 2 and is not available for logins until step 3 has completed. Do not reboot the SMS during this time.

3) The SMS is available while report data is being migrated, but performance may seem slow until migration completes. When this task is complete, a message appears in the SMS Audit Log.

# Known issues

The following known issues apply specifically to this release. For known issues found in previous releases, refer to the release notes for those versions of your product on the TMC.

## Devices

| Device | Description | Reference |
|---|---|---|
| SMS, SSL appliance | If the **SMS connecting to Devices/TMC/LDAP** panel of the TLS page has TLS v1.1 or v1.2 enabled, the SMS cannot manage an SSL appliance or communicate with it.<br>**Workaround**: To manage an SSL appliance and enable communication, do the following on the SMS:<br>1. Enable TLS v1.0 and disable TSL v1.1 and v1.2. Go to **Admin (Server Properties)** > **TLS** > **Edit**.<br>2. Manage the SSL appliance.<br>3. Enable TLS v1.1 or v1.2. | 117628 |
| SMS, TPS | To switch the HA (High Availability) state on a TPS device from the Device Configuration wizard, you must click the **Apply** button.<br>If you set the HA (High Availability) state and click **OK** without clicking **Apply**, the SMS will not save the HA configuration setting. | 117204 |
| SMS, IPS | Attempts of the SMS to remanage a device with TOS v3.9.0 or earlier fail with a `failed to discover device segments` error.<br>**Workaround**: Before attempting to remanage the device, use the device LSM to delete any unknown or special characters in the segment names, including spaces. | 116351 |

# Events

| Device | Description | Reference |
|---|---|---|
| SMS | We recommend that you keep the following default criteria when you create a saved inspection query for URL Threat Analysis:<br>• **Sort Direction** – Sort descending order by time<br>• **Show only the first matching rows** – 10,000 rows<br>• **Time** – Last 15 minutes<br>You can either update your existing saved query or create a new one if the query returns no matching results or if the URL Threat Analysis results are not what you intended. | 117889 |
| SMS, ATP device | For URL Threat Analysis, if a forwarded URL result indicates a failed communication with the SMS, check your ATP device. The SMS will eventually update any URL in the ATP device queue that is in the "unable to communicate" state. | 117747 |
| SMS, ATP device | For URL Threat Analysis, ensure that the IP address for your ATP device is valid in order to avoid a *urlForwarding is disabled* message on the SMS. This error message is displayed when you click on the XML report link after an invalid ATP device sends URL Analysis results. | 117519 |

# Profiles

| Device | Description | Reference |
|---|---|---|
| SMS, NGFW | Some customers noticed a failure of the SMS to distribute profiles to some of its managed NGFW appliances. This was because the configured number of user-defined services exceeded the limit of some of the lower-end NGFW models, which prevented the SMS from distributing profiles to those models. | 114518 |

| Device | Description | Reference |
|---|---|---|
| | **Workaround**: Configure the maximum user-defined services based on the minimum supported services limit for all managed NGFW models in your network. Reduce any duplicated or overlapping configured services used in the firewall rules.<br>The services limit per NGFW model are as follows:<br>• S1020F/S1050F: 256<br>• S3010F/S3020F: 512<br>• S8010F/S8020F: 1024 | |

# Threat Insights

| Device | Description | Reference |
|---|---|---|
| SMS | You cannot access the SMS web management console using a Google Chrome browser in private (incognito) mode on an iOS mobile device. | TPTIG-1032 |
| SMS | After you successfully switch a device cluster into Layer-2 Fallback mode, the Devices Requiring Attention panel on the SMS web management console does not reflect the updated status.<br>**Workaround**: Refresh the webpage to see the updated Layer-2 Fallback status for a device cluster. | TPTIG-1023 |
| SMS | You cannot download saved reports from a mobile device using Safari. | TPTIG-1012 |
| SMS | Pre-Disclosed 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. | TPTIG-968 |
| SMS | The count results for Suspicious Objects differ between the Threat Insights portal and the Suspicious Objects widget.<br>• **Threat Insights** – displays the count of Suspicious Objects hits. | TPTIG-944 |

| Device | Description | Reference |
|---|---|---|
| | • **Suspicious Objects widget** – displays the count of all Suspicious Objects. | |
| SMS | After you log in to the SMS web management console using an HTTPS connection in Google Chrome, you might not be able to log in again using an HTTP connection. | TPTIG-818 |

# Resolved issues

The following items, grouped by category, provide clarification or describe issues fixed in this release.

## Admin

| Device | Description | Reference |
|---|---|---|
| SMS, Identity Agent | Any cleanup of the **Historical IP User Mapping** table after retrieval of user-ID-to-user-IP correlation data by the Identity Agent generated a `DIM_IP_USER_MAPPING` error message.<br>You can now clean up the **Historical IP User Mapping** table on the SMS. | 116182 |
| SMS | The SMS did not automatically adjust to and from the daylight savings time (DST) for the following:<br>• **Report Schedules**: Scheduled reports on the SMS ran an hour off of the previously scheduled time.<br>• **Inspection Profile Distribution Schedule**: Inspection profile distributions were correctly adjusted to the DST change; however, the Schedule (on the Inspection Profile Distribution Schedule) displayed the previously scheduled time.<br>• **DV Distribution Schedule**: DV distributions were correctly adjusted to the DST change; however, the Schedule (on the DV Distribution Schedule) displayed the previously scheduled time.<br>The SMS now correctly adjusts the report schedules to the DST change and displays the correct time on the Inspection Profile Distribution Schedule and the DV Distribution Schedule. | 103320 |

| Device | Description | Reference |
|---|---|---|
| | Reports and distributions scheduled between a DST change (for example, 1:00 A.M. - 3:00 A.M.) might be off by an hour. If this is a concern, avoid this time range when you create a report schedule, an inspection profile distribution schedule, or a DV distribution schedule. | |
| SMS, vTPS, 440T | The SMS stopped sending all remote syslog events and stopped receiving packet capture (PCAP) files when the SMS received an IPS event from a TOS v4.0.1 device (vTPS or 440T). | 113370 |
| SMS | The SMS was updated to address security vulnerabilities: Sweet32 (CVE-2016-2183) and Dirty COW (CVE-2016-5195). | 115825, 115694 |
| SMS | After deploying a new vSMS in v4.5.0 or using a USB fresh install, it took five minutes before you could log in and start the OBE process. | 116578 |

## Devices

| Device | Description | Reference |
|---|---|---|
| SMS | After you changed the IPS hostname, the SMS Dashboard could take up to five minutes to update the **EventRate** widget with the new hostname.<br>The SMS dashboard now automatically updates the **EventRate** widget with the IPS hostname. | 98535 |
| SMS, IPS | Both the distribution thread pool and the concurrent device distributions have been increased to 30. | 116170 |
| SMS, IPS | An SMS managing an NX Series IPS device can now connect directly to the unit's system log when the user double-clicks the Syslog light on the device chassis image on the Devices page. | 114837 |
| SMS, IPS | A failure that prevented the SMS client from correctly registering and displaying the DNS Reputation TSE settings during IPS management or device refresh has been repaired. | 114908, 117212 |

| Device | Description | Reference |
|---|---|---|
| | The SMS client now correctly reflects the DNS Reputation TSE setting from the device. | |
| SMS, SSL appliance | TLS v1.2 is enabled by default in SMS v4.6.0.<br>Previously configured TLS settings will persist after you upgrade to SMS v4.6.0 in addition to TLS v1.2 being enabled. | 117571 |

## Profiles

| Device | Description | Reference |
|---|---|---|
| SMS | Renamed **Copy** to **Save As** in the **Edit** menu and the **Copy** dialog box.<br>To copy an inspection profile using the **Edit** menu, select the profile in the navigation pane, and then select **Edit** > **Save As**. | 97237 |
| SMS, NGFW | Attempts to import a firewall policy return an import failure error. | 114753 |

## Responder

| Device | Description | Reference |
|---|---|---|
| SMS, IPS | The automated SMS Quarantine Responder failed to propagate for an IPS during heavy Responder loads. | 116290 |

## Web API

| Device | Description | Reference |
|---|---|---|
| SMS | If you imported a reputation entry Web API that was not correctly formatted, a returned HTTP 404 response incorrectly indicated that the service was not found. | 113751 |

| Device | Description | Reference |
|---|---|---|
| | Verify that a reputation entry file is correctly formatted before you import it for use on the SMS. For more information, see "Reputation Management" in the *Security Management System External Interface Guide*. | |

# Product support

Information for you to contact product support is available on the TMC at *https://tmc.tippingpoint.com*.

## Legal and notice information



Edition: May 2017