Security Management System Release Notes

Version 5.0.0

Release date: October 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.

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

To ensure that you have the latest version of the release notes and other product documentation, download these documents from the Threat Management Center (TMC) at *https://tmc.tippingpoint.com*, or contact your TippingPoint representative.

This document contains the following important information:

New and changed in this release

This release includes the following new features.

Introduction of the TPS TX Series

SMS v5.0.0 includes support for management of TPS TX Series devices. The TPS TX Series is a powerful network security platform that offers comprehensive threat protection, performance scalability, and high availability.

For more information on TX Series, see the *Threat Protection System Release Notes* and the *Threat Protection System Hardware Specification and Installation Guide* on the TMC at *https://tmc.tippingpoint.com/*.

URL Reputation filtering

With URL Reputation filtering, you can achieve more granular Reputation controls in your security profiles than with Reputation filters based merely on domains or IP addresses. For example, instead of blocking everything at `www.mywebsite.com`, filtering can be configured to block only specific web pages like `www.mywebsite.com/malicious/stuff` but still allow access to `www.mywebsite.com/useful/information`.

You can configure URL Reputation filtering using the SMS. For more information, see the *SMS User Guide* and the *URL Reputation Filtering Deployment and Best Practices Guide* on the TMC at *https://tmc.tippingpoint.com/*.

Licensing

Beginning with v5.0.0, all licensing will be unbundled from the TPS hardware and issued electronically. Improvements and updates were also made to the Trend Micro TippingPoint License Manager.

The license manager, available from the TMC by navigating to **My Account** > **License Manager**, allows you to easily control the certificates and licenses that you purchase for your TPS products. This licensing model enables you to attach and detach TPS speed and feature licenses. For more information, see the *License Manager User Guide* available from the license manager on the TMC at *https://tmc.tippingpoint.com/*.

Additionally, licensing information for managed devices displayed in the SMS client is now in a new section called Licensing within the Admin workspace. For more information, see "Licensing" in the *SMS User Guide*.

Security system preferences

This release includes enhancements for the security levels, password preferences, and sessions on the SMS. For more information, see *System Preferences* in the *SMS User Guide*.

Security Levels

The SMS now includes four security levels. Options include the following:

Level	Description
0 - None	• User names cannot contain spaces. • Password length and complexity are not restricted. **Note:** Do not use spaces in the password.
1 - Low	Passwords must meet Level 0 (None) restrictions and the following: • User names must be at least six characters. • Passwords must be at least eight characters. • New password must be different from the previous password. **Note:** Do not use spaces in the 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 ! ? $ * #). **Note:** Do not use spaces in the password.
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. **Note:** Do not use spaces in the password.

Password preferences

This release includes the following password preferences:

- Require new password to be different from previous passwords.
- Show previous login details when a user logs in.
- Disable inactive user accounts.
- Require user to re-authenticate.
- Enforce a minimum password lifetime.

Total and user sessions

This release allows you to:

- Limit the number of active sessions allowed on the SMS.
- Limit the number of active sessions allowed for a user.

Named IP address groups for Traffic Management filters

This release includes enhanced support for named IP address groups for Traffic Management filters. For more information, see *Traffic Management filters* in the *SMS User Guide*.

Named Resources

Within the SMS, you can use named IP address groups to define single IPv4 or IPv6 addresses, groups of IPv4 or IPv6 addresses, or IPv4 or IPv6 subnets. For more information, see *Named Resources* in the *SMS User Guide*.

Important information after upgrading to SMS v5.0.0

After you upgrade to SMS v5.0.0, a new named IP address group is created for each Traffic Management filter that currently uses a named IP address block. You can consolidate IP address blocks used in a previous SMS version into a single group.

Named IP address group behaviors

Note the following distribution behaviors when importing, activating, or distributing a profile that contains named IP address groups for Traffic Management filters.

Profile import and activation

When you import or activate a profile on the SMS, the SMS verifies whether the named IP address group already exists.

- 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). The SMS assigns one IP address group for each imported IP address group.
- If the named IP address group does not exist on the SMS, the SMS adds it as an unnamed resource.

Profile distribution

The SMS maps IP addresses to Named Resources without involving the TPS and IPS devices to provide an improved user experience.

- 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 sends four filter exceptions to the device, and each exception contains a pair of source and destination IP addresses. You can view these combinations on the device Local Security Manager (LSM).

- When you distribute the IP address group to a device, the SMS only sends the IP address, not the name of the IP address group.

- 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.

  Note: Sending too many Traffic Management filters to the device can exceed the device maximum. To prevent this, ensure that the source or destination addresses has a value of **Any/Any IPv6**. For example, if you select the **IPv6** protocol, select **Any IPv6** for the source or destination addresses.

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.

SMS takes into account both the expanded Traffic Management filters and device resources. If the number of Traffic Management filters for a device exceeds the limit, the SMS prevents the profile distribution and displays a message.

Traffic Management filter limits are as follows:

- **Low-end device limit**: 5,000 filters. Low-end devices include S-Series devices.
- **Medium-end device limit**: 8,000 filters. Medium-end devices include N-Platform, NX-Platform, 440T, and vTPS devices.
- **High-end device limit**: 12,000 filters. High-end devices include 2200T and TX-Series devices.

TACACS+ remote authentication

A Terminal Access Controller Access-Control System Plus (TACACS+) server can now be configured for central authentication of TPS device users. TACACS+ authentication was previously supported for N-

Platform and NX-Platform IPS devices only. Because TACACS+ authenticates over TCP, it does not require transmission control the way RADIUS authentication does.

URL Threat Analysis

URL Threat Analysis reports generated from the Trend Micro Deep Discovery device are now available on the SMS. The **URL Threat Analyzer Results** table includes a link to the report in both HTML and PDF formats. The status must show `Complete` before the SMS displays a link to the report.

For more information, see "URL Threat Analyzer results" in the *SMS User Guide*.

sFlow® traffic sampling

TPS device administrators can now use sFlow® record emission to sample and analyze a random flow of traffic. This way, a baseline of typical application traffic can be established, and anomalous and malicious flows can be detected early. This feature cannot be enabled on vTPS devices.

TPS support for packet captures

You can now use the SMS to manually take a packet capture for TPS devices. For more information, see the *SMS User Guide*.

Inspection bypass enhancements

In addition to the default Bypass action, the following actions are available for inspection bypass:

- Block - Drops traffic.
- Ingress mirror - Sends a copy of the traffic to the mirror target Ethernet port prior to inspection.
- Egress mirror - Sends a copy of the traffic to the mirror target Ethernet port after inspection.
- Redirect - Interrupts the traffic and sends it to the target Ethernet port to prevent inspection.

Installation

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

Important: You can upgrade the SMS to v5.0.0 directly from SMS v4.3.0 or later. If you are running SMS versions older than 4.3.0, upgrade to v4.3.0 before upgrading to v5.0.0.

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 v5.0.0	SMS v4.6.0	SMS v4.5.0	SMS v4.4.0	SMS v4.3.0
TPS	TOS v5.0.0 and earlier	TOS v4.2.0 and earlier	TOS v4.2.0 and earlier	TOS v4.1.0 and earlier	TOS v4.0.0
vTPS	TOS v5.0.0 and earlier	TOS v4.2.0 and earlier	TOS v4.0.2	TOS v4.0.2	Not supported
IPS	TOS v3.9.2 and earlier	TOS v3.9.2 and earlier	TOS v3.9.2 and earlier	TOS v3.8.4 and earlier	TOS v3.8.4 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 v1.2.3 and earlier
Identity Agent	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0

Important: When you add a TPS or vTPS device, always distribute an inspection profile to all segments to begin protecting network traffic. By default, when you add a vTPS or TPS device, all filter categories are disabled in the Default security profile. When a TPS or vTPS device is unmanaged or deleted, there is no change in the filters.

Web certificates

If you are using your own web certificate (**Admin** > **General** > **SMS Web Security SSL Certificate**), the SMS might display a message (asking if you trust the certificate) after upgrading. Click **Yes** to trust the certificate to continue with the login.

Vulnerabilty scans (eVR) converters

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.

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.

End of support

SecBlade: S1200N SecBlade IPS support has ended as of June 30, 2017 (Ref. PB #1035). Future SMS releases beyond this date will not include support for management of this product. Because this is the only

product that uses the 2.5 version of the DV, future SMS releases will also remove support for using the 2.5 DV format.

E-Series IPS devices: Support for E-Series IPS devices and related TOS versions and related features specific to those models, such as Traffic Threshold Filters, ended in 2014 (Ref. PB# 1018). Future releases of the SMS beyond the date of this announcement will not support those IPS models and model specific features. These IPS devices and any associated configuration options might be removed in future SMS software upgrades.

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	30 minutes to one hour[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 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.

Admin

Device	Description	Reference
SMS	Active Directory users cannot log in to the SMS if their distinguished name or common name for the primary group has a comma.	120021

Devices

Device	Description	Reference
SMS	If the slot or port information for a device changes, you might need to manually refresh the device on the SMS to view the latest state. **Workaround:** To refresh the device on the SMS, go to **Devices** > **All Devices** > **[device name]**, and then click **Refresh**.	120438, 120439
SMS	The SMS displays `1000` Mbps as an available line speed for a device's copper ports when **Auto Negotiation** is disabled. The only valid value for a copper port that does not have **Auto Negotiation** enabled is `100` Mbps.	120437, 120428
SMS, 2200T	The SMS allows you to set the port for **Auto Negotiation** on a 1G fiber module for a managed device, but this is not supported. **Workaround:** Use the 2200T device LSM to enable or disable **Auto Negotiation** for a 1G fiber port. However, the LSM might incorrectly state that the **Auto Negotiation** is disabled on the LSM after you enable it (or refresh).	120433

Device	Description	Reference
SMS	If you edit a previously created inspection bypass rule on the segment reference device (SRD) without modifying any of the values, the following warning message appears: `Update Inspection Bypass Rules on device stack member failed`. This issue only occurs on TX Series devices that are in a stack. **Workaround:** Under these circumstances, this warning message can be safely ignored.	120305
SMS	Sometimes the SMS was unable to update the TOS across a stack of devices. **Workaround:** Delete the stack of devices, upgrade each device individually, and then create the stack again.	120263
SMS	For remote authentication, when you attempt to disable administrative login for an authentication server group, sometimes the following error message incorrectly displays: `Remote authentication group must contain at least one valid server`. **Workaround**: Open remote authentication and click **OK** without making any changes. Then you can properly enable or disable the administrative login when you open remote authentication.	120192
SMS	Under the following circumstances the SMS displays multiple "Please Setup SMS Certificate Password" dialog boxes, and as a result, will only successfully manage one device: • SMS is managing multiple TPS devices. • Each TPS device has a certificate with a private key. • The certificate has not been previously imported on the SMS. • A keystore password has not been set. **Workaround:** Enter and confirm your password in only one of the dialog boxes, and then remanage the failed TPS devices.	120187

Device	Description	Reference
	If you enter and confirm your password in multiple dialog boxes, delete every TPS device (even the successfully managed device) and then remanage every device. Alternatively, you can set the SMS certificate password before you manage the TPS devices (go to **Admin** > **Certificate Management** > **Setup Encryption**).	
SMS	The SMS is unable to update inspection bypass rules with VLAN ranges (1–30 to 1–50) for NX-Platform devices.	119836

Profiles

Device	Description	Reference
SMS	When you distribute a profile with Reputation filters to a vTPS device, and the default reputation filter settings have been updated to include the Reputation Enforcement option, the profile distribution might timeout. As a result, on a reboot of the vTPS (normal image), the device may enter the recovery console, where a factory reset is required to recover the device. On a timeout vTPS (normal and performance), the following error is created in the system log: `Install failed: Error installing IPDB package from TOS: Timeout` The Reputation Enforcement option, **Also apply filter actions to HTTP requests with matching DNS names**, is not supported on the vTPS. **Workaround:** To resolve this issue, disable DNS enforcement in the Reputation filter settings and then redistribute the inspection profile. To verify the reputation filter settings for an inspection profile, go to **Profiles** > **Inspection Profiles** > **[profile name]** > **Reputation/ Geo**, then click **Edit Settings**. Under Reputation Enforcement options, verify that the check box is not selected.	120395

Device	Description	Reference
SMS	After you activate and distribute an Auxiliary DV, the device information shows the newly distributed DV, but the distribution information does not display in the Auxiliary DV tables on the SMS. **Workaround:** Close and log back in to the SMS to correctly display the Auxiliary DV information on the SMS.	119731

Resolved issues

The following items provide clarification or describe issues fixed in this release.

MariaDB

The SMS now runs MariaDB 10.1.22. As a result, CVE-2016-6662 was resolved in SMS v5.0.0.

OpenJDK

The SMS upgraded the Open Java Development Kit (OpenJDK) from 1.8.0_102 to 1.8.0_141. As a result, multiple CVEs were resolved. For a complete list of CVEs, see the OpenJDK website.

Admin

Device	Description	Reference
SMS	The random access memory (RAM) displayed in the Admin section was higher than the actual RAM used. This was because buffered and cached data were unnecessarily factored in the calculations. The SMS now displays an accurate representation of RAM usage.	117254

Devices

Device	Description	Reference
SMS	The Adaptive Filter list sometimes appeared and disappeared unexpectedly when the list was refreshed. A message now displays on the SMS if an exception to this list refresh occurs.	119708
SMS, SSL appliance	If the **SMS connecting to Devices/TMC/LDAP** panel of the TLS page had TLS v1.1 or v1.2 enabled, the SMS could not manage an SSL appliance or communicate with it.	117628

Device	Description	Reference
SMS, TPS	You could only switch the HA (High Availability) state on a TPS device by clicking the **Apply** button. If you clicked **OK** without clicking **Apply**, the SMS would not save the HA configuration setting. The **OK** and **Apply** button can now both be used to switch the HA state on a TPS device.	117204

Events

Device	Description	Reference
SMS	Previously, we recommended that you include certain default criteria (i.e., sort descending order by time, show only first matching 10,000 rows, and last 15 minutes) when you created a saved query for URL Threat Analysis. This default criteria is no longer required for a URL Threat Analysis query.	117889
SMS	While using URL Threat Analysis, if a forwarded URL was in a `NonComm` state, there might have been an error on the Deep Discovery Analyzer.	117747
SMS	Multiple error messages displayed when the IP address of the Deep Discovery device for URL Threat Analysis was invalid. Only one error message now displays in the SMS client.	117519
SMS	The SMS was unable to retrieve packet traces from the device for a filter (10966: My SQL Failed Login Response) configured with a **Trace** action set. The SMS can now retrieve packet traces from the device for this filter.	117477

Profiles

Device	Description	Reference
SMS	The SMS was unable to retrieve saved searches or perform additional queries when the & special character was entered in the **Filter Name** field. The SMS can now retrieve saved searches and queries with this special character.	117782
SMS	When a system-defined service port was changed by the user, attempts to change it back to the default port would generate an error in the device System Log. Users can now switch back to the default port without errors.	116496
SMS	An SMS Client latency issue related to using the Real-time option with DNS lookups has been resolved.	115701

Web API

Device	Description	Reference
SMS	The Web API now validates user-provided IP Reputation entries when you import addresses to the SMS. Malformed IP-based entries are now rejected as they are imported.	117288

Product support

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

Legal and notice information

Edition: October 2017