Security Management System Release Notes

Version 4.5.0

Release date: December 2016

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 contains the following important information:

New and changed in this release

This release includes the following new or enhanced features:

Stacking

Stacking enables you to increase the overall inspection capacity of your TippingPoint Intrusion Prevention System (IPS) by grouping multiple NX Series devices and pooling their resources.

You can configure up to five NX Series devices in a stack. The stack operates as a single device that you manage on the SMS. Devices in the stack must be the same model, either all 7100NX devices or all 7500NX devices.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 7500NX added to a stack of 7500NX devices, the inspection capacity increases by 20 Gbps.

The following TippingPoint software is supported for stacking:

- TippingPoint SMS v4.5.0, or later - Centrally manages each stack of devices
- TippingPoint IPS v3.9.0, or later - Must be installed on each security device

Note: No additional licensing is required to implement stacking.

For complete information about stacking, see the *NX Series Stacking Deployment Guide* on the TMC.

Named IP address groups

Named IP address groups simplifies filter exception management on the SMS. This release includes enhanced support for named IP address groups for the following: filter exceptions, SSL inspection policies, Advanced DDoS filters, and quarantine exceptions (whitelist of IP address groups) and quarantine restrictions (blacklist of IP address groups). 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 about creating new IP address groups, adding items to an existing group, or moving items from one IP address group to another, see *Named Resources* in the *Security Management System User Guide*.

Important information after upgrading to SMS v4.5.0

After you upgrade to SMS v4.5.0, a new named IP address group is created for each filter exception 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 behaviors when importing, activating, or distributing a profile that contains named IP address groups (for filter exceptions, quarantine exceptions/restrictions, Advanced DDoS filters, or SSL inspection policies).

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 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). 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

IPS devices are not aware of Named Resources - the SMS maps IP addresses to Named Resources 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.

Profile distribution limit: The SMS restricts the number of all filter exceptions, including IP addresses, for all profiles to 65,536 exceptions per device. If you exceed this limit, you cannot distribute the profile. This limit promotes better performance for your system.

DV Toolkit filter number synchronization

In previous SMS versions, when you distributed a Digital Vaccine Toolkit (DV Toolkit) package to the device, the SMS assigned a new filter number, but the SMS did not synchronize it with the device or the original filter number from the DV Toolkit application. In addition, different devices might have had different numbers for the same DV Toolkit filter.

In SMS v4.5.0, 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), after you upgrade to SMS v4.5.0, 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, after you upgrade to SMS v4.5.0, the event still displays that number, not the new filter number.

- **Device LSM** (Filter Overrides) and **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 numbers assigned from the DV Toolkit application are included on the SMS

The SMS saves the filter number that was originally created from the DV Toolkit application. You can view this filter number on the SMS in the search results.

To view the DV Toolkit filter numbers in the search results, you must first set the visibility, as the DV Toolkit Filter # column is hidden by default. For more information, see *View DV Toolkit filter numbers in the Search Results* in the *Security Management System User Guide*.

Important information after upgrading to SMS v4.5.0

To properly maintain your security policy, perform a one-time DV Toolkit package reinstallation and profile redistribution. When you reinstall the DV Toolkit package, the SMS reassigns filter numbers to previously distributed DV Toolkit filters. When you distribute the profile back to the device, the SMS synchronizes the filter number with the device. For more information, see *Distribute a DV Toolkit package to the device* in the *Security Management System User Guide*.

Released, last modified, and ZDI disclosed dates for DV filters

SMS v4.5.0 includes support for the released, last modified, and Zero Day Initiative (ZDI) disclosed dates for Digital Vaccine (DV) filters and Auxiliary DV filters. You can view the date that indicates when the filter was released by TippingPoint Digital Vaccine Labs (DVLabs). When a filter gets updated, the SMS displays the date on which the filter was last modified. If available, you can also view the date a ZDI filter was publicly disclosed.

- **Profile and global search** - The released and last modified dates are searchable dates available on the SMS. You can quickly select the first date or the most recent date that a filter was released or last updated by TippingPoint. If you know the specific date, you can search for it by entering the date (MM/DD/YYYY). You can also select a DV or Auxiliary DV package using the calendar.
- **Search results** - After you search for a DV filter, you can view the released, last modified, and ZDI disclosed dates, if available, in the Search Results table.
- **Filter details** - When you select a DV filter, you can review the released and last modified dates on the filter details, and the ZDI disclosed date, if available.

Important information after upgrading to SMS v4.5.0

You must activate a new DV in SMS v4.5.0 before you can search for filters by released or last modified dates, or view the dates in the search results and filter details. For more information, see *Activate a DV, virtual DV, or Auxiliary DV package* in the *Security Management System User Guide*.

SMS High Availability (HA)

SMS HA provides the following enhancement in SMS v4.5.0.

Because a device can be managed by only one SMS, 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.

Depending on the TOS version running on the device, and if the original passive SMS server becomes the active SMS server when you disable HA, SMS v4.5.0 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.

For more information, see *Disable the SMS HA cluster* in the *Security Management System User Guide*.

SSL Inspection

SSL Inspection provides the following enhancements in SMS v4.5.0:

- New support for Perfect Forward Secrecy (PFS). SSL Inspection extends key exchange support to Ephemeral Elliptic Curve Diffie-Hellman with RSA signatures (ECDHE-RSA). ECDHE-RSA enables PFS support for inspection of encrypted SSL sessions. Prior to this release, SSL Inspection supported the RSA key exchange, which is the most common key exchange used for SSL today, but did not support PFS.
- The number of supported ciphers has increased from 6 to 14. The ciphers available depend on the TOS version running on the device. The **Profile Distribution Extended Status** on the SMS displays any compatibility errors with your selection and the device TOS version.
- Performance improvements significantly increase the maximum number of concurrent SSL sessions under inspection.
- Enhanced support for RSA AES cipher suites to now include SHA256.

Enterprise Vulnerability Remediation (eVR) converters

With Enterprise Vulnerability Remediation (eVR), you can pull in data from third-party vulnerability management vendors, match CVEs to DV filters, and take immediate action on your security policy, all within the SMS.

In SMS v4.5.0, the custom converter includes an additional converter for Tenable™ Nessus®. For more information, see *Enterprise Vulnerability Remediation* in the *Security Management System User Guide*.

You can also import Nessus vulnerability scan data using the eVR API. For more information, see the *Security Management System External Interface Guide*.

Vulnerabilities resolved in this release

The following Common Vulnerabilities and Exposures (CVEs) were resolved in SMS v4.5.0.

CVE-2016-6302	CVE-2016-6210	CVE-2016-4954
CVE-2016-6303	CVE-2016-2109	CVE-2016-4955
CVE-2016-6304	CVE-2016-2182	CVE-2016-4956
CVE-2016-6306	CVE-2016-5195	CVE-2016-4957
CVE-2007-2243		

The SMS upgraded the Open Java Development Kit (OpenJDK) from 1.8.0_60 to 1.8.0_102. As a result, multiple CVEs were resolved. For a complete list of CVEs, see OpenJDK.

Export a Tech Support Report from an IPS device

On SMS v4.5.0, you can collect diagnostic information from an IPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint Technical Support can use to debug and troubleshoot the device.

Unlike a TSR created on the device LSM, the TSR exported from the SMS does not include snapshot information. However, you can create a snapshot on the SMS.

Note: In this release, you can export a TSR only from an IPS device, not a TPS device.

Enhanced support for TPS devices

SMS v4.5.0 includes the following enhancements for TPS devices (the SMS already supports these features on IPS devices):

- **X-Forwarded For and True client IP support** - Identify a request's source IP address without having to refer to proxy logs or Web server logs.

- **Capture additional event information** - Capture the URI metadata and hostname for an event.

Installation

For installation instructions, refer to the *Install your appliance* documents located on the TMC.

Important: You can upgrade the SMS client automatically from SMS v4.3.0 or later to v4.5.0. However, if you upgrade directly from SMS v4.2.1 or earlier to SMS v4.5.0, you will need to download the client manually from the SMS Web Interface.

Product version compatibility

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

	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 v4.1.0 and earlier	TOS v4.0.0	Not supported	Not supported
vTPS	TOS v4.0.2	TOS v4.0.2	Not supported	Not supported	Not supported
IPS	TOS v3.9.0 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 v1.1.1 and earlier	TOS v1.1.1 and earlier
Identity Agent	v1.0.0	v1.0.0	v1.0.0	v1.0.0	Not supported

Software updates and migration

SMS and vSMS upgrades are supported from v4.1.0. We recommend that you are running at least SMS v4.1.0 before you upgrade to SMS v4.5.0.

Important information when using a 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 v4.5.0 client will not be able to connect to an SMS that is still running with a 1k certificate key (113450).

To avoid this issue, upgrade the SMS from a 1k certificate key to a 2k key. If you cannot connect to the SMS using Mac OS X, you have two options:

1. Temporarily make the following changes to the JRE on your local Mac OS X. - OR -
2. Use a Windows SMS client to update the SMS to a 2K certificate key. After you do this, you will no longer need to temporarily change to the JRE on your local Mac OS X.

How 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.

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

Resolved issues

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

Admin

Device	Description	Reference
SMS	Named Resource tables did not correctly filter on unnamed resources.	113517
SMS	After a backup was restored, the status continued to show that the backup was in progress.	104680
SMS	A user was unable to establish an HA connection. Existing encrypted remote syslog entries no longer fail when you configure SMS HA.	104788
SMS	When you imported new geographic packages, the SMS did not remove older files. This caused space on the SMS to fill up. Now you can only load one geographic package at a time on the SMS.	113388
SMS	The Apache Commons library was updated to address security vulnerabilities.	112572
SMS	The `health.raid` SMS CLI command now returns the RAID controller status on the `SMS H3` and `SMS H3 XL` platforms.	113274

Devices

Device	Description	Reference
SMS	The VLAN ID range on the SMS and on the device LSM were not consistent.	108142

Device	Description	Reference
SMS	The SMS did not correctly display the distribution progress of a new DV.	112423
SMS	The check box to disable the Quarantine Automatically setting in the SMS now works.	112452
SMS	The SNMP and Authentication Preferences preview panels was not available to view in the Import Device Configuration Summary preview page before the configuration import settings were applied.	112520
SMS	If you managed a device with an SMS that did not have a certificate password, and you closed or canceled the Adding Device dialog, an appeared error when you tried to re-add the device that stated that the device already existed in the SMS. This error continued until the adding device process completed. This error no longer appears.	112590
IPS	When a virtual segment was reordered on the SMS, the following message sometimes appeared in the audit log for both affected and non-affected devices: `Update device virtual segment positions for devices <device name>` These messages no longer appear.	112598
SMS	When you downloaded packet traces from multiple devices, expired packet traces from one device might have impacted the download from other devices.	114053
SMS	On SMS v4.3.0 and older, you could select a specific port on the event filtering criteria under **Device** > **Segment** > **Rule Criteria**. However, on SMS v4.4.0, you could only select the entire segment group instead of the specific segments. This functionality was corrected in SMS v4.5.0 to be the same as it was in v4.3.0 and older.	114062

Device	Description	Reference
SMS, TPS	Network port settings reported by SMS for TPS devices were sometimes inconsistent. The Ports page is now consistent with the device.	113663
SMS, TPS	Tier 1 Stats did not show the max values. The following Tier Stat updates were made: • Added max values to TPS Tier Stats • Formatting issues on NX Tier Stats were corrected • Added `min ratio to next tier` values for TPS	113868
NGFW, vTPS	When you upgraded to the 2K key on the SMS, the SMS Certificate Key Upgrade Wizard showed that the device was incompatible. This only occurred on NGFW v1.2.2 and vTPS v4.0.1.	112773, 112842

DV Toolkit

Device	Description	Reference
SMS	When DV Toolkit Packages were overridden and distributed to the device, the filter names in the DV Toolkit package on the device were different from the filter names that displayed on the SMS.	105570

Events

Device	Description	Reference
SMS	On SMS v4.3.0 and older, you could select a specific port on the event filtering criteria under **Device** > **Segment** > **Rule Criteria**. However, on SMS v4.4.0, you could only select the entire segment group instead of the specific segments. This functionality was corrected in SMS v4.5.0 to be the same as it was in SMS v4.3.0.	114062

Reports

Device	Description	Reference
SMS	Matching filter information was missing from **Specific Reputation Events** report.	107109

Profiles

Device	Description	Reference
SMS	A timeout error occurred when several profiles were compared at the same time.	112607
SMS	When you attempted to modify an inherited SSL inspection policy, the policy was no longer visible, but if you logged off and logged back into the SMS, the policy reappeared in the child profile. Changing the parent policy no longer changed the state of the child policy, but the SSL server validation of the parent profile still took into account the state of the SSL server of the child policy, which sometimes caused the SSL server validation to fail.	113117
SMS	Long-running event queries prevented DV, Auxiliary DV, and DV Toolkit activations from succeeding. Date information was added for filters to prevent this.	113511
SMS	During a profile import, the SMS did not include additional custom alert information, like email notifications, for modified filters. This caused the custom profile import to fail. Additional alert elements are now included in the import.	113630
SMS	The default timeout value of the Profile Change History in the Database Maintenance table was too small. The default value was changed from 30 days to 365 days.	108397

Responder

Device	Description	Reference
SMS	Cached active responses caused memory usage to increase and SMS functionality to slow down.	55096
SMS	Quarantine event names displayed as `<unknown> (The active DV on the SMS may be out of date)` in the Events view. The quarantine event name now displays as `Active Response XXX`, where `XXX` represents the active response ID number.	109174

Web API

Device	Description	Reference
SMS	When a web service logon failed because of invalid credentials, the HTTP response sent back a `200` response, which incorrectly indicated a successful logon. The HTTP response now sends back a `401 Not Authorized` response.	113433

Known issues

This release contains the following known issues.

Admin

Device	Description	Reference
SMS	When you upgrade or restore a backup from a release prior to version 4.5.0 while the SMS is in FIPS Crypto Core mode, the SMS web certificate does not migrate correctly into the SMS certificate repository. The private key is not migrated, and the certificate appears as "broken". This does not cause any issues with the SMS client. However, you cannot use the certificate until you import the private key back onto the SMS certificate repository by using the "repair" option on the certificate.	114510
SMS	After you click **Export and Archives** in a web browser, the following message appears in the SMS audit log each time you manage or delete a device: `Attempt to get a user group with id: SMS_EXPORT_ARCHIVE failed`. This may also occur when you import or delete DV Toolkit packages. **Workaround**: These messages do not affect functionality and can be ignored.	112837
SMS	Common Access Card (CAC) authentication is not supported on Windows 10.	116001
SMS	If you check the usages of multiple certificates on the SMS (**Admin** > **Certificate Management** > **Certificates** or **CA Certificates**), non-specific device certificate usages might not display if any of the certificates are used on the SMS (i.e., RADIUS, Web, etc.). **Note:** This does not affect certificates that have device usage, such as User Authentication or VPN.	111547

Device	Description	Reference
	Workaround: Check the usages of the individual certificates on the SMS.	
SMS	You can import any valid ZIP file to the Geo Locator Database. After you import the file, the SMS audit log does not reflect the number of entries, and the entries do not appear on the SMS. **Workaround:** Only Import the GeoLite City - CSV/ZIP file format from MaxMind, and then check the SMS audit log to verify that the SMS imported the correct package.	116581
SMS, IPS	After you restore a backup on the SMS, the TLS settings display all of the **SMS connecting to Device/TMC/LDAP** options as enabled, instead of each setting in the backup.	111789

Devices

Device	Description	Reference
SMS	When you create virtual segments, warning messages display in the **Validation Report** tab. However, the tab still displays green, even when there are warning messages. **Workaround**: Before you save a new virtual segment, check the **Validation Report** tab for warning messages.	108083
SMS	When you attempt distribute an Inspection profile that contains an invalid SSL policy or SSL server name to a user-defined virtual segment, the distribution fails. **Note:** The only valid characters are spaces, alphanumeric, and the following special characters: -, _, &, <, >, (,)	112724
SMS, TPS	If the master-key for the TPS device is set with a device-specific key instead of a passphrase, the SMS does not show the system master-key information under **Device Configuration** > **Log Configuration**. As a result, you cannot edit the configuration.	111321

Device	Description	Reference
	Workaround: Do not use a device-generated key instead of a system master key to manage a device on the SMS.	
SMS, TPS	The SMS does not clearly indicate that you cannot delete a user role because it is assigned to a user group. **Workaround**: Remove the user role from the user group that references it, and then delete the user role.	111985
SMS, TPS	If a device was previously managed on the SMS using TLSv1.1 or higher, and was then changed to use TLSv1.0 only, the SMS is not able to manage the device. **Workaround**: To be able to manage the device again, change the TLS setting back to v1.1 or higher, restart the SMS, or allow the 24-hour connection timeout to occur. To avoid this issue, use the device LSM to change the TLS configuration to TLSv1.0 when TLSv1.1 or higher was previously set.	112536
SMS, vTPS	The NGFW mode in vTPS does not support Jumbo frames, and the MTU value cannot be set higher than 1500. The MTU value is fixed and cannot be modified.	112230
SMS, vTPS	The SMS does not distribute a reputation filter to the vTPS. **Workaround**: Perform a full synchronization of the Reputation database within the SMS. Select **Profiles** > **Reputation Database** > **Edit** > **Full Sync**.	112589
SMS, 2200T	If two or more different SSL policies are using two different SSL servers and running the same certificate, when you distribute a profile that deletes these SSL policies, the SMS: • Distributes the profile. • Displays an error on the distribution dialog. • Logs a message in the SMS syslog **Workaround**: Delete each SSL policy separately, and distribute the policy to the device before you delete the next policy.	113249

Device	Description	Reference
SMS, IPS, NGFW	Device LSM users cannot be forcibly logged out from the SMS. **Workaround**: Device LSM users are automatically logged out after a period of idleness (15 minutes) and when managed by the SMS, an LSM user has a read-only view that cannot modify the device configuration.	101042
SMS, NGFW	When you configure PPP interfaces (PPTP, PPPoE, L2TP), you cannot remove the password without removing the user. **Workaround**: To remove the password, remove the user ID.	104416
SMS, NGFW	You can create a device user group with a role of "none." This role has no capabilities.	105107
vTPS, TPS	The Device SLG page does not correctly display the state of Performance Protection mode.	113132
SMS, IPS	When you disable auto-negotiation on an N-Series Intrusion Prevention System (IPS), an invalid parameter error occurs. **Workaround**: Do not disable auto-negotiation on the management or data ports of an N-Series IPS device.	115784
SMS, IPS	The SMS times out when you try view a large Traffic Capture file using the Internal Packet Trace Viewer. (All Devices > Member Summary > Traffic Capture > Existing Captures > View). **Workaround**: To view a large traffic capture file (which is combination of Maximum Packets and Maximum File Size), select one of the following from the SMS: • Application registered with the .pcap file association • Define and use an external packet capture viewer Alternatively, you can decrease the limits on the SMS for the Maximum Packets and Maximum File Size allowed.	104884
SMS, Stack	After you perform a TOS upgrade on a stack, the Sync Health might display the profile as 'unknown' on some of the stack member devices.	116472

Device	Description	Reference
	Workaround: When you perform a TOS upgrade on a stack, you must re-distribute the profile to the stack.	

DV Toolkit

Device	Description	Reference
SMS	When you distribute a DV Toolkit package, the device system log shows a different package ID than is shown on the SMS system log. **Workaround**: The device system log reflects the merged packet ID. This discrepancy can be ignored because there is no functional impact.	106097
SMS	When you distribute a DV Toolkit package, the SMS successfully distributes the package, but the distribution queue for the device does not display the distribution type, and the **Package** field is blank.	116590
SMS	If a user with SuperUser capabilities deactivates a DV Toolkit package on a shared profile, and then a user with Admin capabilities deletes that profile, the SMS displays a `UserNotAuthorized` error. **Workaround**: If a profile is shared among users with different capabilities, a SuperUser should delete the profile.	106231
SMS	When you use the **Overwrite** option while you activate a DV Toolkit package, the SMS displays the installed devices of the previously active DV Toolkit instead of the devices for the new DV Toolkit. **Workaround**: Distribute the current, active package.	108137
SMS, NGFW	A version error and exception may display when you distribute the same DV Toolkit package to the firewalls in the cluster. **Workaround**: Uninstall the DV Toolkit packages from the firewall appliances, and then click **Sync Configuration Now**.	105136

Events

Device	Description	Reference
SMS	You cannot save an IPS event query when the firewall profile is included in the query.	105963
SMS, TPS	Instead of displaying the segment name, the interface grid under **Events** > **SSL sessions** appears as ethernetX.	113102
SMS, TPS	When you assign an SSL inspection profile to a segment, if the SSL inspection profile is assigned to only one of the ports on the segment (such as A > B), and a non-SSL inspection profile is assigned to the other port (such as A < B), inspection events on SSL traffic incorrectly indicate the non-SSL inspection profile is associated with the filter hit. **Workaround:** Assign the same SSL inspection profile to both ports (A > B and A < B) of the segment. SSL inspection profiles do not support policy in a single direction	116485
SMS, IPS	URI metadata might not be available for some event listings because the device sends URI metadata in two separate logs.	101575
SMS, IPS	When you distribute a profile with a **Permit + Notify + Trace** or a **Block + Notify + Trace** action set, the SMS notifies the management console in the form of an event listing and logs all information about the packet according to the trace settings, but you cannot capture the packet from the event. **Workaround**: To capture the packet for that event listing, you must create a new Traffic Capture file. Select **Devices** > **Member Summary** > **Traffic Capture** > **New** > and then specify the **Segment** where the event occurred.	116266

Profiles

Device	Description	Reference
SMS	When you uninstall an Auxiliary DV package, the SMS removes the package from the device, but an alert appears on the DV Inventory to indicate that the uninstall has failed. **Workaround**: Log out, and then log back on. The DV Inventory shows that the Auxiliary DV package is removed from all devices.	105246
SMS	When the SMS is unable to complete an DV package refresh, the SMS appears to indicate that more than one DV package is active. **Workaround**: To resolve the refresh issue, log out, and then log back on. The SMS shows only one active DV package.	105344
SMS	If a user with Admin capabilities uses a 'Save As' option to copy a profile, the Admin user cannot access the profile until a user with SuperUser capabilities gives the Admin user access to the profile. **Workaround**: A SuperUser can give the Admin user access to the copied profile. Alternatively, the Admin user can export the copied profile and them import it.	106325
SMS	When export or import a profile from one SMS to another SMS, and when either or both of them are in FIPS mode, the selected SMS become unavailable, and the export/import fails. **Workaround**: Export the profile to a local file, and then import it onto the SMS.	106570
SMS	When you import a profile from a device segment group, the version number of the active profile might not match the version number on the Profile Details. **Workaround**: Log off the SMS. When you log back on, the correct profile version displays.	108034
SMS	The system log sometimes displays a foreign key-constraint error when you activate an Auxiliary DV package.	108055

Device	Description	Reference
	Workaround: This error message can be safely ignored.	
SMS	When a profile is distributed using a schedule, the version of the profile displays "null" or is missing in the audit log. **Workaround**: Distribute the profile on demand.	112217
SMS	When you remove a single list value from a tag category, the SMS removes the tags from the user-entry categories that use that tag. **Workaround**: Export the user entries from the SMS, edit them, and then re-import them on the SMS. Alternatively, you can also make a new tag category with the list values.	113302
SMS	After you import an SSL policy that is disabled, the SMS automatically enables the SSL policy. **Workaround**: After you import a disabled SSL policy, disable it again.	113240
SMS	When you export a 'parent' profile, and then import the same profile as a 'child' profile, the SMS displays the correct settings for the 'child' profile. However, if you edit any of the filter overrides, the SMS reverts the settings back to the 'parent' profile settings.	115943
SMS	If you do not enable certificate management, when you export a SSL inspection policy, the SMS displays an error and the receiving SMS imports the profile without the SSL inspection policy. **Workaround**: Enable certificate management on the SMS in which you will import the profile (with the SSL inspection policy), and then import the profile. If you export the profile without first enabling certificate management on the receiving SMS, cancel the export from the SMS and do not distribute the profile.	114919
SMS	The reputation database full-synchronization displays a sync as "in queue", and does not update. **Workaround**: To verify the actual progress, select **Reputation Database** > **Activity** > **Sync Progrss**.	108870

Device	Description	Reference
SMS, 2200T	When you rollback a TOS while simultaneously distributing a profile, subsequent profile distributions might fail, unless you perform a filter reset. **Workaround**: Do not distribute a profile while a TOS rollback is in progress.	116484
SMS, IPS	When you delete an SSL policy on the SMS, the SSL profile and server are deleted, but sometimes the certificate is not deleted. **Workaround**: Delete the certificate by using the device LSM.	108971
SMS, NGFW	When you import a policy with a firewall rule that contains a user-defined service, the import fails and displays an error message.	116267

Reports

Device	Description	Reference
SMS	When you generate an executive report, the event query displays an inaccurate query structure.	103620
SMS	When you generate any of the following reports, and click a link in the report, you cannot use the **Refresh** button on the Events panel until you restart the SMS client: • Inspection report with county criteria • Specific Country (Inspection Security report) • Specific Country (Inspection Application report)	106322
SMS	The DDoS report might display a higher value for SYNs rejected for the last 7 days and the first 24 hours.	115671
SMS, Stack	When you generate the IPS Physical Port report, and select a stack name from the Device or Segment criteria, the report displays "All" instead of the selected stack name.	115712

Device	Description	Reference
SMS, IPS	When you generate a Rate Limit report, the date for some devices does not display.	115799

Web API

Device	Description	Reference
SMS	A user can export and distribute a profile to a device or segment without the proper access to those profiles, devices, or segments.	108052
SMS	When you run a position update on a virtual segment with a number that exceeds the number of segments on the list, an `Unexpected Error Occurred` message is returned.	108182
SMS	When there are duplicate VLAN IDs in an XML file and you use the Web API virtual segment Create command, an unexpected error occurs. **Workaround**: Do not duplicate VLAN IDs in the XML file when you create virtual segments.	108184
SMS	The SMS audit log does not display the profile name when you distribute a profile using the API.	108197
SMS	An error message is returned if virtual segments with the same name are sent to a device.	108267
SMS	If you use the API to import a reputation entry (with errors), an HTTP 404 response is returned which incorrectly indicates that the service was not found. **Workaround**: 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 Interfaces Guide*.	113751

vSMS

Device	Description	Reference
vSMS	When deploying a new vSMS, it might take up to five minutes before the OBE process starts.	116578

Product support

Get support for your product by using any of the following options:

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

Legal and notice information

Security Management System Release Notes

Edition: December 2016

Publication Part Number: B09152011