Security Management System Release Notes

Version 4.4.0

Release date: July 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. 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:

- *Virtual Threat Protection System* on page 2
- *Threat Protection System - 2200T device* on page 2
- *Certificate management* on page 2
- *SSL Inspection for 2200T devices* on page 2
- *TippingPoint license package enhancements* on page 3
- *TLS settings* on page 3

- *SMS certificate key* on page 3
- *SMTP server settings - email aggregation* on page 4
- *High Availability (HA) configurable timeout values* on page 5
- *Common Access Card (CAC) authentication* on page 5

Virtual Threat Protection System

The Virtual Threat Protection System (vTPS) is a software device designed to provide the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

The TOS 4.0.1 version of the vTPS supports the majority of features that were introduced with the 4.0.0 release of the 440T TPS device.

For additional information on the vTPS device, refer to the TMC.

Threat Protection System - 2200T device

The 2200T device delivers the highest level of defense against network intrusion and provides application control. The 2200T device includes:

- Threat Suppression Engine (TSE) which scans, detects, and responds to network traffic according to the filters, action sets, and global settings maintained on each device
- Built-in intrinsic High Availability (HA) features, guaranteeing continuity in the event of system failure
- Up to 2Gbps aggregate across all ten segments
- Device management through the Local Security Manager (LSM) or centralized management through the SMS

For additional information on the 2200T device, refer to the TMC.

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.

SSL Inspection for 2200T devices

The TippingPoint Threat Protection System (TPS) 2200T provides in-line, real-time threat protection for inbound SSL traffic. The 2200T manages its own private keys and certificates from the servers it is securing;

these can either be stored on the device itself or accessed at run-time from the Security Management System (SMS).

TippingPoint license package enhancements

The TippingPoint license package contains customer information about the status and the availability of TippingPoint products and services for licensed devices. SMS version 4.4.0 now supports Throughput and SSL Inspection licenses.

TPS devices running TOS v4.1.0 support higher throughput licenses. 2200T TPS devices support SSL inspection capabilities and higher throughput license.

You can use the TMC to update the license package and assign an SSL Inspection or Throughput Upgrade license to a 440T or 2200T device.

If you purchased an SSL Inspection or Throughput Upgrade license when you ordered the device, you must also update the license package and assign the license to the device. You are not required to assign the license that you purchased with the device to that device.

SSL Inspection and Throughput Upgrades are licensed separately. To request a license, contact your sales representative.

TLS settings

You can define and manage which TLS versions (v1.0, v1.1, and v1.2) will be enabled for the various SMS communication channels.

SMS certificate key

The SMS 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 1K key (1024 bits). We recommend that you upgrade this certificate with the 2K (2048 bits) version, which also uses stronger hashing functions. The upgraded 2K key certificate will have the same serial number as the one it replaces. If SMS is currently running a 1K key, it will display a message about upgrading to a 2K key.

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 4.4.0 client will not be able to connect to an SMS that is still running with a 1k certificate key. To avoid this issue, you must 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 *SMS User Guide*.

Review the SMS certificate key compatibility matrix for your device.

SMTP server settings - email aggregation

Alert aggregation allows you to receive alert notifications at intervals to prevent an overload of the mechanism that sends the notifications.

The **Edit SMTP Server Settings** has been updated with a new field, **Aggregation Period**. You can set the 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.

High Availability (HA) configurable timeout values

When configuring a SMS HA cluster, you can specify the parameters that the SMS 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 already 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 already 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.

Common Access Card (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 offers:

- Interoperability with ActivClient software and Windows compatible smart card readers
- Support for government-issued Common Access Cards (CAC)
- Compatibility with major certificate authorities using PIN-protected Public Key Infrastructure (PKI) certificates

Installation

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

Important: You can upgrade the client automatically from SMS version 4.3.0 to version 4.4.0. However, if you upgrade directly from version 4.2.1 or earlier to version 4.4.0, you will need to download the client manually from the SMS Web Interface.

Important: When you upgrade or restore a backup from a release prior to version 4.4.0 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 web server. Client connections will still be allowed. However, this web certificate cannot be used again until the private key is imported into the SMS certificate repository using the "repair" option on the certificate. (111741)

Product version compatibility

The following table lists all compatible versions of the vTPS, TPS, IPS, NGFW, and Identity Agent devices with different SMS versions.

	SMS v4.4.0	SMS v4.3.0	SMS v4.2.0	SMS v4.1.0
vTPS	TOS v4.0.1	Not supported	Not supported	Not supported
TPS	TOS v4.1 and earlier	TOS v4.0.0	Not supported	Not supported
IPS	TOS v3.8.x and earlier	TOS v3.8.x and earlier	TOS v3.8.x and earlier	TOS v3.7.x and earlier
NGFW	TOS v1.2.2 and earlier	TOS v1.2.2 and earlier	TOS v1.1.1 and earlier	TOS v1.1 and earlier
Identity Agent	v1.0.0	v1.0.0	v1.0.0	Not supported

Software updates and migration

SMS and vSMS upgrades are supported from version 4.1.0. We recommend that you are running at least SMS version 4.1.0 before you upgrade to SMS version 4.4.0.

You must allow background processes to complete before you begin migration to SMS version 4.4.0.

Resolved issues

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

Admin

Device	Description	Reference
SMS	If you imported an SMS Web Security SSL Certificate and then imported a RADIUS certificate without restarting the SMS while the SMS was in FIPS Crypto Core mode, the SMS would display a `NullPointerException` error message.	101767

Device	Description	Reference
SMS	If you imported a SMS Web Security SSL Certificate while the SMS was in FIPS Crypto Core mode, the following certificate information was not updated until the SMS was restarted: • Subject DN • Valid After • Expires	101302

Devices

Device	Description	Reference
SMS	If you created or updated a virtual segment in a device task and one of the devices was unmanaged, then an exception error sometimes occurred.	108269
SMS, TPS	If you unmanaged the device and then edited a user role in the Local Security Manager (LSM), the role capabilities did not display in the SMS when you remanaged the device.	104684

DV Toolkit

Device	Description	Reference
SMS	When you distributed a DV Toolkit package to all devices, the package appeared inactive on the DV Toolkit Details screen.	105480
SMS	After you imported a new DV Toolkit package (with the **Activate the imported DV Toolkit package** check box selected to overwrite an existing, active filter package), the Device Summary screen did not display the name of the new DV Toolkit package.	105789

Device	Description	Reference
SMS	The DV Toolkit package displayed `unknown` on the DV Toolkit Distribute dialog box when you distributed a different DV Toolkit package to the device. `Unknown` displayed because you did not have access to that package.	105846
SMS	Sometimes you had to uninstall the DV Toolkit package twice for the package to be uninstalled.	105891
SMS	Sometimes if you had several individual DV Toolkit distributions happening to the same device at the same time on the SMS, some DV Toolkit packages might not have distributed to the device. When this happened, the Distribution Extended status did not list the DV Toolkit package that was not distributed to the device. This situation sometimes also happened if you uninstalled multiple DV Toolkit packages from the same device.	106058, 106350, 105492
SMS	When you distributed a DV Toolkit package that had several filter overrides, an `isValid: Signature` message displayed in the device log if there were differences between the profile and DV Toolkit package.	106236
NGFW	When you distributed a firewall profile to an NGFW appliance, a mismatch warning sometimes displayed even though the SMS and NGFW appliance had the same DV Toolkit package.	104445

Profiles

Device	Description	Reference
SMS	When you imported a profile from a device that had nonstandard service ports, the SMS updated inspection services for each profile and changed the version and modified dates for all the profiles on the SMS.	105964
SMS	When you imported an existing profile name, it was invalid if it had the same name as another profile but used a different case. However, a warning conflict did not appear to let you know that the name was	108260

Device	Description	Reference
	invalid before you imported the profile. Instead, the following error message appeared: `The Profile could not be imported. An unexpected error occurred while trying to import the profile.`	
SMS	Profile distribution sometimes caused certain filter overrides on other segments of the same device to revert to category settings.	108783
SMS	Bulk edit of multiple filter settings are now logged in detail (similar to how they were logged in SMS version 4.2.0 and earlier). In this release, the SMS lists each filter change instead of a single summarized message ("bulk update of x filters").	108617
NGFW	After you imported a Reputation profile from an NGFW appliance, the SMS displayed an error when you attempted to edit or distribute a Reputation filter. When you performed a filter search, the Reputation filter did not display in the profile filter summary or the profile search results.	105008

Reports

Device	Description	Reference
SMS	After you created a report schedule, you could not make modifications to the schedule.	105349

Reputation

Device	Description	Reference
IPS	When DNS entries that contained international domain names were imported, sometimes the SMS did not convert them correctly. This resulted in `Out of order IPDB database errors` on the IPS.	111925

Web API

Device	Description	Reference
SMS	When a device was removed from a virtual segment, the SMS response did not include the device name on the device result.	108265
SMS	The Web API `Update Virtual Segment` command did not allow you to rename the virtual segment.	108270

Known issues

This release contains the following known issues.

Admin

Device	Description	Reference
SMS	After a backup is restored, the status continues to show that the backup is in progress. **Workaround**: This status can be ignored.	104680
SMS	If you upgrade the SMS from v4.3.0 to v4.4.0 while in FIPS Crypto Core mode and the same certificate is being used for both the remote system log and either LDAP or RADIUS, then the remote system log certificate will not appear. **Workaround**: To resolve this issue, re-import the certificate into the certificate store, and re-configure the certificate for the remote system log.	112430
SMS	After you click on the **Export and Archives** page in a web browser, the following message appears in the 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.	112837

Device	Description	Reference
	Workaround: These messages do not affect functionality and can be ignored.	
SMS	SMS Client Communication protocols cannot be changed while in FIPS Crypto Core mode. For example, if you select TLS v1.1, and then go into FIPS Crypto Core, you will not be able to change the TLS version. **Workaround**: To change the TLS version, leave FIPS Crypto Core, make the change, and then go back into FIPS Crypto Core.	113000
IPS	After restoring a backup on the SMS, the TLS settings displayed all of the **SMS connecting to Device/TMC/LDAP** options as enabled, instead of how it was edited in the backup.	111789
vTPS, 440T	The SMS is unable to retrieve remote syslog events and packet capture (PCAP) files when the SMS receives an IPS event from a TOS v4.0.1 device (vTPS or 440T). **Workaround**: A hotfix is available that prevents the issue or otherwise restarts the event and automatic PCAP downloads from where they stopped. The device will continue to function and enforce your configured policy; however, IPS events and/or PCAPs may be lost if the SMS is in the state long enough for the following to occur: • Cleanup on the SMS event database • Rollover by managed IPS devices of the storage required to temporarily preserve PCAPs with new packet captures If your SMS is managing or you plan to manage a TOS v4.0.1 device, contact TAC for this hotfix.	113370

Client

Device	Description	Reference
SMS	If you check the usages of multiple certificates on the SMS **Admin** > **Certificate Management** > **Certificates** or **CA Certificates** pages, non-specific device certificate usages may not be displayed if any of the certificates have a usage on the SMS (RADIUS, Web, etc.). **Note:** This does not affect certificates that have device usages such as User Authentication or VPN. **Workaround**: Check the usages of the individual certificates.	111547
SMS	Before you can install the SMS client on an OS X computer, you must first install Java 8 Runtime. An SMS Client that runs on Mac with Oracle Java Runtime version 1.8u71 or later will not be able to connect to an SMS that still runs with a 1K certificate key. **Workaround**: Change the SMS to use the 2K certificate key. Go to **Admin** > **General** > **SMS Certificate Key**, and upgrade to use a 2K key.	111633, 112699

Devices

Device	Description	Reference
SMS	When you create virtual segments, warning messages display in the **Validation Report** tab. However, the tab will still display as green even when there are warning messages. **Workaround**: Before you save a new virtual segment, check the **Validation Report** tab for warning messages, even if the tab is green.	108083
SMS	The VLAN ID range on the SMS and on the device LSM are not consistent. **Workaround**: Do not create a VLAN ID range that starts with 0 or ends with 4095.	108142

Device	Description	Reference
SMS	The check box to disable the Quarantine Automatically setting in the SMS does not work. **Workaround**: Disable the Quarantine Automatically setting through the LSM by navigating to **Policy** > **Settings** > **Quarantined Address** and selecting the check box **Automatically release quarantined address**.	112452
SMS	The SNMP and Authentication Preferences preview panels are not available to view in the Import Device Configuration Summary preview page before the configuration import settings are applied.	112520
SMS	If you manage a device with an SMS that does not have a certificate password, and you close or cancel the **Adding Device** dialog, you will get an error when you try to re-add the device that states that the device already exists in the SMS. This error will continue until the adding-device process completes. **Workaround**: When the **Adding device** dialog appears, do not close it; leave it open until it completes, or you receive an error message stating that you need to setup the password.	112590
SMS	When an inspection profile is distributed with an invalidly named SSL Policy or SSL Server to a user-defined virtual segment, the distribution fails. **Note:** The only valid characters are spaces, alphanumeric, and the following special characters: -, _, &, <, >, (,)	112724
Identity Agent	TLSv1.2 cannot be used to communicate with Identity Agent unless the SMS Certificate Key is upgraded to a 2K key. TLSv1.2 is enabled under **SMS connecting to Devices/TMC/LDAP** in **Admin** > **Server Properties** > **TLS**. **Workaround**: To upgrade the SMS Certificate Key to a 2K key, go to **Admin** > **General** > **SMS Certificate Key**.	111922

Device	Description	Reference
IPS	When a virtual segment is reordered on the SMS, the following message may appear in the audit log for both affected and non-affected devices: `Update device virtual segment positions for devices <device name>`. **Note:** Only the devices associated with the reordered virtual segments are actually changed. **Workaround**: These audit log messages can be safely ignored on devices unassociated with the change.	112598
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**. Because of this, the SMS will not allow you to edit the configuration. **Workaround**: Do not use a device-generated key instead of a system master key to manage a device using the SMS.	111321
TPS	An SSL Appliance 1500S cannot be managed unless TLSv1.0 is enabled. **Workaround**: To enable TLSv1.0, go to **Admin** > **Server Properties** > **TLS**, and under **SMS connecting to Devices/TMC/LDAP**, enable TLS v1.0 only.	111677
TPS	The SMS does not clearly indicate that a user role cannot be deleted because it is assigned to a user group. **Workaround**: Remove the user role from the user group that references it, then delete the user role.	111985
TPS	If a device was previously managed by the SMS using TLSv1.1 or higher and was then changed to use TLSv1.0 only, the SMS will not be 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 LSM to change the TLS configuration to TLSv1.0 when TLSv1.1 or higher was previously set.	112536

Device	Description	Reference
TPS	After you perform a device replace, sometimes the new device becomes unmanaged. **Workaround**: Manage the new device manually.	112753
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
vTPS	The SMS fails to distribute a reputation filter to the vTPS. **Workaround**: Perform a full synchronization of the Reputation database (from the SMS Profiles navigation pane, click **Reputation Database** > **Edit** > **Full Sync**).	112589
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 will: • Distribute the profile • Display an error on the distribution dialog • Log 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
IPS, NGFW	LSM users cannot be forcibly logged out from the SMS. **Workaround**: There is no workaround. However, 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), it is not possible to remove the password without removing the user. **Workaround**: To remove the password, remove the user ID.	104416

Device	Description	Reference
SMS, NGFW	You can create a device user group with a role of "none." This role has no capabilities.	105107
SMS, IPS	When you edit the IPS physical segment settings (i.e., Intrinsic Network High Availability (INHA) and Link Down Synchronization), the SMS client may display a RuntimeException error. **Workaround**: These error messages can be safely ignored. The SMS and the LSM for the device will display the modified settings.	113273
TPS, vTPS	When you create a virtual segment on all physical segments, and two or more devices are being managed by the SMS, you will not be able to add these new "any" segments to the devices. **Workaround**: Create multiple virtual segments for each device.	112623
NGFW, vTPS	When you upgrade to the 2K key on the SMS, the SMS Certificate Key Upgrade Wizard shows that the device is incompatible. This only occurs for NGFW v1.2.2 and vTPS v4.0.1. **Workaround**: Ignore this warning message if it appears when the SMS is managing a device with one of the above versions.	112773, 112842
vTPS, TPS	The Device SLG page does not correctly display the state of Performance Protection mode.	113132

DV Toolkit

Device	Description	Reference
SMS	When you override DV Toolkit Packages and distribute them to the device, the filter names in the DV Toolkit package on the device are different from the filter names that display on the SMS. For example, if a DV Toolkit package has a filter named `C031 Snort Rule`, the device displays the filter name as `C1000001 Snort Rule`.	105570

Device	Description	Reference
SMS	When you distribute a DV Toolkit package, the device system log shows a different package ID than is shown in 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, NGFW	You may notice a version error and exception when you distribute the same DV Toolkit package to NGFW devices in a cluster. **Workaround**: Uninstall the DV Toolkit packages from the devices, 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	Instead of displaying the segment name, the interface grid under **Events** > **SSL sessions** appears as ethernetX.	113102
IPS	The SMS has problems synchronizing the URI metadata for events in the alerts table because the device sends URI metadata in two separate logs. As a result, the URI metadata may not be available for some events.	101575

Profiles

Device	Description	Reference
SMS	When you uninstall a Malware Filter Package from devices, the DV Inventory screen incorrectly reports that the uninstall failed on one device.	105246

Device	Description	Reference
	Workaround: This display issue can be safely ignored. Logging out and logging back in will show that the package is removed from all devices.	
SMS	A refresh issue makes it appear that the Malware Filter Package Update allows more than one Malware Filter Package to be active. **Workaround**: This display issue can be safely ignored. Logging out and logging back in will show that only one package is active.	105344
SMS	A `UserNotAuthorized` error occurs when an administrator deletes the shared profile after the SuperUser deactivates the DVT package. **Workaround**: A SuperUser should delete the profile.	106231
SMS	When an Admin user copies a profile using a **Save As** operation, the Admin user will not have access to the copied profile until a SuperUser gives the Admin user access. **Workaround**: The SuperUser can give the Admin user access to the copied profile. Alternatively, the Admin user can access the profile by exporting and then importing it.	106325
SMS	When you try to export/import a profile from one SMS to another SMS, and when either or both of them are in FIPS Crypto Core mode, the selected SMS does not become available, and the export/import fails. **Workaround**: Export the profile to a local file, and then import it into the SMS.	106570
SMS	When a profile is imported from a device segment group, sometimes the active profile version does not match what is shown in the **Details** screen display. **Workaround**: Log out and log back in to the SMS for the version numbers to display correctly.	108034
SMS	A foreign key-constraint error sometimes appears in the SMS system log during an AUX DV package activation.	108055

Device	Description	Reference
	Workaround: This error message can be safely ignored.	
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 CSW.	108137
SMS	When an SSL policy is deleted through the SMS, the SSL profile and server are deleted, but sometimes the certificate is not deleted. **Workaround**: Delete the certificate manually through the LSM.	108971
SMS	When a profile is distributed using a schedule, the version of the profile is displayed as "null" or is missing in the audit log. **Workaround**: Distribute the profile on demand using the UI to display the correct version.	112217
SMS	The SMS does not correctly display the distribution progress of a new DV. **Workaround**: Log off and log back in to the SMS to display the correct distribution version.	112423
SMS	When you attempt to modify an inherited SSL inspection policy, the policy will no longer be visible, but if you log off and log back into the SMS, the policy will reappear in the child profile. Changing the parent policy no longer changes the state of the child policy, but the SSL server validation of the parent profile will still take into account the state of the SSL server of the child policy, which might cause the SSL server validation to fail.	113117
SMS	When an inspection profile has an SSL policy and any option selected as the destination IP address in a DDoS filter, the SMS displays an error message. **Workaround**: Use 0.0.0.1/0 for the **Any** selection in the DDos filter.	113245

Device	Description	Reference
SMS	When you remove a single list value from a tag category, the SMS will remove 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
TPS	If the SMS is running a DV that is older than 4.0 when you activate a vTPS DV (DV version 4.0), the complete DV will be re-loaded instead of just signatures with an updated iteration ID. This DV activation will take longer and will also reset any user-configured policy parameters for Scan and Sweep filters.	108614
IPS	Using non-ASCII characters in a profile description may cause problems on the device.	112910
IPS	When managed by the SMS, if you have configured Advanced Distributed Denial of Service (DDoS) filters to protect against SYN floods, the IPS supports DDoS protection of the SSL server, but not on the ports where we are performing inspection of SSL traffic. For example, if you have a server at 1.1.1.1, and that server responds to HTTP traffic on port 80 and HTTPS traffic on port 443, and you have configured SSL Inspection of the traffic on 1.1.1.1:443, and you have configured DDoS protection of 1.1.1.1 - then you will get DDoS protection on 1.1.1.1:80, but not on 1.1.1.1:443.	111903

Reports

Device	Description	Reference
SMS	When you generate an executive report, the event query will display an inaccurate query structure.	103620

Device	Description	Reference
SMS	When you generate a Specific Country report (**Inspection** > **Security** or **Inspection** > **Application**), or when you generate an Inspection report (Security or Application) and the report has country criteria, if you click a link in the report, you cannot use the **Refresh** button on the Events panel until you restart the SMS client.	106322

Reputation

Device	Description	Reference
SMS	The progress window that displays during a Reputation Database Full Sync does not update and will only show that the sync is "In Queue". **Workaround**: Click on the **Reputation Database** > **Activity** tab to verify the actual progress.	108870
SMS	The date of imported Reputation User Provided Entries is based on the time-zone set on the SMS server, not the SMS client. Any date fields will be updated to reflect the time-zone of the SMS server.	109210

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.	108184

Device	Description	Reference
	Workaround: Do not duplicate VLAN IDs in the XML file when you create virtual segments.	
SMS	The profile name does not display in the SMS audit log message when a profile is distributed through web services.	108197
SMS	An error message is displayed if virtual segments with the same name are sent to a device.	108267

Contacting support

Contact the TippingPoint Technical Assistance Center (TAC) 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: June 2016

Publication Part Number: B09152011