



TrendAI™ TippingPoint™ Security Management System Release Notes

Version 6.7.0

To ensure that you have the latest versions of product documentation, visit the [Online Help Center](#).

- You can only upgrade to SMS 6.7.0 from SMS 6.6.0 or later. If your SMS is running a release earlier than 6.6.0, upgrade to 6.6.0 first, and then upgrade to 6.7.0.
- On some SMS versions, a software update downloaded from the TMC might not appear as available to install until you log out and back into the SMS client; this is fixed in 6.7.0.
- If you are upgrading from an earlier version, refer to the release notes of any interim releases for additional enhancements.
- If your SMS system is operating in High Availability (HA) mode, you must break HA and upgrade each SMS independently before re-establishing your SMS HA cluster.
- Upgrades to this release version require TLS v1.2 to be enabled for SMS client communication before beginning the upgrade process.
- Any earlier version of SMS running in FIPS Crypto Core mode with a 1024-bit certificate cannot be upgraded to SMS v6.7.0. A 2048-bit (or 2k) certificate is required.
- SMS v6.7.0 ships with Digital Vaccine (DV) version 4.0.0.10201.
- The time required to upgrade will vary based on the version from which you are upgrading and the quantity of data to migrate. [Learn more](#).
- For information about third party and open source licenses, refer to the [Third-Party Licensing](#) document.

Product version compatibility

Any upgrade to v6.7.0 on an SMS that is managing an unsupported device will fail. Both a UI dialog and a system log message will indicate which devices need to be deleted first. Likewise, restoring a pre-v6.7.0 version that includes unsupported managed devices will succeed only after the restore automatically deletes those devices (indicated in the system log). For a list of currently supported TPS devices and any scheduled End of Life dates, refer to the [TippingPoint End of Life \(EOL\) dates](#).

For TPS and vTPS managed devices, your SMS must have the same or later version of the TOS that the managed device has. For example:

- **Correct:** SMS v6.7.0 managing TPS v6.7.0
- **Incorrect:** SMS v6.4.0 managing TPS v6.7.0

Note: As a best practice, be sure to update the SMS before upgrading the device TOS.

Software updates and migration

You cannot upgrade any SMS or vSMS from a version that is no longer supported. [Learn more](#) about which versions are no longer supported.

- Upgrading SMS on Gen9 hardware is not supported. Gen9 is a hardware platform that shows as system model SMS H3 or SMS H3 XL in the SMS CLI. To determine your system model, run the `get sys.model` command from the SMS CLI:

```
smsname SMS=> get sys.model
```

```
System model (sys.model) = SMS H3
```

Attempting to upgrade to this release on Gen9 hardware will return an error.

- The SMS only supports backups from releases that are currently supported during the time of a new release. SMS 6.7.0 only supports backups from SMS version 6.2.0 or newer.
- If you are upgrading from a release between v6.2.0 and v6.5.1, you must first upgrade to SMS v6.6.0 before upgrading to v6.7.0. Log in to the SMS to activate a Digital Vaccine, and then upgrade to v6.7.0. [Learn more](#).
- Upgrades to this release version require TLS v1.2 to be enabled for SMS client communication before beginning the upgrade process.
- If your SMS system is operating in High Availability (HA) mode, you must break HA and upgrade each SMS independently before re-establishing your SMS HA cluster.

The estimated times noted in the following table apply to users upgrading from SMS v6.6.0. You can monitor your upgrade status from the VGA console or virtual console.

Step	Task	Process	Estimated time	SMS status
1	Download upgrade package.	Manual	Varies ¹	Available
2	Install upgrade package.	Apply the upgrade package on the SMS. The system performs pre-checks, installs components, and prepares for database migration.	7-13 minutes ²	Unavailable
3	Migrate data.	The SMS applies a database schema update. No historical data is exported or re-imported.	Less than 1 minute ³	Unavailable

¹ Network speed determines the time to download a 1 GB file.

² Varies with platform rather than with the size of your database. The SMS automatically reboots once after you install this release, and is not available for logins until step 3 has completed. Do not reboot the SMS during the upgrade.

³ SMS 6.7.0 applies a database schema update rather than moving historical reporting data, so this step no longer grows with the number of historical rows the way it did in earlier releases. It completed in under one minute on every system tested, including systems holding several hundred million historical rows, and applies whether you upgrade from SMS 6.6.0 or 6.6.1.

Additional notes

1. Earlier releases moved historical reporting data into a new database during the upgrade, and that step grew with the number of historical rows. SMS 6.7.0 does not perform that data movement, so migration time no longer grows with the size of your Historical tables.
2. The pre-upgrade steps that shortened migration in earlier releases — resetting large Historical tables, or upgrading from a backup without Events — have no material effect on 6.7.0 migration duration. They remain relevant when performing a fresh install followed by a backup restore, where restore time does scale with row counts.
3. Before upgrading, it is strongly recommended to perform a full SMS backup (including Events) to ensure all data is preserved prior to any cleanup or migration actions.

Release contents

Description	Reference
The SMS now supports automating the full certificate lifecycle using the ACME protocol with any ACME-compatible certificate authority. Previously, ACME support was tied specifically to Let's Encrypt. Note: The macOS Intel-based SMS client is no longer supported as of SMS 6.7.0. Organizations using macOS Intel systems should transition to supported platforms or contact support for migration assistance.	TIP-128523
The SMS now offers a recurring License Throughput Utilization report, showing per-device license usage trends and peak licensed throughput across the reporting period.	TIP-135165

The SMS now offers a recurring ZDI Filter report, summarizing pre- and post-disclosed ZDI filter hits, associated CVEs, last-match times, and block/permit counts across the reporting period.	TIP-135166
The SMS now offers a recurring Device Health Summary report, covering major or critical system health issues, performance and congestion statistics, aggregate throughput, and per-device license utilization across the reporting period.	TIP-135169
The SMS now supports NTPv4 client time synchronization with authenticated time sources, including FIPS-approved cryptographic algorithms.	TIP-137695
The SMS now supports importing and managing custom Root and Intermediate CA certificates for TrendAI Vision One™ SPC connectivity directly from the SMS Web UI.	TIP-161266
The SMS now supports authentication via 90 Meter Smart Card Middleware, enabling MFA login with DoD-issued SIPRNet tokens for smart-card-enforced environments.	TIP-161772
The SMS Audit Log now captures detailed profile change events, including per-filter enable/disable and action set changes. Bulk changes generate a separate audit record per affected filter.	TIP-205197
The SMS now automatically generates a Technical Support Report (TSR) on a managed device before initiating a TOS upgrade, preserving pre-upgrade device state for support investigations if the upgrade fails. NOTE: • The TSR export can only be done one device at a time. • Each export could take two minutes or longer. Consider upgrading in batches or opt-out using the checkbox to reduce wait time.	TIP-205198
The SMS has a new Web API endpoint that returns all licensing information shown on the Admin > Licensing panel, including license version, status, timestamps, and per-device totals, in JSON. This information can be used for programmatic access and compliance reporting.	TIP-209113
The SMS now supports TACACS+ AAA role mapping using the user-group attribute pushed from the AAA server, removing the need to maintain a corresponding local user account for each externally authenticated user.	TIP-209117
The SMS now displays the user's full name (as provided by TACACS+) in the Active Sessions table, making it easier for administrators to identify who is currently logged in.	TIP-209124
The SMS has four new Web API endpoints that return all user accounts, roles, and groups including the same data shown on the Roles, Groups, and Users menus under Admin > Authentication & Authorization, in JSON. An additional option to export a CSV of all users is also available for programmatic access and audit reporting.	TIP-209119
The SMS now ships with OpenSSL 3.5.6 (FIPS 140-3 validated) and OpenSSH 10.3, maintaining FIPS 140-3 compliance for regulated deployments.	TIP-264707

An issue where the SMS Web UI displayed time incorrectly for timezones with partial-hour offsets has been fixed.	TIP-130982 PCT-47773
An issue where an unknown error message appeared when reopening the SSL Client Proxy trust store has been fixed.	TIP-154170 PCT-78539
An issue where Digital Vaccine Toolkit filter names were corrupted after importing multiple packages, causing filters to not appear in search results, has been fixed.	TIP-155575 PCT-80829
Fixed an issue where setting the lock timeout value equal to or within two of the session timeout value caused validation failures.	TIP-155694 TIP-159621 PCT-84817
Fixed an issue that could cause the SMS to stop parsing log entries for a particular device and log type until the SMS was rebooted or the device was unmanaged/remanaged.	TIP-156541 PCT-69420
An issue where the SMS unintentionally performed DNS lookups on domain names when they were imported into the Reputation Database has been fixed.	TIP-158286 PCT-78806 PCT-65899
An issue where the SMS Console did not display alerts when the user disk was unmounted or missing has been fixed. The SMS now shows the appropriate health status indicators when user disk issues are detected.	TIP-160323 PCT-80681
An issue where the IP Address Lookup Results reset function in SMS Database Maintenance returned a NOT IMPLEMENTED error has been fixed.	TIP-160513 PCT-83901
An issue where the SMS device screen incorrectly displayed a critical status for Management Port and Health with no corresponding issues or logs has been fixed.	TIP-161405 PCT-72061
An issue where SMS continued to send TMC connection alert emails even when TMC upload was disabled has been fixed.	TIP-161580 PCT-89554
An issue where custom segment names did not consistently appear in the segment selection window when distributing a profile has been fixed.	TIP-162029 TIP-237516 TIP-160743 TIP-182734 PCT-85104
Fixed an issue in scheduled SMS database backups when reputation database modifies transient tables during the backup process	TIP-162108 PCT-92039
An issue where Named IP Address Groups imported from CSV files appeared blank in the SMS has been fixed.	TIP-173458 PCT-49052

An issue where SMS profiles and filter override data no longer appeared in TrendAI Vision One™ after upgrading to SMS 6.6.0 has been fixed.	TIP-209445 PCT-95451
An issue that prevented the `/opt/sms` filesystem from being extended on vSMS due to an unmount failure has been fixed.	TIP-209870 PCT-93753
An issue where the SMS database cleanup process remained in a pending state and did not complete without manual intervention has been fixed.	TIP-237452 PCT-78669
An issue where the SMS database storage file grew excessively large, filling the database partition and causing SMS operational errors, has been fixed.	TIP-238565 PCT-94331
An issue where Online Certificate Status Protocol (OCSP) requests bypassed the configured HTTP proxy server when validating certificates has been fixed.	TIP-262775 PCT-105827
An issue where Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) traffic from the SMS bypassed the configured proxy server has been fixed.	TIP-264809 PCT-105827
An issue where SMS database cleanup could race with reporting data import and corrupt the internal extent map, causing backup failures and database errors, has been fixed.	TIP-270273 PCT-108770
The SMS client trust store is reset during a client upgrade. If a custom Web security SSL certificate is being used on the SMS, a dialog box might appear at your next SMS client login attempt prompting you to trust the SMS certificate.	TIP-161524 TIP-137906
An issue where the Specific Country report would take over ten minutes to load has been fixed.	TIP-148132
The SMS was confirmed to not be vulnerable to CVE-2026-46242. This release also includes an upgraded kernel that does not include this issue.	PCT-109329
An issue where SMS database backups could not be saved to an SMB share with SMBv3 encryption enabled has been fixed.	TIP-238557 PCT-70187
An issue where client software installers could not be downloaded from the SMS server has been fixed.	TIP-250010
An issue where TrendAI Vision One™ could not display event logs because of corrupted values in the ALERT table has been fixed.	TIP-154859 PCT-83064
Fixed an issue where an SMS software package downloaded from the TMC could complete successfully but not appear as available to install, requiring a client logout/login to see the package.	TIP-269318

Known issues

Description	Reference
When a snapshot from SMS after changing the master key, wait a few minutes before attempting to restore the snapshot so that the SMS and the device can properly sync up.	TIP-129644
When changes are made to management ports through the CLI, sometimes those changes are not correctly reflected on the SMS Client. Edit the device configuration page dialogue to correctly display your management ports after making a change using the CLI.	TIP-135363
Importing a device configuration exported from a different device family/model can silently fail to apply Data Security settings instead of showing an error.	TIP-136032
If you log out of the SMS or have a session timeout while uploading a software package, you might be unable to resume the package upload without restarting the SMS.	TIP-139589
A software package distribution might fail because there was not enough room for the package, which generates a <code>PackageOpenError</code> message. To resolve this issue, delete an unneeded boot image (excluding the factory image). Use the following CLI command on the TPS device: <code>boot delete-image</code>	TIP-262250
SMS LDAPS authentication fails in FIPS mode without TLSv1.3.	TIP-275717

Product support

For assistance, call one of the TippingPoint numbers on the [Contact Support site](#).

TrendAI™, the Trend Micro t-ball logo, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of TrendAI™ Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.
Copyright © 2024. TrendAI™ Incorporated. All rights reserved.