Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.2.0

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Important: Because of an Operating System (OS) migration from CentOS to Rocky Linux, the SMS TOS v6.2.0 installation package exceeds the size limit of the SMS Software auto-download function on all currently supported TOS versions of SMS. To install SMS TOS v6.2.0, customers must manually download the package from TMC and import it to their SMS server(s).

- 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.
- SMS v6.2.0 upgrades are only supported from an SMS installed with SMS v5.4.1 or later. Attempts to upgrade from an older release will return an error.
- Any earlier version of SMS running in FIPS Crypto Core mode with a 1024-bit certificate cannot be upgraded to SMS v6.2.0. A 2048-bit (or 2k) certificate is required.
- SMS v6.2.0 ships with Digital Vaccine (DV) version 4.0.0.9862.
- With the end of support for CentOS 7 ending June 30th, 2024, SMS v6.2.0 has migrated to Rocky Linux 9. To avoid encountering compliance issues, upgrade your SMS to v6.2.0 at your earliest convenience.
- 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 under the Documentation node on the Threat Management Center (TMC).

Product version compatibility

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 v6.2.0 managing TPS v6.2.0
- **Incorrect:** SMS v6.1.0 managing TPS v6.2.0

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

Software updates and migration

Important: Because of an Operating System (OS) migration from CentOS to Rocky Linux, the SMS TOS v6.2.0 installation package exceeds the size limit of the SMS Software auto-download function on all currently supported TOS versions of SMS. To install SMS TOS v6.2.0, customers must manually download the package from TMC and import it to their SMS server(s).

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 Gen6 hardware is not supported. Learn more in Product Bulletin 1041. Gen6 is a hardware platform that shows as system model SMS H1 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 H1
  ```

  Attempting to upgrade to this release on Gen6 hardware will return an error.

- You must upgrade the SMS from SMS v5.4.1 or later. If you are upgrading from a release earlier than v5.4.1, you must first upgrade to SMS v5.4.1, log in to the SMS to activate a Digital Vaccine, and then upgrade to v6.2.0. Learn more.

- 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 v5.4.1 and later. 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.	Manual	10-15 minutes	Unavailable
3	Migrate data.	Automatic	30 to 90 minutes[2]	Unavailable

1) Network speed determines the time to download a 2.5+ GB file.

2) Depends on the amount of data to migrate. 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***.

Release contents

Description	Reference
Enhancements to Trend Vision One™ integration include: • TLS Network Telemetry for efficient monitoring and analysis of events in real time • Suspicious Object Sync no longer requires a Service Gateway • A Disconnect button on the Connect to Trend Vision One page to conveniently disconnect your SMS locally instead of using Trend Vision One's Product Connector • Network Intrusion Prevention operations in Trend Vision One now can simulate traffic that triggers specified IPS filters associated with your integrated SMS. These simulated attacks correspond to Inspection Events on the SMS Client and can be viewed from the Trend Vision One Workbench. To learn more, refer to the *Integrating SMS with Trend Vision One Software Guide*.	New
This release provides the ability to leverage Server Name Indicator (SNI) extensions to expediently check entries in the Reputation Database and block specific HTTPS traffic without relying on TLS decryption and HTTPS Get requests.	New
The SMS CLI provides two new commands: • `ntp.status` – Lists the status of all SMS NTP servers by their IP address. • `ntp.clients` – Lists NTP clients/hosts that have successfully polled the SMS to synchronize their time. To learn more about these commands, refer to the *SMS CLI Reference*.	New

For idle user sessions, the SMS can now lock the session until a user provides authentication to unlock it.	New
The SMS now supports multiple CAC reader cards that are attached to the user's system.	New
The SMS can now log the IP addresses of all the endpoints (including Syslog, Radius, and AD servers) with which it communicates. This feature is turned off by default.	New
During an upgrade to TOS v6.2, an SMS with an outdated 1K certificate key automatically contacts the TMC up to three times to install any available 2K certificate key. If a more secure 2K key fails to be installed, the resulting entry in the system log will indicate to your TAC representative options for remediation. Normal SMS operations will not be affected.	TIP-101050
This release enhances the automation of DV updates without relying on client access for distribution.	TIP-101061
The SMS extends its certificate support to include Elliptic Curve Digital Signature Algorithms (ECDSA) with secp224rl, secp384rl, and prime256v1 curves. ECDSA certificates can be used for TLS inspection configuration only. Support for ECDSA ciphers has also been added.	TIP-101058
SMS file uploads to TPS 440T and 2200T devices no longer fail with a File too big error.	TIP-93110 PCT-1741 SEG-180383
The SMS OpenSSL version has been upgraded to version 3.0.8.	TIP-102893
An OpenSSH vulnerability (CVE-2023-48795) that enabled attackers to manipulate sequence numbers during the SSH handshake has been repaired in this release.	TIP-107615
An issue affecting outbound SSL Client Proxy configurations has been fixed so that the Decrypted Service value can now be set to something besides <Other>.	TIP-106043
This release improves performance for the function that exports Trace Events from TPS devices to the SMS.	TIP-101057

Known issues

Description	Reference
When you activate a profile snapshot after adding an SSL client policy to the profile, the UI displays the client policy rather than the profile snapshot.	TIP-88920
You can safely ignore the following System log warning message: `SOAP Daemon: Fault returned to SMS 'Error getting noisy security policies from TOS'.`	TIP-91196 SEG-170389
Restoring a backup that contains a 1K web certificate will fail if your SMS is in FIPS mode. Disable FIPS using the `fips-mode disable` command, reconnect the SMS Client, and then replace the 1K web certificate with a 2K (or higher) certificate before re-enabling FIPS mode.	TIP-107918

Product support

For assistance, contact the *Technical Assistance Center (TAC)*.