Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.5.1

This release includes all issues fixed in the Security Management System Release Notes Version 6.5.0. To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Important: If you are using SMS 6.5.0 and none of your managed devices use the 3.2.0 Digital Vaccine (DV) version, you must upgrade to SMS 6.5.1 by manually downloading the package from the TMC website and importing it to the SMS.

- 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.
- SMS v6.5.1 upgrades are only supported from an SMS installed with SMS v6.2.*x* 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 v6.5.1. A 2048-bit (or 2k) certificate is required.
- SMS v6.5.1 ships with Digital Vaccine (DV) versions 3.2.0.10004 and 4.0.0.10004.
- 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 v6.5.1 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-v6.5.1 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 v6.5.1 managing TPS v6.5.0
- **Incorrect:** SMS v6.4.0 managing TPS v6.5.0

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 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.

- The SMS only supports backups that are currently supported during the time of a new release. SMS 6.5.1 only supports backups from SMS version 5.5.4 or newer.

- Upgrades to this release version require TLS v1.2 to be enabled for SMS client communication before beginning the upgrade process.

- You must upgrade the SMS from SMS v6.2.0 or later. If you are upgrading from a release earlier than v6.2.0, you must first upgrade to SMS v6.2.0, log in to the SMS to activate a Digital Vaccine, and then upgrade to v6.5.1. 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 v6.2.0. 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.	Manual	10-15 minutes	Unavailable
3	Migrate data.	Automatic	30 minutes[2]	Unavailable

[1] Network speed determines the time to download a 850+ MB file.

[2] Depends on the amount of data to migrate. An SMS with User URL Reputation configured can last an additional one to three hours. 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
The vSMS is now supported on the Microsoft Hyper-V platform for Microsoft Windows Server 2022 and Microsoft Windows Server 2025. For information on deploying the vSMS on Microsoft Hyper-V, see the deployment steps in the vSMS User Guide.	New
This release expands SMS management support to include the new TPS 5600TXE model.	New
A Certificate Expiration Summary page has been added to **Admin > Certificate Management**. You can view up-to-the-minute counts of your certificates that have expired or are about to expire and configure the frequency of the notifications you receive.	New
This release expands application layer protocol capabilities for sharing threat intelligence by embedding a TAXII 2.1 server, in addition to a TAXII 2.0 server, in the SMS.	New
This release updates the implementation of the Certificate Revocation List (CRL) to use the SMS proxy.	New
This release expands the File Reputation feature by enabling SMS to process File Hashes from Deep Discovery Analyzer (DDAN).	New
The SMS now sends notifications and administrator emails when the SMS is not able to update package file versions or download package files from TMC for any reason. This happens for both automatic and user-initiated package requests, and includes Digital Vaccines, Threat DV IP/Domain Reputation, Threat DV URL Feed, Auxiliary DV. Capacity License, Entitlement, FIPS Keys, Geo Locator DB, and SMS & TOS software packages.	New
An issue where you could not automatically upgrade the SMS from version 6.5.0 in certain circumstances has been fixed.	TIP-138813
An SMS API issue was fixed. This fix allows the SMS to reconnect to Vision One to handle incoming API calls after being disconnected for over an hour.	TIP-138450 PCT-61994 PCT-52228 PCT-63172

This fix addresses a specific issue where device port indexes were left uninitialized, causing reports to incorrectly show that the device was not receiving traffic.	TIP-138326 PCT-66914
Backup restorations from unsupported releases are no longer supported. Only backups from supported SMS versions from SMS v5.5.4.205331 and newer can be restored.	TIP-131137
When you edit a stack name using the SMS client’s Edit button, configuring resilience and SRD values now works as expected.	TIP-131001
This release contains security updates, including a kernel update for CVE-2024-43856.	TIP-129081 PCT-38104
This release fixes an issue that caused Named IP Address Group to be duplicated when the profile was distributed.	TIP-104312 PCT-2029
After an upgrade to v6.4.0, Dell H4 platforms no longer show an amber LED and return the following hardware system error in iDRAC: `A fatal error was detected on a component at bus 2 device 0 function 0.`	TIP-134131 PCT-53957
A table showing the device snapshots for all devices is now available in the Snapshots tab under **Devices > All Devices > Member Summary**. If the **Show All Devices** checkbox is selected, users with appropriate permissions can view and export snapshot data for all devices to a file (select **Export to File > All Rows** from the context menu).	TIP-132302 TVO-5883
OpenSSH has been upgraded to version 9.9p2 for security fixes and addresses the following vulnerabilities: CVE-2025-26465 and CVE-2025-26466.	TIP-134202
The Access SMS Web Services capability (**Edit Role > Capabilities > Admin > Admin Section > SMS Management > Access Management**) is no longer required for downloading the client install image, upgrading or patching the client, or accessing files from Exports and Archives through the Web UI.	TIP-134728 TIP-134519 PCT-55283
An issue where some users could not access the SMS client after upgrading to SMS v6.4.0 or later has been fixed.	TIP-134851 PCT-55004
A startup issue that occurred after expanding the virtual disk on a vSMS has been fixed.	TIP-134705
This release fixes a problem that caused the SMS to stop pulling Suspicious Objects from Trend Vision One if more than 1000 Suspicious Objects were added between polls.	TIP-133988 PCT-49572 PCT-50210
This release fixes an issue where the passive device of an SMS High Availability (HA) pair would stay connected to Trend Vision One™ when the SMS HA was disabled. Now the passive device disconnects from Trend Vision One™.	TIP-131092

The reputation setting `To HTTP requests with matching domain names` now defaults to `false` for file distributions.	TIP-133942
When the Reputation Entries TTL capability is enabled, three bulk deletion operations are now visible: IP/Domain, URL, and File Hash.	TIP-133516

Known issues

Description	Reference
When restoring 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 changing the sFlow Collector IP address setting for a managed device, you might encounter an exception in the Status Details field. This error can be safely ignored, and the actual change remains in the database.	TIP-130872
When configuring HA, the SMS might, in some cases, allow the pairing of dissimilar devices. However, this is **not** a supported configuration — only devices of the same model type are supported in an HA pair.	TIP-135328
Before updating or migrating the SMS, make sure that any queued entries in the Reputation Database have completed to avoid a log error.	PCT-57458 TIP-137693

Product support

For questions or technical assistance, on any Trend Micro TippingPoint product, please contact the Trend Micro TippingPoint Technical Assistance Center (TAC).