Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.3.0

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

- 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 v6.3.0 upgrades are only supported from an SMS installed with SMS v6.2.0. 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 v6.3.0. A 2048-bit (or 2k) certificate is required.
- SMS v6.3.0 ships with Digital Vaccine (DV) version 3.2.0.9889.
- 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

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 v6.3.0 managing TPS v6.3.0
- **Incorrect:** SMS v6.2.0 managing TPS v6.3.0

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.

- 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. 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 v6.3.0. 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 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 515+ 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
This release expands SMS management support to include the new TPS 8600TXE model.	New

This release introduces the ability to enable, configure, and disable daily device discovery so that it will not conflict with other deployments. This daily refresh is now disabled by default.
To display device discovery status, enter the following from the SMS CLI:
`get repos.device.refresh.enable`
To enable device discovery, enter the following from the SMS CLI:
`set repos.device.refresh.enable`
`Enabled daily device refresh (repos.device-refresh-enable) = yes`
To display the refresh time, enter the following from the SMS CLI:
`get repos.device.refresh.time`
`Time-of-day to run device refresh (HH:MM, 24-hour) (repos.device-refresh-time) = <HH:MM>`
To set the refresh time, enter the following from the SMS CLI:
`set repos.device.refresh.time`
`Time-of-day to run device refresh (HH:MM, 24-hour) (repos.device-refresh-time) = <HH:MM>`
To disable device discovery, enter the following from the SMS CLI:
`set repos.device.refresh.enable`
`Enabled daily device refresh (repos.device-refresh-enable=[yes]) = no`
	New

The hostname can now be used to configure PCAP offload for SMB.	TIP-116377
The SMS client's Certificate Signing Request editor now accepts multiple organization unit (OU) or department name values for the certificate's subject Distinguished Name (DN). There is no limit for the number of entries within the field's 4k space allowance. Enter one value per line.	TIP-101244
Port 443 must remain open for downloading installer applications from a web browser. When port 443 is enabled, the client UI will use it for downloading updates and patches during login; if this port is disabled, the client UI will fall back to java message Service (JMS) ports.	TIP-116410 PCT-20438
A condition that caused RADIUS authentication to fail intermittently has been repaired.	TIP-116312 PCT-18412
Version 3 of the `snmpwalk` command now works correctly.	TIP-109563 PCT-16165
The Performance Protection Graph no longer indicates that performance protection is turned	TIP-107842

on when it is not enabled on the device.	TIP-107287 PCT-1738
Performance issues affecting SMS profile distributions have been repaired	TIP-107299 PCT-2015
The error message has been improved when a device is managed using an expired password.	TIP-107289 PCT-1730
Resetting RepDV after bringing an SMS back online no longer results in excessive incremental updates.	TIP-107280 PCT-1165 PCT-10709
The **New** and **Delete** buttons now work as expected in the System Snapshots interface on the SMS client.	TIP-106903 PCT-2027
The way the SMS stores and encodes URI Metadata in the database has been enhanced for detection data monitoring that is encoded in other languages.	TIP-106902 PCT-4236
Fixed an open file handle leak for Trend Vision One TLS Telemetry.	TIP-109599 PCT-15707
Fixed an issue that prevented the geolocation of IPs in Events from displaying.	TIP-117156 PCT-20591

Known issues

Description	Reference
When you disable an inspection bypass rule that has an action of either redirect, egress mirror, or ingress mirror, the target port gets modified if the device is managed by an SMS. To disable the rule, unmanage your device and disable the rule using the device CLI before managing the device again. You must also unmanage the device and use the CLI if you want to re-enable the rule.	TIP-117093

Product support

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