Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.6.0

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

- 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 6.6.0 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 v6.6.0 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 v6.6.0. A 2048-bit (or 2k) certificate is required.
- SMS v6.6.0 ships with Digital Vaccine (DV) versions 3.2.0.10111 and 4.0.0.10111.
- 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 v6.6.0 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-v6.6.0 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 v6.6.0 managing TPS v6.6.0
- **Incorrect:** SMS v6.4.0 managing TPS v6.6.0

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 6.6.0 only supports backups from SMS version 6.2.0 or newer.

- 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 v6.6.0. 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 v6.2.0. You can monitor your upgrade status from the VGA console or virtual console.

Step	Task	Process	Estimated time	SMS status
1	Download upgrade package.	Retrieve the 6.6.0 upgrade package from the distribution source.	Network speed and package size determine download duration. Typical considerations include bandwidth constraints and repository latency.	Available
2	Install upgrade package.	Apply the upgrade package on the SMS. The system performs pre-checks, installs components, and prepares for database migration.	Time varies based on platform performance (SSD vs HDD), system load, and configuration complexity. The SMS automatically reboots after installation.	Unavailable
3	Migrate data.	SMS performs database export → import of historical reporting data into the new MariaDB columnstore reporting database.	Depends entirely on data volume (row counts in Historical tables). SSD platforms migrate ~25M rows/hour; HDD systems significantly slower. SMS is unavailable for login during this stage. Do not reboot the system until migration completes.	Unavailable

Additional notes

1. During data migration, the SMS local console provides real-time visibility into progress, including the current reporting table being processed and the data chunk in progress. 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***.
2. Systems with large datasets (for example, hundreds of millions of historical rows) may require extended migration times. Typical durations range from 12 to 24 hours depending on platform performance and data volume.
3. To help minimize migration duration, customers may consider optional pre-upgrade steps such as:
4. Resetting large Historical tables to remove old reporting data.
5. Performing an upgrade using a backup without Events and restoring after installation.
6. 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
You can now add failed SSL client connections to SSL Client domain exclusions. Excluded domains are not decrypted or inspected, allowing you to continue to connect to those domains. You can also enable Automatic SSL Client Domain Exclusions to add some future failed connections to the exclusions list automatically. For more information, see the SSL Deployment Inspection Guide.	New
TippingPoint SMS v6.6.0 and later uses a new domain to communicate with the Threat	New

Management Center (TMC). If you apply domain-level access control on your firewall and/or proxies, you may require a configuration change to allow access to the new domains: “msd.trendmicro.com” and “ws.trendmicro.com” on TCP/443. For more information, see Ports required for software and security updates in the SMS User Guide.	
SMS backups with historical events can now to be restored without including historical data.	TIP-145892
A problem where duplicate audit and system logs were sent out from the SMS over syslog was fixed.	TIP-138390 PCT-42478
When configuring HA, the SMS sometimes allowed dissimilar TPS devices to be paired. This issue has been fixed.	TIP-135328
An issue with SMS database cleanup has been fixed. Database cleanup now works for historical tables when the SMS is configured for HA.	TIP-138161 PCT-66915
An SMS certificate issue was fixed in this release. 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-136299
Dynamic memory is now disabled by default on the vSMS Hyper-V platform.	TIP-139317
A potential script-related HTML tag vulnerability was addressed in this release with the following: Input sanitization and HTML output encoding Content Security Policy (CSP) header implementation in the Undertow/WildFly application server	TIP-130989
Added a CLI command for specific environments to configure SSH/SCP IPQoS settings with QoS policies that might impact SMS HA synchronization traffic.	TIP-118057 PCT-21191
This release addresses an issue in SMS device SNMP configuration for traps and communities. The issue prevented more than one trap being associated with the same user or one community with multiple IP/subnet.	TIP-135722 TIP-137632 PCT-56606 PCT-87721
This release fixes a profile version activation issue, where SSL client policies were not properly cleared in the UI.	TIP-134707 PCT-58136
This release enhances encryption of sensitive data in the SMS client.	TIP-135943 PCT-60109
Upgraded the MariaDB version and optimized the database configuration settings to resolve corruption issues, which improved performance, security, data integrity, and system stability.	TIP-137756 TIP-139765 PCT-62879 PCT-67974
This release fixed an issue that sometimes prevented client log in because of a log folder permission problem.	TIP-137311 PCT-64606
This release enhanced the reliability of the SMS high-availability communication channel.	TIP-137125

	TIP-137124 PCT-64850
An issue where the high availability (HA) failover button performed a swap instead of a failover when the crypto password prompt was dismissed was fixed.	TIP-145864 PCT-77229
This release prevents an HA synchronization failures that occurred when a failed synchronization source was selected. The issue happened when certificate private key encryption was enabled, and the password was not entered when prompted.	TIP-145748 PCT-77347
This release fixed an issue where large reputation database distributions failed with the error "Distribution package file is empty or does not exist." The SMS now has better detection for supported IPDB file sizes on devices.	TIP-135835 PCT-82050
Fixed backup exports that use SMBv3.	TIP-144102 PCT-70187

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
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
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
TLS v1.3 for communication is enabled by default on a fresh installed SMS, but an upgraded SMS or an SMS restored from a backup does not have TLS v1.3 enabled. For SMS FIPS Crypto Core management of FIPS enabled TPS devices, ensure that TLS v1.3 server communication is enabled on the SMS.	DOC-10035
Rate limit reports that use the "Last Hour" time range might not display results. To view recent rate limit data, use the "Incremental" time search option, and select 2 hours as the time frame.	TIP-162092

Product support

For assistance, call one of the TippingPoint numbers on the ***Contact Support site.***