Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.4.0

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 v6.4.0 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 v6.4.0. A 2048-bit (or 2k) certificate is required.
- SMS v6.4.0 ships with Digital Vaccine (DV) versions 3.2.0.9972 and 4.0.0.9972.
- 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 v6.4.0 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-v6.4.0 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 v6.4.0 managing TPS v6.4.0
- **Incorrect:** SMS v6.3.0 managing TPS v6.4.0

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 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 v6.4.0. 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. 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
This release introduces the next generation of SMS appliances, the Dell PowerEdge R660 SMS H5 and H5 XL rack servers, for greater available storage. Refer to the *SMS H5/H5 XL Appliance Guide* on the Online Help Center.	New
Support for a new type of Reputation filtering enables users to alert and/or block malicious files according to their hash values. You can add as many as 35,000 SHA-1 or SHA-256 file hashes of any type to the Reputation Database. In this release, file hash is applied to http (or https when decrypting) get requests, for all files except the following: • HTML • Audio or video • Font • Files larger than 50 MB When the **Suspicious Object Sync** connectivity setting to Trend Vision One is enabled, the SMS can now pull SHA-1/SHA-256 file hashes from Trend Vision One into the SMS reputation database, along with IPv4/IPv6 addresses, Domain name entries, and URLs. File Hash Reputation does not support an action set with a **Rate Limit** flow control. For those entries, you can change the action set to one with a different flow control type or remove file hashes from the entry criteria. Users upgrading to v6.4.0 must ensure that they also activate the corresponding Digital Vaccine (DV) version, 3.2.0.9962 in order to use file hash Reputation filtering.	New
By using the Let's Encrypt (LE) CA for ACME certificate requests, TLS certificate renewal is automated. You no longer have to manually request TLS certificates and keys from a protected web server for the initial TLS configuration and then again every time these assets expire. Automation includes: • **Certificate Issuance**. Automatically obtain a new certificate when needed. • **Validation**. Verify domain ownership without manual intervention. • **Installation**. Install and configure the CA-signed certificate for transparent inspection of encrypted web traffic.	New

Server name indication (SNI) filtering has been added to the Domain Suspicious Objects database. The TLS handshake inspection this provides enables you to filter servers by FQDN instead of wildcarded URLs, while sustaining the ability to inspect encrypted traffic without having to decrypt. In addition, Domain reputation filtering has been enhanced to support wildcards, allowing filtering by country code or top-level domains.	New
The Digital Vaccine (DV) has a new deployment setting, Evaluation, which uses the same filters that are enabled in the Default deployment mode, but with a **Permit+Notify** posture instead of **Block**. **Note:** Certain traffic normalization filters that detect malformed IP packets must remain configured to **Block**. For any filters that have a recommended configuration of **Block**, you must manually override the default setting and set them to **Block** yourself prior to distribution of the new DV that contains the Evaluation deployment mode. If the DV with the new Evaluation mode is deployed without this manual override, any profile that uses the new Evaluation deployment mode will have its existing default **Block** filters modified to **Permit+Notify** after the profile is distributed to the device.	New
This release adds support for TLS 1.3, delivering enhanced security, faster performance, and a streamlined protocol for improved reliability and efficiency.	New
A new `punycode` parameter has been added to the `repEntries/query?dns` SMS API call. This parameter causes the output from a DNS query to show punycode-encoded domain names instead of unicode domain names.	TIP-119878
The following host key algorithms are no longer supported for SSH access to the SMS: • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521	TIP-124500
The SMS no longer uses the following ports: • 10042 • 10043 • 1098 • 1099 • 4444	TIP-122285
This release fixes an issue that prevented users from accessing the SMS web management console after a reboot.	TIP-126039 PCT-36927
In addition to x86 (Intel) processors, the SMS client can now also use ARM (Apple Silicon) processors.	TIP-107667 PCT-2003

From the SMS Web interface, download the MacOS SMS client installer specifically designed for ARM-based CPUs and begin the upgrade process. Upgrades from a client version previous to v6.4.0 on MacOS 15 and later will fail because of a known issue with the Rosetta 2 emulator.	
To improve scale and resilience, packet traces generated when a filter is matched can now be included as part of the syslog message output from SMS to a SIEM/collector. This can improve scale and helps avoid challenges related to matching pcap files with security events.	TIP-101055
An audit log spamming condition that caused the TPS disk to show as full has been repaired.	TIP-129720 PCT-45160
This release fixes a status display issue for 8600TXE fans and power supplies.	TIP-128963 PCT-43558
The KVM console readout no longer continuously shows disconnects and reconnects of the keyboard and mouse after an upgrade.	TIP-128659 PCT-42102
When exporting a device configuration from SMS, the file no longer stores SNMP passwords in plain text.	TIP-127960 PCT-39454
This release fixes incorrect file permissions on the `smsportfwd` file that could cause a loss of access to the SMS Web interface.	TIP-126039 PCT-36927
When you disable SMS High Availability with the intention of using the SMSs independently, if Trend Vision One integration has been used, the passive SMS must be factory reset. Do not disconnect from Trend Vision One prior to the factory reset.	TIP-131092
An issue that caused `SOAP Daemon: Fault returned to SMS 'Error getting noisy security policies from TOS'` to repeatedly display in the system log has been fixed.	TIP-112692 TIP-117214 PCT-1740 SEG-170389
Filter exceptions no longer permit invalid IP ranges to be entered.	TIP-117866 PCT-20092
This release removes the `diffie-hellman-group14-sha1` SSH key algorithm.	TIP-117711 PCT-17718
Two SMS Web Server vulnerabilities, `No Same site attribute: JSESSIONID` and `Slowloris Denial of service vulnerability`, are addressed by an upgrade to the Java environment (Wildfly) in this release.	TIP-119418 TIP-119417 PCT-23692
This release fixes an SMS Java Version Disclosure vulnerability through an upgrade to the Java environment (Wildfly).	TIP-117409 PCT-1315
This release fixes an issue where multiple versions of snapshots were all marked as “Allow Restore.”	TIP-128956 TIP-110115 PCT-41490

This release fixes an issue where Scheduled Reports erroneously displayed as empty.	TIP-107858 PCT-1708
The help screen for the ThreatDV URL Lookup now displays correctly.	TIP-107098 PCT-3181
An issue that prevented profile distribution with the `failed to build url` error has been resolved.	TIP-106751 PCT-2006
Users no longer have to remove all leading or trailing spaces in their filter names (including Traffic Management, Advanced DDoS, Reputation, and SSL inbound/outbound filters) during an upgrade.	TIP-123602
Both HA nodes require an SMS certificate key size of 2048 bits before HA is configured.	TIP-129960
An issue was fixed on historical port graphs that caused the y-axis port speed labels to sometimes display incorrectly.	TIP-118419 PCT-19499
Enhancements in this release prevent data duplication for events in the remote syslog that could occur under rare conditions: • **New preference setting for events.** A new system preference setting, **Retrieve New Events/Logs Only**, restricts the SMS to examining only recent entries from a device when the last fetched event is indeterminate or the device is newly managed. This is enabled by default. • **Event transmission control.** To further reduce data duplication and to ensure the relevance and efficiency of data transmission, the system now restricts transmitting remote syslog server events to those generated within the last 24 hours.	TIP-120358 PCT-7954

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 you change any sFlow IP Address, an exception error is returned even though the update succeeds on both the device and the SMS.	TIP-130872
Disabling TLS 1.2 for “SMS connecting to Device/TMC/LDAP” will disrupt the connection to TMC and block access to the latest software updates.	TIP-128681
When you edit a stack name using the SMS client’s Edit button, resilience and SRD configuration will not work. You will have to delete the stack and re-create it to change these values.	TIP-131001

Product support

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