



Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.1.0

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.
- SMS v6.1.0 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 v6.1.0. A 2048-bit (or 2k) certificate is required.
- 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 v6.1.0 managing TPS v6.1.0
- **Incorrect:** SMS v5.5.4 managing TPS v6.0

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:

```
smsdev 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 v6.1.0. [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 750+ 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
<p>Enhancements to Trend Vision One™ integration include the abilities to:</p> <ul style="list-style-type: none"> Integrate your SMS with Network Intrusion Prevention without deploying a Service Gateway Send URLs for Cloud Sandbox Analysis <p>To learn more, refer to the <i>Integrating SMS with Trend Micro Vision One Software Guide</i>.</p>	New
<p>This release extends the VMware vSphere environment to include support for VMWare ESX/ESXi version 8.0 for vSMS appliances.</p>	New
<p>Beginning with TOS v6.1.0, a vSMS requires a minimum of 8 CPUs and 32 GB of memory.</p>	TIP-92633
<p>An upgrade issue has been fixed in which the list of SSL server proxies defined from TOS v5.4.0 would be truncated.</p>	TIP-92579 SEG-180520
<p>FQDN-DNS resolution now functions correctly for SSH.</p>	TIP-90414 SEG-174412
<p>CAC authentication logins can now accommodate multiple cards and card readers. When multiple cards are inserted during a log in or session unlock, a dialog is displayed that lets you specify a card reader.</p>	TIP-93434
<p>An issue that caused the SMS Client to display the shelf-level view of a device in an <code>updating view</code> state that never resolves has been fixed.</p>	TIP-89746
<p>The same distribution status email no longer gets repeatedly sent after a distribution.</p>	SEG-167420
<p>After reconfiguring a certificate on an SSL server proxy, the SMS no longer incorrectly removes CA certificates from TPS devices that other SSL Server Proxies are still using.</p>	TIP-92704 SEG-173745 TIP-91481 SEG-171933
<p>A performance issue with SMS and Trend Vision One™ integration that caused SMS event reporting delays has been repaired.</p>	SEG-165162 TIP-87911
<p>Performance issues affecting SMS profile distributions have been repaired.</p>	SEG-164976 TIP-88125 SEG-166650 TIP-88310
<p>When it does not have direct internet access, the SMS now displays a yellow warning symbol instead of a red critical symbol for <code>Undetermined Revocation Status</code>. This properly reflects the lower severity when OCSP/CRL URI cannot be reached.</p>	SEG-155765 TIP-86234

<p>The SMS now indicates when a CA certificate is expired:</p> <ul style="list-style-type: none"> • In the Certificate Details > Path panel • After a certificate's tooltip <code>Expires On</code> date in the CA Certificates table 	TIP-85164
<p>This release fixes an issue that caused profile distributions to fail because of special characters used in the SSL profile description.</p>	TIP-80858
<p>Under high CPU usage conditions, the SMS client no longer hangs when trying to access the vSMS.</p>	SEG-165834 TIP-88696
<p>The SMS interface no longer hangs after running a saved report.</p>	SEG-169383 TIP-89250
<p>An email alert is now sent after a scheduled or automatic Auxiliary DV download/activation/distribution.</p>	SEG-90493 TIP-41314 SEG-136653 TIP-85340
<p>The SMS database cleanup processes now work correctly on row-based partitioned tables.</p>	TIP-89402
<p>You can now select multiple users across multiple TPS devices and specify a new password across all those TPS devices at the same time.</p> <p>Navigate to Devices > All Devices > Member Summary > Device Users, select the users whose passwords you want changed, and click Edit.</p>	TIP-69514
<p>Updated time zone libraries to accommodate countries that no longer observe Daylight Savings Time.</p>	TIP-93066 SEG-175263
<p>The SMS audit logs now display the complete details, including all changes made, that the device audit logs display.</p>	TIP-91158 SEG-158043
<p>This release resolves an issue that required an SMS to use 2048-bit (2K) keys to communicate with a device.</p> <p>Although this issue is resolved, you can avoid future compatibility issues by upgrading your SMS Certificate Key to a 2K key.</p>	TIP-102107
<p>This release enables the sflow daemon to automatically restart if it unexpectedly exits.</p>	TIP-93846

Known issues

Description	Reference
<p>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.</p>	TIP-88920

For outbound SSL Client Proxy configurations, the Decrypted Service value cannot be changed. It is always set to <Other>.	TIP-106043
---	------------

Product support

For assistance, contact the [Technical Assistance Center \(TAC\)](#).

© Copyright 2023 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks of their respective owners.