Trend Micro™ TippingPoint™ Security Management System Release Notes

Version 6.0

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 v6.0 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.

- 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](#).

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 v6.0 managing TPS v6.0
- **Incorrect:** SMS v5.5.4 managing TPS v6.0

Use SMS v4.4 or later to manage Identity Agent v1.0.0.

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 v6.0. 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
This release expands SMS management support to include the new TPS 9200TXE model. To manage a 9200TXE device, the SMS must have a 2K key installed to communicate with the device. **Note:** Installing a 2K key requires a restart of the SMS. The 2K key will not be in use until you restart the SMS. **Note:** If you have an SMS cluster, you cannot install the 2K key in either SMS while the SMS is running in HA. You must first disable the HA cluster, install the 2K key on each SMS, and then reconfigure the SMS HA cluster.	New
You can now send detection events and filter status to Trend Vision One without deploying the Service Gateway. For more information, refer to the *Integrating SMS with Trend Micro Vision One Software Guide*.	TIP-83831
You can now select multiple users across multiple TPS devices and specify a new password across all those TPS devices at the same time. Navigate to **Devices > All Devices > Member Summary > Device Users**, select the users whose passwords you want changed, and click **Edit**.	TIP-69514
For enhanced security, you can specify a more robust signature algorithm (SHA256, SHA384, or SHA512) when creating Certificate Signing Requests (CSRs).	TIP-86918
The SMS Client no longer reverses the SMS Management Interface Port Statistics for the column values in: • **Total In:Discards** and **Total Out:Discards** • **Total In:Errors** and **Total Out:Errors**	TIP-65696
You can now enable and disable the high-speed network interface card (NIC) for the SMS management network interface (eth0) using the `mgmtsettings` command. This command will display descriptive prompts and automatically restart the networking service if needed.	TIP-36825
Different screens across the SMS user interface now consistently show the same status indicator for when a port is disabled.	TIP-65700
This release adds SSL configuration support for downgrading inbound HTTP/2 connections to HTTP/1 on 9200TXE devices so that the 9200txe device can inspect the decrypted traffic.	TIP-54910
This release fixes an issue that caused profile distributions to fail because of special characters used in the SSL profile description.	TIP-80858

When it does not have direct internet access, the SMS now displays a yellow warning symbol instead of a red critical symbol for `Undetermined Revocation Status`. This properly reflects the lower severity when OCSP/CRL URI cannot be reached.	SEG-155765 TIP-86234
In order for users to access the Performance Insights page, the **Edit filter performance correlation configuration** capability must first be enabled for that user's role.	SEG-159591 TIP-87035

Known issues

Description	Reference
The following features are not supported on TXE devices: • 802.1ah/ MAC-in-MAC • FIPS	TIP-88298
An issue prevents the SMS from recognizing a device's correct interface in the SSL logs.	TIP-88888 TIP-88726
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.	TIP-88920
Under high CPU usage conditions, the SMS client might hang when trying to access the vSMS.	TIP-88696

Product support

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

Security Management System Release Notes