Security Management System Release Notes

Version 5.5.4

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 v5.5.4 upgrades are only supported from an SMS installed with SMS v5.3.0 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 v5.5.4 managing TPS v5.5.4
- **Incorrect:** SMS v5.3.0 managing TPS v5.5

Use SMS v5.0.1 Patch 2 and later for managing IPS devices running TOS v3.9.6 and earlier.

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

Beginning with TOS v5.5.4, only 64-bit versions of the SMS Java Client are supported.

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 to SMS v5.3.0 or later. If you are upgrading from a release earlier than v5.3.0, you must first upgrade to SMS v5.3.0, log in to the SMS to activate a Digital Vaccine, and then upgrade to v5.5.4. 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 v5.4.0 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+ MB 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 enables users to properly configure their security policies according to the visibility of CVEs in their network environments that Vision One provides.	New
SMS high availability is now supported in FIPS mode if both systems have a 2K key and the same FIPS mode configured.	New
An SMS syslog message has been added so that every boot indicates if existing minimum requirements are not set.	New
For secure mail transfers, the **Enable SMTPS** option has been added to the Edit SMTP Server Settings dialog.	New
When used in an SSL policy name or SSL profile description, some characters can trigger a condition that causes profile distributions to fail. When naming your SSL policy or entering an SSL profile description, use only these characters: • Alphanumeric characters: a through z, A through Z, and 0 through 9 • Special characters: ( )	TIP-80858 SEG-145514
When an import of a certificate fails, the resulting error messages now provide more constructive details.	TIP-81922 SEG-141695
The SMS remote syslog no longer sends old Alert log events after a high availability (HA) failover or swap.	TIP-81117 SEG-134638
The vSMS default virtual disk size can be dynamically increased from 300 GB to 600 GB or greater for increased disk partition sizes.	TIP-81369 SEG-147435 SEG-156829
The recommended minimum amount of memory for a vSMS is 32 GB. A warning system log entry will be added any time memory is less than 32 GB when the SMS application restarts.	TIP-57021 SEG-147435
This release fixes an issue with PKCS12 certificate name validation that prevented TLS inspection profile distribution.	TIP-80857 SEG-141581
When you attempt an SMS swap and then disable HA, the previously managed devices no longer fail to get remanaged.	TIP-80776 SEG-145432
This release ensures that listeners registered by the client can be automatically cleaned up.	TIP-79105
An issue that caused file storage space issues on managed devices has been fixed.	TIP-77849 SEG-138156

This release removes a vulnerable Java version of OpenJDK.	TIP-73557 SEG-123256
Updates to a profile's action set no longer produce inaccurate information in the Profile Version Details, and no longer cause display issues in the client profile history.	TIP-77113 SEG-134750
Stronger TLS ciphers are now supported and enabled by default. Weaker TLS ciphers are now disabled. Weak SSH MAC algorithms are also disabled.	TIP-82421 SEG-161705
The SMS no longer deletes certificates (including expired intermediate certificates) from managed devices during SSL inspection profile distribution when the full chain fails to validate.	TIP- 78909 SEG- 133553
This release contains database changes that improve performance and prevent disk space utilization issues.	TIP-81010 TIP-84977 SEG-147601
SMS v5.5.4 requires TLS v1.2 for communication. If you disable TLS v1.2, you will not be able to manage the device from SMS.	TIP-83949

Known issues

Description	Reference
Trend Micro Vision One^{TM} supports integration with only one SMS per account.	TIP-84650
Under some circumstances, managed devices do not get listed in the SMS Client nor in the SMS Web Console.	TIP-84386
If your SMS does not have direct internet access, an `Undetermined Revocation Status` notification will be displayed with a red symbol in the certificate manager for certificates that contain an OCSP/CRL URI. This does not prevent the usage of these certificates for any purposes.	SEG-155765

Product support

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