Security Management System Release Notes

Version 5.5.3

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 v5.5.3 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 v5.5.3 managing TPS v5.5.3
- **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.

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 v5.5.3. 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
After upgrading to 5.5, some users noticed issues with the historical graphs, including units of measurement not being displayed, and data getting dropped when switching time periods.	TIP-72090 SEG-120666
The SMB timeout has been increased to prevent SMS backup failures when using SMB encryption.	TIP-74774 SEG-118198
Additional cipher support has been added to prevent SMS backup failures with sFTP.	TIP-74536 SEG-128861
You can now configure a second Active Directory server that the SMS can use for authentication when the primary authentication server cannot be reached.	TIP-77583
To improve the collection and analysis of threat statistics, the TMC Information Share setting **Enable ThreatLinQ event sharing** now defaults to **ENABLED**, with the option **Hide All IP Addresses in ThreatLinQ** selected.	TIP-77732 TIP-77864
To avoid distribution delays after an SMS restart, restore the AuxDV schedule distribution.	TIP-73834 SEG-125973
To secure sensitive login information, the auto-complete feature setting for browsers defaults to **off**. However, when users reflexively click **Yes** after the browser prompts them to remember login information, the users must manually remove the login information in order to prevent the browser from storing it.	TIP-73560 SEG-124587
With FIPS and TLS1.2 enabled, the SMS no longer fails when connecting to a secure LDAP server that had certain ciphers enabled.	TIP-76499
Performance has been improved in remote syslog over TCP.	TIP-76351 SEG-129341
Remote SMS Authentication from a device would not work properly if that device was managed by another SMS while the remote authentication feature was still enabled.	TIP-71137 SEG-112688
A vulnerability (CVE-2021-3449) that could enable attackers to exploit an OpenSSL TLS server with a malicious Client Hello message has been resolved in this release. Learn more.	SEG-139152
This release sanitizes the names of policy exceptions so that invalid names do not cause profile distributions to fail.	SEG-122201
The SMS ssh package has been updated to include security and bug fixes.	TIP-76669

Known issues

Description	Reference
Attempts to upgrade from a release earlier than v5.3.0 result in an error message. If the error message is blank, check the SMS system log for the entire error message.	TIP-47930
Performing a backup and restore of the SMS database will not preserve Filter Performance Correlation data.	TIP-42709
SSL inspection cannot occur when web mode is enabled. By default, web mode is disabled.	TIP-64243
The **Edit Bulk** action does not remove tag categories from user-provided Reputation entries. To remove tag categories from an entry, go to **Profiles > Reputation Database > Search Entries**, search for an entry, select entries in the search results, and click **Edit**. The search results display the first 10,000 entries. If you are modifying more than 10,000 entries, you must repeat this procedure. When searching for URL entries, the search results table will not automatically refresh. Click **Search** to refresh the table.	TIP-37913
When used in an SSL policy name, some special characters can trigger a condition that causes profile distributions to fail. When naming your SSL policy, use only these characters: • Alphanumeric characters: **a** through **z**, **A** through **Z**, and **0** through **9** • Special characters: **( )**	TIP-38808
The SMS web management console shows the incorrect time zone only when set to GMT +/- 00:30 time zones. For the correct time, refer to the SMS Client console.	TIP-33377
The SMS does not activate a Digital Vaccine package when it contains a significant number of malware tags for a filter.	TIP-33378
When you attempt to distribute too many TLS/SSL certificates to a device, the resulting error message incorrectly specifies CA certificates as the problem.	TIP-44753
When you remove a CA certificate used for authentication from the SMS Authentication CA certificate list—for example, when you delete the authentication configuration from the SMS—the CA certificate is also deleted from the device. If this same CA certificate was distributed to a device as part of the SSL server certificate chain, the device would have an SSL server with a missing CA certificate in its SSL certificate chain.	TIP-44645

Product support

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