Security Management System Release Notes

Version 5.4.0

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

- If you are upgrading from a previous 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 v5.4.0 upgrades are only supported from an SMS installed with SMS v5.3.0 or later. Attempts to upgrade to 5.4.0 from an older release will result in an error message.
- 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 v5.4.0 managing TPS v5.4.0
- **Incorrect:** SMS v5.3.0.2 managing TPS v5.4.0

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 in this release. 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 result in an error.

- You must upgrade the SMS to v5.4.0 from SMS v5.3.0.*x*. If you are upgrading from a release earlier than v5.3.0.*x*, you must first upgrade to SMS v5.3.0, log in to the SMS to activate a Digital Vaccine, and then upgrade to v5.4.0. 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 v5.3.0 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+ 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
Added real-time threat protection for outbound client SSL traffic.	New
The SMS now supports TLSv1.3 in FIPS mode for the following: • SMS Client communication (ports 9003 and 10042) • TMC connections • Device connections • LDAP connections	New
The vSMS now supports VMware vSphere 6.7 and 7.0.	New
Performance enhancements prevent SMS clients from being locked out after HA events.	TIP-44446
SMS Client does not show device system logs beyond 7 days.	TIP-47162
Fixed an issue where the SMS was only adding its name to syslog records for certain types of events. It is now always adding its name properly.	TIP-45991
Local scheduled backups no longer fail.	TIP-54353 TIP-53109
When you use an encrypted TCP syslog, you no longer have to restart the SMS before certificate changes go into effect.	TIP-52245
The vSMS VMWare image is now signed with a cert that expires in three years instead of in one year.	TIP-46428
Restrictions for validating host names from the SMS device editor required that the host names matched what was on the device LSM or CLI. This was corrected on the SMS so that fully qualified domain names could be entered into the host name field.	TIP-44716
Syntax problems in the CSV file caused the maximum record size to be exceeded, which also caused the error message to not display correctly in the UI.	TIP-47381
Repeated CPU halting caused by the kernel version that SMS v5.3 shipped with could cause the Vertica database to become corrupted.	TIP-50630
When run from the SMS client, the WHOIS command sometimes yields no results.	TIP-52081
An issue that caused URL normalization errors on some devices during URL reputation filtering no longer occurs.	TIP-48354

Clicking on the Devices panel would sometimes fail to display the managed devices. Clicking on any other panel after this would freeze the interface.	TIP-49499
Under rare conditions, the SMS Diagnostic files could inflate inordinately.	TIP-52211
Some Reputation IP exceptions updates were not being applied to the exceptions list after the profile was distributed. This has been corrected.	TIP-47958
If a user without access to all groups on the SMS performed an action that would restart the RADIUS login module on the SMS, the map of groups used in RADIUS group mapping would be re-created to contain only the groups that user had permission to view. This release ensures that if the RADIUS login module is restarted, the map will contain all groups on the SMS regardless of user permissions.	TIP-53284
An issue that caused the syslog to display old events along with new ones, even though the deployment was configured to forward only new events, has been corrected.	TIP-45360
An issue that caused the SMS to enable Auto-Negotiation on a TPS device after an upgrade has been corrected.	TIP-47526

Known issues

Description	Reference
Attempts to upgrade to v5.4.0 from a release earlier than v5.3.0 results 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
After you increase the vSMS disk size, you must turn on and then reboot the vSMS again before the extra disk space is achieved. If you originally deployed the vSMS using TOS v5.2.0 or earlier, the increased disk space cannot be fully achieved.	TIP-54547 TIP-54548
After an upgrade to SMS v5.3.0 from a previous version, the number of Attacked Vulnerable Hosts on the SMS web management console does not reflect the pre-migration count.	TIP-44771

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
Certain naming configurations could trigger a condition that causes profile distributions to fail. To prevent failures, make sure that the names of your profiles, segments, virtual segments, and certificates are less than 55 characters.	TIP-45073 TIP-38808
The System Health and Performance graphics display a different power supply status for 440T devices depending on which TOS the SMS is running. SMS v5.0.1 displays `n/a`, and SMS v5.1.0 displays `50%`.	TIP-36468
Exporting the hourly report to the SMB share does not work on systems upgraded to SMS 5.3.0.1.	SEG-77932
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).