Security Management System Release Notes

Version 5.3

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

Important notes

- 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.
- Expect an upgrade to SMS v5.3 to take substantially longer than previous upgrades. 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.

Important

Because of an issue preventing URL normalization that results in system log notification errors, you must follow these steps before upgrading to v5.3.0 if you are using URL Reputation and wildcards in URL entries. To determine if you meet these criteria, navigate to **Reputation Database > Search Entries** and enter `\*` in the URL text box.

To enable URL normalization, follow these steps before upgrading:

1. Disable any feeds going into the Reputation User Entry database (such as URL Forwarding and scripts that update entries using web APIs).
2. Export all user entries (including IP and DNS) by navigating to **Profiles > Reputation Database > User Entries > Export** from the SMS interface.
3. Delete all user entries.
4. Complete the migration to v5.3.0. Refer to Software upgrades and migration.
5. Import IP, DNS, and URL entries

If you have already upgraded to v5.3.0, contact TAC for assistance.

Product version compatibility

	SMS v5.3	SMS v5.2	SMS v5.1.1	SMS v5.1	SMS v5.0.1 P2	SMS v5.0.1 P1	SMS v5.0	SMS v4.6	SMS v4.5	SMS v4.4
TPS	TOS v5.3 and earlier	TOS v5.2 and earlier	TOS v5.1.x and earlier	TOS v5.1 and earlier	TOS v5.0.0 and earlier	TOS v5.0.0 and earlier	TOS v5.0.0 and earlier	TOS v4.2.x and earlier	TOS v4.2.x and earlier	TOS v4.1.0 and earlier
vTPS	TOS v5.3 and earlier	TOS v5.2 and earlier	TOS v5.1,x and earlier	TOS v5.1 and earlier	TOS v5.0.0 and earlier	TOS v5.0.0 and earlier	TOS v5.0.0 and earlier	TOS v4.2.0 and earlier	TOS v4.2.0	TOS v4.0.2
IPS	TOS v3.9.6 and earlier	TOS v3.9.6 and earlier	TOS v3.9.6 and earlier	TOS v3.9.6 and earlier	TOS v3.9.6 and earlier	TOS v3.9.4 and earlier	TOS v3.9.3 and earlier	TOS v3.9.3 and earlier	TOS v3.9.3 and earlier	TOS v3.8.4 and earlier
Identity Agent	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0	v1.0.0

Software updates and migration

Be sure to perform a full backup with events prior to attempting an upgrade.

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 can upgrade the SMS to v5.3 directly from SMS v5.0.1 or later. If you are upgrading from a release earlier than v5.0.1 you must first upgrade to SMS 5.0.1, log in to the SMS to activate a Digital Vaccine, and then upgrade to v5.3. Learn more.

- A vSMS must run partition version 2 or higher to upgrade to SMS v5.3. If your vSMS is running partition 0 and 1, you cannot upgrade to this version of SMS. You must first perform a full SMS backup, redeploy the v5.0.1 vSMS or the current v5.3 vSMS to get the latest partition version, and then restore the backup. You can restore any SMS database backups beginning with SMS 4.4.0 or later on an SMS running SMS v5.3. Run the `get repos.partition-version` command from the SMS CLI to identify the partition version on the vSMS.

Because the SMS ssh keys are re-created after a full upgrade, you might see a message identifying the SMS as an unknown host during the ssh connection.

Important: Do not interrupt an upgrade that is in progress. If you attempt to reboot the SMS, or if there is a loss of power, the disruption could result in complete data loss and render the system unrecoverable.

The SMS v5.3 upgrade package requires at least 12 GB of memory and 300 GB of space. Because this larger package involves staging and restoring data across two reboots, a full upgrade to SMS v5.3 can take between 35 minutes and several hours to complete. Factor in 90 seconds for every 2 million records of historical data that you want restored. If you do not require historical data, you can reduce the upgrade time by navigating to **Admin > Database** in the SMS Client and deleting it.

For vSMS, upgrade times depend on the number of configured CPUs and the virtual disk performance.

The estimated times noted in the following table apply to users upgrading from SMS v5.0.1 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	2-10 minutes	Unavailable
3	Migrate data.	Automatic	Up to 3 hours[2]	Unavailable

1) Network speed determines the time to download a 1.8 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
The Filters for Review interface of the SMS web management console provides operational, security, and performance contexts so you can make strategic changes to your security policy according to filter factors relevant to the policy. Performance management features of the SMS web management console's Filters for Review interface are supported only on TPS and vTPS devices running TOS v5.3 or later. To learn more about this feature, refer to the *SMS User Guide*.	New
With the Server Name Indication (SNI) protocol extension, the SMS can now accept multiple certificates and keys from a single SSL server. This enables the server to safely host multiple TLS/SSL certificates (up to 1000 per device) for multiple sites under a single IP. When configuring SSL to accept multiple certificates and keys, ensure that you do *not* enable the SSLv3 protocol. The SSLv3 protocol is disabled by default.	New

The SMS now supports TLSv1.2 in FIPS mode for the following: • SMS Client communication (ports 9003 and 10042) • TMC connections • Device connections • LDAP connections	New
The number of supported ciphers for SSL inspection has increased from 11 to 14. The following three cipher suites are now supported: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 To see the full list of supported cipher suites, navigate to **Profiles** > **Shared Settings** > **SSL Servers** > **New** in the SMS Client. The list of supported cipher suites automatically updates based on your protocol selections.	New
The SMS database has increased its maximum entries for the following statistics: • Historical Port Traffic Stats to 150 million • Device Traffic Data to 40 million	TIP-26599
The SMS now sends an SNMP trap to the network management console with information on which profile, DV, or other object had a distribution failure.	TIP-35736
Scheduled SMS database backups to an external NFS system no longer fail intermittently.	TIP-37132
Enterprise Vulnerability Remediation (eVR) scans now support non-ASCII characters in filenames.	TIP-35729
Profile distributions no longer fail when a DNS exception conflicts with a URL exception that has been removed.	TIP-40289
SSL inspection active session information has been removed from both the SMS and LSM.	TIP-43661
Performance issues and dropped packets occurring repeatedly after distributing profile updates has been addressed in this release.	TIP-40771
Quarantine exceptions no longer fail if they are also named resources.	TIP-33585
The documentation has been updated to clarify that users with Administrative privileges can view and clear the audit logs for TPS devices.	TIP-36496
An issue that encumbered SMS logins has been resolved.	TIP-39910

Recurring DV and profile distribution schedules and history now include a time zone so the time displayed is unambiguous. The time zone displayed matches the SMS client.	TIP-41430
The TPS and SMS interfaces no longer permit hostnames to include periods (.). Hostnames can consist only of alpha-numeric characters and hyphens, and cannot exceed 63 characters or have a hyphen at the beginning or end.	TIP-44323

Known issues

Description	Reference
Performing a backup and restore of the SMS database will not preserve Filter Performance Correlation data.	TIP-42709
After an upgrade to SMS v5.3 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
When you enable SSL inspection on a device, the SMS does not notify you that you must reboot.	TIP-43951
When you attempt to distribute too many TLS/SSL certificates to a device, the resulting error message incorrectly specifies CA certificates as the problem. Disregard the error and reduce the number of certificates.	TIP-44753
The `File System: OS` information is displayed twice in the SMS Health Statistics.	TIP-39833
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. Also restrict the characters in the name of your SSL policy to alphanumeric characters only. The use of special characters in the SSL policy name has caused profile distributions to fail, including: `& < > , :`	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

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 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
When run from the SMS client, the WHOIS command sometimes yields no results.	TIP-52081
When you use an encrypted TCP syslog, you must restart the SMS before certificate changes will go into effect.	TIP-52245

Product support

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