Security Management System Release Notes

Version 5.1

Important notes

- You can upgrade the SMS to v5.1 directly from SMS v4.4 or later. If you are upgrading from a release earlier than v4.4 you must first upgrade to SMS 4.4, log in to the SMS to activate a DV, and then upgrade to v5.1. For assistance with upgrades from older systems, contact the Technical Assistance Center (TAC).
- 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 time required to upgrade will vary based on the version from which you are upgrading and the quantity of data to migrate. Learn more.
- End of support for NGFW products was announced on December 17, 2015. SMS management support and related bug fixes and patches for NGFW management will continue through the end of support period (January 31, 2019) for the NGFW hardware; however, this SMS release has removed support for NGFW management. SMS management support for NGFW will only occur on SMS 5.0.1 and earlier. When an SMS upgrades to 5.1 all NGFW devices that are managed on it become automatically unmanaged. If you attempt to re-manage them or add a new one, an error message returns.

Upgrade limitations

- 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.

- vSMS no longer allows upgrades to systems that do not meet the minimum disk space and memory requirements. To add disk space you must redeploy your vSMS, so ensure your system meets the requirements before installing or upgrading. To upgrade, first back up your vSMS, redeploy a 5.1 vSMS, and then restore your backup. Learn more in the *vSMS Getting Started Guide*.

Product version compatibility

	SMS v5.1	SMS v5.0.x	SMS v4.6.0	SMS v4.5.0	SMS v4.4.0
TPS	TOS v5.1 and earlier	TOS v5.0.0 and earlier	TOS v4.2.0 and earlier	TOS v4.2.0 and earlier	TOS v4.1.0 and earlier
vTPS	TOS v5.1 and earlier	TOS v5.0.0 and earlier	TOS v4.2.0 and earlier	TOS v4.0.2	TOS v4.0.2
IPS	TOS v3.9.3 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

Software updates and migration

The estimated times noted in this table apply to users upgrading from SMS v4.5 and later. Users upgrading to v5.1 directly from SMS v4.4.0 will require more time; refer to the Release Notes for your v4.4.x version.

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	30 to 90 minutes[2]	Unavailable
4	Migrate report data.	Automatic	Up to 2 hours[3]	Available

—

1) Network speed determines the time to download 800+ 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.

3) The SMS is available while report data is migrating, but performance may seem slow until migration completes. When this task is complete, a message appears in the SMS Audit Log.

Release contents

Description	Reference
Structured Threat Information eXpression (STIX) 2.0 data provides open source cyber threat intelligence that can be transferred to the SMS, and now provides a Trusted Automated eXchange of Indicator Information (TAXII) 2.0 inbox service for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs). The advanced threat intelligence provided in tag categories keeps the Reputation Database updated, and enables robust reputation filters for enhanced protection of your system.	new
DoDIN APL support is included in this release. This release has been certified and meets all necessary requirements for product approvals. Learn more at https://www.disa.mil/Network-Services/UCCO. Specific enhancements related to these requirements include: ▪ SMS can now automatically disable accounts after a 35-day period of account inactivity. ▪ SMS and its authentication server will never automatically remove or disable the emergency administrator accounts. ▪ After you log in, SMS shows the number of unsuccessful login attempts since the last successful login. SMS also shows the location of the last logon (IPv4 and IPv6). ▪ When using CAC authentication the user accounts now need to exist in an Active Directory server. Learn more about authentication and user roles in the *SMS User Guide*. ▪ SMS now authenticates Network Time Protocol sources using authentication that is cryptographically based (NTPv3 using SHA1 key).	new
Added the ability to re-enable filters from SMS which have been disabled via Adaptive Filter Control (AFC). You can view a list of filters most recently affected by adaptive filtering, and in this release, you can now clear the filter, which re-enables the filter state. Go to **Devices > All Devices > Member Summary > Events**, and then select the **Adaptive Filter** tab to view or clear the list of filters.	new
SMS now automatically downloads the latest Geo IP database which correlates IP addresses to geographic locations (enabled by default). Learn more about how to disable the auto-update feature and manually import a geo package in the *SMS User Guide*.	new
You can now re-manage multiple devices, devices groups, or both at the same time.	new
URL Threat Analysis enables the SMS to automatically use the Deep Discovery (DD) Analyzer device to analyze suspicious content in HTTP traffic. Using DD Analyzer you can detect malware threats to browsing clients in your network. In this release, URL Threat Analysis uses IP, DNS, and URL data types. From Threat Insights, you can use suspicious objects to include URLs. Refer to the *SMS User Guide* to learn more about URL Threat Analysis and Threat Insights.	new
Support for accessing the SMS server using HTTP or Telnet is no longer available in this release. To access the SMS server, use HTTPS or SSH.	new

From the SMS and the device CLI, you can rename TPS physical segments, as you could for IPS physical segments, with the following restrictions: ▪ Restrict characters to letters A–Z and a–z, digits 0–9, spaces, periods (.), underscores (_), and hyphens (-). ▪ Include at least one alphabetical character. ▪ Do not begin or end the name with spaces. ▪ Do not extend a name beyond 32 characters. A new segments command in the CLI enables you to rename individual segments.	new
New or enhanced APIs Traffic management enhancements Add Reputation entries enhancements You can generate an API key on the SMS that you can use instead of your username/password to access the SMS Web API. Navigate to **Admin > Authentication and Authorization > Users** to generate (or regenerate) the API key. You must use the API key as part of the HTTP request HEADER, which appears as: `X-SMS-API-KEY: <String>` The remote device management API enables you to retrieve the Layer 2 Fallback status for a device or device group managed on the SMS. You can also put a device or device group into or out of Layer 2 Fallback. getFallback - view Layer 2 Fallback status for any device or device group on the SMS. setFallback - place a device or device group into or out of Layer 2 Fallback. New STIX/TAXII API which provides a TAXII 2.0 Inbox Service that supports adding STIX 2.0 IP, DNS, and URL IoCs to the SMS Reputation database. Learn more in the *SMS Web API Guide*.	new
To provide improved search results, the Reputation Type criteria now appears as a combo box field with the following options: All, Both Reputation and Geographic, Reputation Only, Geographic Only, and Non-Reputation.	new
Issues with logging in to an SMS HA cluster from the SMS client have been addressed in this release. Users no longer need to disable HA before logging in.	120407
If you enter a comma in the Organization (O) field when filling out a CSR (**Admin > Certificate Management > Signing Request**), an error no longer returns.	120841 123776
The **View Packet Trace** button no longer appears grayed out in the Event Details when a Packet Trace exists.	121261 120514

Entries with the same start address were merged in search results causing searches of the Reputation database on SMS (**Profiles > Reputation Database > Search Entries**) for database entries that match a reputation filter's criteria to yield no matching results. If the same criteria used to create the filter is entered into the search criteria, matching results are now returned.	121255
The system now checks for users who do not meet the authentication security level standard, and requests them to change their password at the next login.	107705
Attempts to activate new DVs became suspended while the SMS waited for sufficient memory to accommodate long strings, resulting in an out of memory error in the logs. This issue has been addressed and the error no longer appears.	121094
Activating a Digital Vaccine (DV) or an Auxiliary DV from the SMS no longer fails, and does not require that you turn off high availability or un-manage devices.	121877 (122870)
Errors no longer occur when removing a filter override after activating a DV that had deleted that filter. Previously this occurred because the deleted filter override remained in the device package, causing a package mismatch. Learn more in Product Bulletin 1078.	123030
Manually entering an IP/DNS reputation entry to the SMS is now processed so that deleted values and tables no longer remain in the database causing unpredictable results.	122763 (120619)
Entitlements now lists the SMS in addition to all devices.	120970
Changing the device hostname using the SMS client no longer reverts back to the original name on the SMS.	122868
Several improvements in disk space management are available in this release.	113122
SMS health warnings no longer occur inappropriately on HP G9 platforms; threshold values for temperature have been adjusted to align with BIOS: "Thresholds: Major/Critical 85 / 90 C"	123522
Options selected during a scheduled backup now remain checked if selected. Previously, if the Include Private Keys option was selected, private keys were included in the backup correctly but the SMS showed the option as unselected.	121402

The Reputation database search engine now returns a complete list of entries according to the search criteria.	120814
When performing an action with filters enabled on columns in a table, an error is no longer returned and results are refreshed appropriately.	107555 (120779)
You can now save a profile search if one of the included filter criteria is 'Filter Released' or 'Filter Last Modified'.	120963
When used as a hostname, a fully qualified domain name can now extend to 64 characters.	106043
You can now select multiple DVs from the **Profile > Digital Vaccines** page and the **Auxiliary DVs** page.	113331
The results of a DV packages search are now sorted with the most current DV package listed at the top.	117792
CVE 2015-1379 was mitigated and addressed in this release.	121065
The error message resulting from attempts to delete a named resource that is in use now includes the profile name.	120419
An error returns if you attempt to edit an action set with a rate limit that is unsupported. The acceptable rate limit range is 0.05 – 2000 Mbps.	122664
Filters referencing CVEs now have updated and corrected external links to mitre.org.	123346
On TPS devices, you can now change the name of system-defined segments and virtual segments.	116818
In the **Edit System Preferences** menu, disabling an inactive user account has been extended to 365 days.	120944
SMS no longer returns an error indicating a reboot is necessary to activate a pending certificate when a user does not have the correct permissions for Web SSL certificates.	120658
Reputation and profile distributions now appear separately in the Distribution Progress. When a reputation filter distribution fails, a new error is returned: "Failed reputation database distribution ($device_name)."	121896

Performance graphs and bandwidth usage graphs no longer show breaks in data for TX systems that had resulted from duplicate polling data.	124025 (123961)
The time to complete a profile distribution no longer significantly increases after DV activation with no service changes.	123024
Information such as country, type, and score for DNS reputation events is now included in the Block or Audit logs.	123021

Known issues

Description	Reference
A filter comment search returns results only if the search contains a consecutive string of alphanumeric characters with no spaces or special characters.	121433
In environments with high reputation activity and a large number of devices, it is possible to have a distribution failure with a `Too many open files` error. If you encounter this issue, contact product support for a hotfix.	124848
If you change the SNMP community string from 'public' you must reboot the SMS in order to restart SNMP services.	123299
SMS sends unreadable characters in the audit log entries to the remote syslog server.	123383
An issue in which reports containing un-escaped special characters has been addressed. However, reports created in SMS 5.0.1 or earlier will still contain this problem after migrating to v5.1. To work around this issue, re-create the report from v5.1.	123973
When you run a **Device Traffic – IPS Physical Port** report for a device group in which one of the devices has been replaced, the system generates an empty report when you identify the IPS device by name instead of specific ports. To work around this issue, run the report from specific segments or run reports using **IPS Devices – Events – Traffic**.	120815
Although SMS allows you to add more than 1024 SSL policy exceptions by using groups, this results in a deployment failure. Limit policy exceptions to 1024 for the best performance.	124581

Although SMS allows you to enter DNS domain names that exceed the 254 limit by 1 character, this returns an error on the device. Do not enter domain names longer than 254 characters.	124189
You are unable to unlock advanced DDos filters from the SMS interface since the OK button appears grayed out. To work around this issue, delete the filter or save it as a new filter.	124599

Product support

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