TippingPoint

Security Management System Release Notes

Version 4.3.0

September 2015

This document contains release-specific information for the HP TippingPoint Security Management System (SMS). The *Security Management System Release Notes* describe new features and changes for an SMS release.

This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining HP TippingPoint SMS appliances and associated devices. This document includes the following sections:

Overview

This document contains important information for installing and using the SMS version 4.3.0 release. Read through all preparation instructions and safety requirements before installing your HP TippingPoint product.

Note: To ensure that you have the latest version of the release notes and other product documentation, download these documents from the Threat Management Center (TMC) at https://tmc.tippingpoint.com, or contact your HP TippingPoint representative.

New and changed in this release

SMS version 4.3.0 improves support for HP TippingPoint Next Generation (NGFW), Intrusion Protection System (IPS), and Threat Protection System (TPS). SMS provides management capabilities for your NGFW, IPS, and TPS devices, including:

- Support for NGFW TOS v1.2 and earlier

- Support for IPS TOS v. 3.8.1 and earlier
- Support for TPS TOS v. 4.0.0

See Product Version Compatibility on page 5 for additional information about which HP TippingPoint product versions are compatible.

Threat Protection System devices

A Threat Protection System (TPS) device is a high-performance, enterprise-class solution that offers the option of deploying as a Next Generation Firewall (NGFW) appliance or as an Intrusion Prevention System (IPS) device. During the out-of-box-experience (OBE), you specify whether your device will function as an NGFW or as an IPS. After you make the selection, only those features of the selected mode are available.

If you later decide you want the other mode instead, you can redeploy the device by running the OBE again and selecting the other mode. The TPS device must be version 4.0.0 or later. To manage the TPS device, the SMS must be version 4.3.0 or later.

- **NGFW deployment** — Offers a sophisticated and comprehensive defense against network invasion, proliferation of unauthorized application use, and business interruption at critical access points, including the network perimeter. When the TPS device is deployed in this mode, it includes many of the same features that are included in the HP S1000 Series.
- **IPS deployment** — Protects your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device. With an IPS deployment, the TPS device is optimized for high resiliency, high availability, and network segment protection from both external and internal attacks. When the TPS device is deployed in this mode, it includes many of the same features that are included in the S-Series devices.

Before you can add a TPS device to the SMS as a managed device, you must install and configure the components and run through the OBE Setup Wizard. For more information, refer to the *440T Threat Protection System Hardware Specification and Installation Guide*. To add a TPS device to the SMS, refer to the "Adding, editing, or deleting a device" section of the *SMS User Interface Guide*.

DV Toolkit Packages

Digital Vaccine Toolkit (DV Toolkit) enables you to create custom attack filters that can be used to detect and prevent network intrusions. Our latest round of SMS features and enhancements makes it even easier to get value out of your DV Toolkit filter packages, fast.

What's new in version 4.3.0:

- Ability to activate and distribute a new DV Toolkit package on the SMS without losing filter overrides on existing DV Toolkit packages.
- Support for multiple, active DV Toolkit packages on the SMS. Although the SMS supports multiple packages, you can only import a specific DV Toolkit package once.

- Ability to use role-based access control for DV Toolkit packages. Multitenancy allows you to supercharge your users' productivity with the right DV Toolkit packages to the right users at the right time.

  Note: For more information on how to use this feature, see the *Digital Vaccine Toolkit* section under *Profiles* in the *SMS User Guide*.

  Note: When creating an Inspection Profile, if you want to override DV Toolkit filters, you should not use category settings.

Activate and distribute a new DV Toolkit package without losing filter overrides for existing DV Toolkit packages

When you import a new DV Toolkit package, select the **Activate the imported DV Toolkit package** check box to overwrite an existing, active filter package. The SMS keeps all existing profile filter overrides for the overwritten package.

Activate multiple DV Toolkit packages on the SMS

In version 4.3.0, you can activate as many DV Toolkit packages on the SMS to meet your specific needs. You can merge DV Toolkit packages without using the DV Toolkit application--these changes are made automatically and happen behind the scenes. When you distribute the packages to the device, the SMS merges multiple DV Toolkit packages into a single package as the device only supports one DV Toolkit package.

Use multitenancy to limit access to DV Toolkit packages

The SMS now supports role-based access control for DV Toolkit packages. With multitenant DV Toolkit packages, multiple users can have separate, active DV Toolkit packages running on the same SMS. Access control lets you independently customize access rights and restrictions for each user based on role and group settings. As a result, you can set up DV Toolkit packages that only a certain group of users can see.

To limit access to DV Toolkit packages, go to **Admin** > **Authentication and Authorization** and then:

- Create (or edit) a role and set capabilities for DV Toolkit Management.
- Create (or edit) a group for each role and set which DV Toolkit packages the group can access.
- Create (or edit) a user and assign the group to the user.

Note: For more information on role-based access control, see the *Admin* section in the *SMS User Guide.*

DV Toolkit packages best practices

Make sure you review our recommended best practices to ensure your continued success.

Remove DV Toolkit packages from the device and the SMS

Removing DV Toolkit packages from the device and the SMS involves these steps:

1. Deactive the DV Toolkit package on the SMS.
2. Redistribute the profiles that have filter overrides from the DV Toolkit package to the device(s).

3. Uninstall the DV Toolkit package from the device.
4. Delete the DV Toolkit package from the SMS.

If you deactivated or deleted a DV Toolkit package from the SMS that you want to uninstall from the device, you must re-import the package and then uninstall it from the device

Edit multiple device configurations

In version 4.3.0, you can now edit different device configurations at the same time. When you make device changes, the SMS lists every device that is being modified. You can use the icons located in the Device Configuration wizard to quickly see if the information for a category applies to an IPS devices or an NGFW appliance. A binoculars icon () indicates that the information applies to an IPS device. A fire icon () indicates that the information applies to an NGFW appliance. The number in the parentheses indicates the number of devices. On any Device Configuration screen, you can hover your mouse over the binoculars and fire icons to the respective fields.

Export user-provided Reputation entries

With SMS version 4.3.0, you can export user-provided Reputation entries to a comma-separated value (CSV) file. Exporting Reputation entries enables you to have more control over the user-provided Reputation entries. You can capture the state of the Reputation database and then quickly restore it at a later time.

PCAP retrieval

Retrieving PCAPs from managed devices changed in SMS 4.3.0. In version 4.3.0, the SMS retrieves the most recent PCAPs first and then works backward to retrieve older PCAPs. This change ensures that newer PCAPs are downloaded by the SMS even if a device accumulates PCAPs at a rate faster than the SMS can retrieve them. If the SMS cannot retrieve all PCAPs from the device, the SMS will generate a message in the system log.

SMS displays the updated filter name for overridden filters

The TippingPoint DVLabs security team develops new attack filters to address vulnerabilities and incorporates these filters into Digital Vaccines. Digital Vaccines are delivered to customers weekly. When critical vulnerabilities and threats emerge, they are delivered immediately. New filters are continuously fed to the SMS to keep it up-to-date against the latest vulnerabilities. Each filter can be thought of as a virtual software patch that is created within the network to protect downstream hosts for attack. As more information becomes available, the filter name may change.

In version 4.3.0, the SMS displays the updated filter name (within a Digital Vaccine package) for filter overrides.

Vulnerability converters

SMS version 4.3.0 includes two new vulnerability scan converters by default:

- Rapid7 (Nexpose XML 2.0 format)
- Qualys (csv format)

Web API

For SMS version 4.3.0, the Web API version is now 2.2.

Installation

For installation instructions, refer to the *HP TippingPoint SMS Quick Start* or the *Read Me First* documents.

Product version compatibility

The following table lists all compatible versions of the NGFW, IPS, TPS, and Identity Agent devices with different SMS versions.

Important: The SMS client will not connect or automatically prompt you to upgrade when the SMS server is upgraded to version 4.3.0. You must use the web browser to download and install the 4.3.0 client.

	SMS v4.3	SMS v4.2	SMS v4.1	SMS v4.0	SMS v3.6
NGFW	TOS v1.2.0 and earlier	TOS v1.1.1 and earlier	TOS v1.1 and earlier	TOS v1.0	Not supported
IPS	TOS v3.8.1 and earlier	TOS v3.8.1 and earlier	TOS v3.7.1 and earlier	TOS v3.6 and earlier	Only TOS v3.6 and earlier
Identity Agent	v1.0.0	v1.0.0			
TPS	TOS v4.0.0				

Software updates and migration

SMS and vSMS upgrades are supported from version 3.6. We recommend that you are running at least SMS version 3.6 before you upgrade to SMS version 4.3.0. For details on the migration path, refer to the SMS version 3.6 Release Notes.

You must allow background processes to complete before you begin migration to SMS version 4.3.0.

SMS FIPS

You must disable FIPS on the SMS before you upgrade to SMS version 4.3.0. Changes made to the SMS FIPS certification from earlier versions require you to perform this configuration step before you migrate to SMS 4.3.0, or the upgrade will fail.

After you complete the migration to SMS 4.3.0, you can enable FIPS.

Backup and restore the SMS database

Because FIPS certification changed in SMS version 4.3.0, we recommend that you disable FIPS before you back up the SMS database. After you complete the migration to SMS 4.3.0, you can initiate the restore process while FIPS mode is disabled. After the restore completes, you can then enable FIPS mode. If you do not follow this process, the database restoration process will fail.

Historical events

To migrate historical event data for an SMS upgrade, you must have at least 20 GB of free space in the database partition. If space is unavailable, the upgrade process ends, and a message warns you that cleanup is required.

You may be able to free space by deleting old device snapshots, saved reports, profiles, or DV and TOS packages. Otherwise, contact HP TippingPoint Support for detailed cleanup instructions. The SMS client shows the current state of the partition (File system: Database) on the System Health screen of the Admin workspace.

The number of Max Rows for Historical Events data changed in SMS 4.3.0. Use the following table to view the Max Rows values by device for SMS 4.3.0 and later versions.

	H3	H3 XL
SMS 4.2.1	200,000,000	500,000,000
SMS 4.3.0	200,000,000	600,000,000

When a system is migrated from SMS 3.5 to 3.6 or later, results from saved reports are written to an archive file, 3.5SavedReport.tar.gz, and will no longer be available from the SMS Client. The archive file is saved for 60 days; after 60 days, the tar file is deleted automatically during a file cleanup process.

Depending on the quantity of event data to be migrated, the time necessary to upgrade might be longer than expected.

Step	Task	Manual/automatic	Estimated time	SMS status
1	Download upgrade package	Manual	Varies[A]	Available
2	Install upgrade package	Manual	2-10 minutes	Unavailable
3	Migrate data	Automatic	Up to 4 hours[B]	Unavailable
4	Migrate report data	Automatic	Up to 2 hours[C]	Available

Notes

A Network speed determines the time to download 600+ MB file.

B Depends on the amount of event data to be migrated. 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.

C The SMS is available while report data is being migrated, but performance may seem slow until migration completes. When this task is complete, the SMS Audit Log shows the message: “Migrate alerts from version 3.5.0.0 to version 3.6.0.0.”

Beginning with version 3.5, the SMS uses Password Authentication Protocol (PAP) by default. While using PAP, the AUTH-REQUEST sent by the SMS to the RADIUS server includes three attributes: User-Name, User-Password, and Message-Authenticator.

If the RADIUS server requires attributes that the SMS does not provide, SMS users with RADIUS authentication type can no longer log in. As a workaround, make temporary changes on the RADIUS server to remove restrictions that the AUTH-REQUEST include other attributes.

Authentication protocol options for RADIUS include PAP, MD5, and PEAP/EAP-MSCHAPv2.

Note: As a general best practice, a local user should always be enabled and added on the SMS.

Clarifications and known issues

The following summaries, grouped by category, provide clarification or describe known issues for the SMS.

Admin

Device	Description	Reference
SMS	When the SMS is in FIPS Crypto Core mode, if you import an SMS Web Security SSL Certificate and then import a RADIUS certificate without restarting the SMS, the SMS will display a `NullPointerException` error message. **Workaround**: After you import an SMS Web Security SSL Certificate, restart the SMS before you import a RADIUS certificate.	101767
SMS	When the SMS is in FIPS Crypto Core mode, if you import an SMS Web Security SSL Certificate, the following certificate information will not be updated until you restart the SMS: • Subject DN • Valid After • Expires **Workaround**: Restart the SMS after you import an SMS Web Security SSL Certificate.	101302
SMS	After a backup is restored, the status continues to show that the backup is in progress. **Workaround**: This status can be ignored.	104680

Devices

Device	Description	Reference
SMS, NGFW	When you configure PPP interfaces (PPTP, PPPoE, L2TP), there may be minor differences that display in the SMS and the CLI and LSM of the NGFW appliance. **Workaround** To remove the password, remove the user id.	104416
SMS, TPS	If you unmanage the device and then edit a user role in the LSM, the role capabilities do not display in the SMS when you remanage the device. **Workaround**	104684

Device	Description	Reference
	If you use the LSM to edit a user role that was originally created in the SMS, you must always use the LSM to edit that user role.	
SMS	When Enabling and Disabling Network ports on TPS devices, the SMS does not refresh the port list as frequently as it does on IPS devices. TPS devices do not send SNMP traps to the SMS. The SMS periodically polls the TPS device to get the status. There may be a delay (up to one minute) before the SMS displays the TPS device state.	104911
SMS, NGFW	You can create a device user group with a role of "none." This role has no capabilities.	105107
SMS, NGFW	Sometimes after you reboot the NGFW appliance, the SMS client may still indicate that the NGFW is rebooting even though the reboot is complete. **Workaround** Manually refresh the NGFW appliance by clicking the **Refresh** button in the SMS client.	105939

Events

Device	Description	Reference
SMS	You cannot save an IPS event query when the firewall profile is included in the query.	105963

Profiles

Device	Description	Reference
NGFW	After you import a Reputation profile from an NGFW appliance, the SMS displays an error when you attempt to edit or distribute a Reputation filter. When you perform a filter search, the Reputation filter does not display in the profile filter summary or the profile search results. **Workaround** Create a new Reputation profile with reputation entries in the SMS.	105008

Device	Description	Reference
SMS	When you uninstall a Malware Filter Package from devices, the DV Inventory screen incorrectly reports that the uninstall failed on one device. **Workaround** This display issue can be safely ignored. Logging out and logging back in will show that the package is removed from all devices.	105246
SMS	A refresh issue makes it appear that the `Malware Filter Package Update` allows more than one Malware Filter Package to be active. **Workaround** This display issue can be safely ignored. Logging out and logging back in will show that only one package is active.	105344
SMS	When you import a profile from a device that has nonstandard service ports, the SMS updates inspection services for each profile and changes the version and modified dates for all the profiles on the SMS.	105964
SMS	When an Admin user copies a profile using a **Save As** operation, the Admin user will not have access to the copied profile until a SuperUser gives the Admin user access. **Workaround** The SuperUser can give the Admin user access to the copied profile. Alternatively, the Admin user can access the profile by exporting and then importing it.	106325

SMS client

Device	Description	Reference
SMS	The SMS client will not connect or automatically prompt you to upgrade when the SMS server is upgraded to version 4.3.0. **Workaround** You must use the web browser to download and install the 4.3.0 client.	102535

Reports

Device	Description	Reference
SMS	Scheduled executive reports display a `malformed URL exception` error for some Reputation IP addresses every time the report is generated.	101524
SMS	When you generate an executive report, the event query will display an inaccurate query structure.	103620
SMS	After you create a report schedule you cannot make modifications to the schedule. **Workaround** Delete the existing schedule and create a new schedule with modified criteria.	105349
SMS	When you generate a Specific Country report (**Inspection** > **Security** or **Inspection** > **Application**), or when you generate an Inspection report (Security or Application) and the report has country criteria, if you click a link in the report, you cannot use the **Refresh** button on the Events panel until you restart the SMS client.	106322

DV Toolkit

Device	Description	Reference
NGFW	When you distribute a firewall profile to an NGFW appliance, a mismatch warning may display even though the SMS and NGFW appliance have the same DV Toolkit package. **Workaround** This warning can be safely ignored.	104445
SMS	Depending on the number of DV Toolkit packages on the device, the Device Configuration (Management Information) may not display all of the package names. **Workaround** You can see the complete list of DV Toolkit packages for the device on the Device Configuration Summary.	104856

Device	Description	Reference
SMS, NGFW	You may notice a version error and exception when you distribute the same DV Toolkit package to NGFW devices in a cluster. **Workaround** Uninstall the DV Toolkit from each NGFW device of the cluster, select the cluster on the Devices screen and click **Sync Configuration Now**. Then redistribute the DV Toolkit packages back to each NGFW cluster device.	105136
SMS	When you distribute a DV Toolkit package to all devices, the package appears inactive on the DV Toolkit Details screen. **Workaround** To refresh the DV Toolkit Packages status, select a package that is already active in the Device DV Toolkit Inventory table, and then click **Activate** to activate it again. This re-syncs the packages. Alternatively, log out and log back in to the SMS client.	105480
SMS	When you override DV Toolkit Packages and distribute them to the device, the filter names in the DV Toolkit package on the device are different from the filter names that display on the SMS. For example, if a DV Toolkit package has a filter named `C031 Snort Rule`, the device displays the filter name as `C1000001 Snort Rule`.	105570
SMS	After you import a new DV Toolkit package (with the **Activate the imported DV Toolkit package** check box selected to overwrite an existing, active filter package), the Device Summary screen does not display the name of the new DV Toolkit package. **Workaround** After you distribute the overwritten DV Toolkit package to the device, the Device Summary screen will display the correct name of the package.	105789
SMS	The DV Toolkit package displays `unknown` on the DV Toolkit Distribute dialog box when you distribute a different DV Toolkit package to the device. `Unknown` displays because you do not have access to this package.	105846
SMS	Sometimes you must uninstall the DV Toolkit package twice for a DV Toolkit package to be uninstalled. **Workaround**	105891

Device	Description	Reference
	Uninstall the DV Toolkit package when there is no DV Toolkit distribution in progress.	
SMS	Sometimes if you have several individual DV Toolkit distributions happening to the same device at the same time on the SMS, some DV Toolkit packages may not be distributed to the device. When this happens, the Distribution Extended status does not list the DV Toolkit package that was not distributed to the device. This situation may also happen if you are uninstalling multiple DV Toolkit packages from the same device. **Workaround** Select multiple DV Toolkit packages (instead of individual DV Toolkit packages) and then redistribute the packages to the device.	106058, 106350, 105492
SMS	When you distribute a DV Toolkit package, the device system log shows a different package ID than is shown in the SMS system log. **Workaround** The device system log reflects the merged packet ID. This discrepancy can be ignored because there is no functional impact.	106097
SMS	When you distribute a DV Toolkit package that has several filter overrides, an `isValid: Signature` message displays in the device log if there are differences between the profile and DV Toolkit package. **Workaround** Unistall the DV Toolkit package from the device and redistribute the DV Toolkit package to the device. Then redistribute the profile. If you are unable to uninstall the DV Toolkit package from the device, restart the SMS client.	106236

Additional information

The following information applies to the SMS version 4.3.0 release.

Product name change

Reputation Digital Vaccine, also referred to as Reputation DV or Rep DV, has begun transitioning its product name to Threat Digital Vaccine or ThreatDV.

While the product name changes across products, documentation, and webpages, you can use the following table to map previous product names to their new names:

Old Name	New Name
Reputation Digital Vaccine	Threat Digital Vaccine or Reputation Feed
Reputation DV	ThreatDV or Reputation Feed
RepDV	ThreatDV or Rep Feed
RepDV Query Portal	Rep Search
Anti-Malware Digital Vaccine	Malware Filter Package
Anti-Malware DV	Malware Filter Package
Anti-Malware Filters	Malware Filters
MalwareAux	Malware
DVLabs Malware Protection Auxiliary DV	Malware Filter Package Update

Windows XP support has ended

Support for Windows XP is discontinued as of version 4.3.0. HP TippingPoint support will not investigate issues related to Windows XP after this date.

Customer support

HP TippingPoint is committed to providing quality customer support for all of its products. If you need customer support, contact the HP support center for your product. You can find the customer support contact information for your product in the Read Me First document that is in your product shipment. The Read Me First document is also available on the HP TippingPoint Threat Management Center (TMC).

If this is your first purchase of an HP TippingPoint product, contact customer support to register your product and access online support.

Self-service portal

HP provides an online self-service portal for HP TippingPoint customers. The Self-Service Portal provides a tool for customers to manage their support cases. After registering for an account, you can submit new technical support cases and manage existing ones. For more information about accessing the online Self-Service Portal, refer to the *Read Me First* document.

Contacting support

To expedite your support request, please take a moment to gather some basic information from your records and from your system before contacting customer support. For example, your support representative may need your device serial number and the versions of your product software to assist you. For additional details about contacting support and gathering needed information before contacting support, refer to the *Read Me First* document.

HP website

For the name of the nearest HP authorized reseller, see the Contact HP Worldwide website:

http://www.hp.com/country/us/en/wwcontact.html

Legal and notice information

HP TippingPoint Security Management System Release Notes Version 4.3.0

Publication Part Number: B09152011