



TippingPoint™

Security Management System Release Notes

Version 4.5.0 Patch 1

Release date: January 2018

This document contains release-specific information for the TippingPoint Security Management System (SMS). The release notes describe new features and changes included in this release. This document is intended for system administrators, technicians, and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint SMS appliances and associated devices.

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 TippingPoint representative.

This document contains the following important information:

- *New and changed in this release* on page 1
- *Resolved issues* on page 2

New and changed in this release

This document contains information on issues and updates specific to SMS v4.5.0 Patch 1, described in *Resolved issues* on page 2.

For information on new features in SMS v4.5.0, refer to the SMS documentation located on the TMC at <https://tmc.tippingpoint.com/>.

Important note for users of the SMS Web API authenticating with URL encoded credentials

This patch changes what data SMS debug logs include when logging web access requests to exclude those credentials. For details on this change and best practices, refer to [PB#1071](#).

Important notes for SMS

- Patch installation should take approximately 15 minutes. During installation, the SMS client will become unresponsive; do not cancel the operation or reboot the SMS. The SMS Server will automatically reboot after the patch is installed. You will then be prompted to update the SMS client.
- A patch may be rolled back or uninstalled to the previous version.

- If your SMS system is operating in High Availability (HA) mode, you are no longer required to break HA to apply this patch.

Resolved issues

The following items, grouped by category, provide clarification or describe issues fixed in this patch.

Admin

Device	Description	Reference
SMS	The remote syslog has been enhanced with new format options.	116903
TPS	The SMS was unable to retrieve remote syslog events and packet capture (PCAP) files when the SMS received an IPS event from a TOS v4.5.0.1 device.	113370

Devices

Device	Description	Reference
SMS, TPS, IPS, Core Controller	<p>When HA is disabled in an SMS cluster, an API that changes the SMS serial number would get called by the Passive peer instead of by the Active peer. All managed devices would then appear to be managed by both SMS devices in the HA cluster.</p> <p>This patch resolves this issue.</p>	118005
SMS, IPS	<p>Optimized IPS Quarantine synchronization between the SMS and managed devices.</p> <p>Resolved an issue with a permitted address that caused the IPS Quarantine action to stop sending new automatic quarantines.</p>	117297
SMS	After a device refresh, the order of the devices on the Devices page became rearranged. This complicated device management, especially in environments with hundreds of managed devices.	116323

Device	Description	Reference
	The arrangement of the devices on the Devices page no longer changes after a refresh.	

Profiles

Device	Description	Reference
SMS	<p>Attempts to distribute a digital vaccine (DV) package to a single managed device resulted in the package being distributed to all managed devices.</p> <p>This patch resolves this issue.</p>	120308
SMS	An issue that caused a table (related to the Reputation feature) to fill up and the SMS to slow down or hang during device discovery or profile distribution has been repaired.	118407

Web API

Device	Description	Reference
SMS	Added a delete option to the SMS Web API. This option allows the user reputation entry to remove the entry by using a file that contains reputation entries.	116170

Product support

Information for you to contact product support is available on the TMC at <https://tmc.tippingpoint.com>.

Legal and notice information

© Copyright 2018 Trend Micro Incorporated. All rights reserved. TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. TippingPoint Reg. U.S. Pat. & Tm. Off. All other company and/or product names may be trademarks of their respective owners.

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced in any form or by any means, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

Edition: January 2018