



# 4.6.0 TippingPoint™ Security Management System (SMS)

Advanced Threat API Guide



TippingPoint™

# Security Management System Advanced Threat API Guide

Version 4.6.0

May 2017

## **Legal and notice information**

© Copyright 2017 Trend Micro

Trend Micro 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 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, or translated into another language without the prior written consent of Trend Micro. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro 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 shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint®, the TippingPoint logo, and Digital Vaccine® are registered trademarks of Trend Micro. Vertica Copyright © 2016 Hewlett Packard Enterprise Development Company LP. All other company and product names may be trademarks of their respective holders. All rights reserved. This document contains confidential information, trade secrets or both, which are the property of Trend Micro. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint Security Management System Advanced Threat API Guide

# Contents

<b>About this guide.....</b>	<b>1</b>
Target audience.....	1
Related documentation.....	1
Conventions.....	1
Product support.....	2
<b>Advanced threat protection integration &amp; reputation overview.....</b>	<b>3</b>
SMS integration.....	3
Reputation database.....	3
Predefined reputation tag categories.....	3
Reputation filters.....	5
Profiles.....	5
<b>SMS Reputation Management API.....</b>	<b>6</b>
Integrated environment.....	6
<b>Network enforcement &amp; policy management using ATP device data.....</b>	<b>7</b>
Transforming reputation entries into distributed policy.....	7

# About this guide

This guide provides integration information for ATP devices with the TippingPoint Security Management System (SMS) alongside one or more inline TippingPoint IPS and TPS devices.

This section includes the following topics:

- *Target audience* on page 1
- *Related documentation* on page 1
- *Conventions* on page 1
- *Product support* on page 2

## Target audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Network security
- Routing

## Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at: <https://tmc.tippingpoint.com>. The documentation generally includes installation and user guides, command-line interface (CLI) references, safety and compliance information, and release notes.

## Conventions

This information uses the following conventions.

### Typefaces

TippingPoint uses the following typographic conventions for structuring information.

Convention	Element
<b>Bold font</b>	<ul style="list-style-type: none"><li>• Key names</li></ul>

Convention	Element
	<ul style="list-style-type: none"> <li>Text typed into a GUI element, such as into a box</li> <li>GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click <b>OK</b> to accept.</li> </ul>
<i>Italics font</i>	Text emphasis, important terms, variables, and publication titles
<b>Monospace font</b>	<ul style="list-style-type: none"> <li>File and directory names</li> <li>System output</li> <li>Code</li> <li>Text typed at the command-line</li> </ul>
<i>Monospace, italic font</i>	<ul style="list-style-type: none"> <li>Code variables</li> <li>Command-line variables</li> </ul>
<b>Monospace, bold font</b>	Emphasis of file and directory names, system output, code, and text typed at the command line

## Messages

Messages are special text that is emphasized by font, format, and icons.

**⚠️ Warning!** Alerts you to potential danger of bodily harm or other potential harmful consequences.

**⚠️ Caution:** Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

**Note:** Provides additional information to explain a concept or complete a task.

**Important:** Provides significant information or specific instructions.

**Tip:** Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

## Product support

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

# Advanced threat protection integration & reputation overview

The SMS Reputation Management API uses intelligence from advanced threat protection (ATP) devices to provide in-line blocking at wire speed with TippingPoint Intrusion Prevention System (IPS) and Threat Protection System (TPS) devices. This provides an advanced layer of protection to prevent advanced malware from communicating to command/control systems, non-patient zero infections, and prevent malware from spreading.

## SMS integration

An ATP device integrated in an SMS environment can help your customers disrupt malware communications, isolate infected resources, and protect critical resources. The integrated environment enables flexible action and enforcement options based on advanced threat-provided metadata and reputation data from Digital Vaccines (DVs) and the reputation database.

An integrated environment enables customers to take enforcement actions, such as:

- Block against command and control network traffic generated by malware source.
- Send notifications when an infected host attempts to initiate communications.
- Quarantine an infected host.
- Block network traffic against malware source.

The ATP device uses the SMS Reputation Management API to connect with the SMS, enabling the device to trigger reputation events.

## Reputation database

The TippingPoint *reputation database* is a collection of IP addresses and DNS names on an SMS that represents potential risks to network security. The reputation database contains entries that are predefined on the SMS, are user-generated, or are contained in reputation DVs. The entries in the reputation database are used to create reputation filters that target specific network security needs. See [Reputation filters](#) on page 5.

## Predefined reputation tag categories

The SMS incorporates predefined tag categories from ATP devices. The advanced threat intelligence provided in these categories keeps the Reputation Database updated and enables robust reputation filters for enhanced protection of your system.

You can either configure your ATP device to send this data automatically to the SMS (as a tag entry), or you can use the SMS to manually add or import the entries. To configure this integration from your ATP device, refer to the ATP device documentation on the Trend Micro documentation site. To add these entries manually, you must define the tag categories listed in the following table so that the specific data you need can be mapped to the SMS.

**Important:** Only users with SuperUser permissions should manually add the predefined tag categories. For more information on account settings, see *Authentication and authorization* in the *Security Management System User Guide*.

The SMS automatically includes the following predefined tag categories.

**Table 1. Predefined reputation tag categories**

Name	Type	Settings	Notes
Trend Micro Detection Category	List	Pre-defined values of: <ul style="list-style-type: none"> <li>Suspicious Object</li> <li>C&amp;C Callback Address</li> </ul>	Specifies which category the detection falls under.
Trend Micro Publisher	Text	Up to 255 characters	Can be used to identify the Trend Micro product name that discovered the threat.
Trend Micro Severity	List	Pre-defined values of: <ul style="list-style-type: none"> <li>High</li> <li>Medium</li> <li>Low</li> </ul>	Identifies the threat severity.
Trend Micro Source	Text	Up to 255 characters	Can be used to identify the configured host name of the Trend Micro device that discovered the threat.

# Reputation filters

A *reputation filter* associates an action set (defined on the SMS) with one or more entries in the Reputation Database. An *action set* determines how the system responds when a packet triggers a filter. Default actions include *Block*, *Permit*, *Notify*, and *Trace*. The SMS client also enables you to create custom action sets that include *Quarantine* and *Rate Limit*.

When the reputation filter is distributed to a device, the specified actions are applied to traffic that matches the tagged entries in the reputation database. When you create a reputation filter using a predefined tag category from the reputation database, any address associated with the tag category is included in the filter.

**Note:** Reputation filters are created on the SMS and distributed to SMS-managed devices.

# Profiles

A *profile* is a collection of filters or rules that enable you to set up security configuration options for TippingPoint solutions. Profiles enable you to distribute filters to multiple devices, specific devices, physical segments controlled by a specific device, or even virtual segments.

Profiles are created and modified through the SMS client, which is also used to distribute profiles to managed devices. Each profile can be distributed separately, to specific devices. When a profile is distributed, it includes shared settings (such as action sets, notification contacts, and services) as well as associated filters and filter setting modifications.

# SMS Reputation Management API

The following information describes the initial network topology, method for importing reputation entries into the Reputation Database, the reputation import record format, and performance guidelines.

It should be noted that Reputation Management is one portion of the SMS Web API. For more information about the full external SMS API, refer to *TippingPoint Security Management System External Interface Guide* included in the latest SMS release.

## Integrated environment

In the proposed integrated environment, an out-of-line ATP device is connected to the your LAN environment with a switch. The switch is configured to replicate traffic from one port to another port so that you can allow pass-through traffic and redirect duplicate traffic to the ATP device.

The SMS Reputation Management API enables an ATP device to connect with the SMS through a secure Web interface, enabling the ATP device to update the reputation database. This allows you to leverage advanced threat intelligence to create reputation filters and better protect your systems.

**Note:** When interfacing with the SMS programmatically, the client must be able to trust the certificate on the SMS, whether it is self signed or signed by an outside source.

# Network enforcement & policy management using ATP device data

The information in this section describes tasks required to use reputation entries to build reputation filters which are distributed to managed devices.

This information allows you to leverage ATP device data in an integrated environment and to set up the following responses to reputation event triggers:

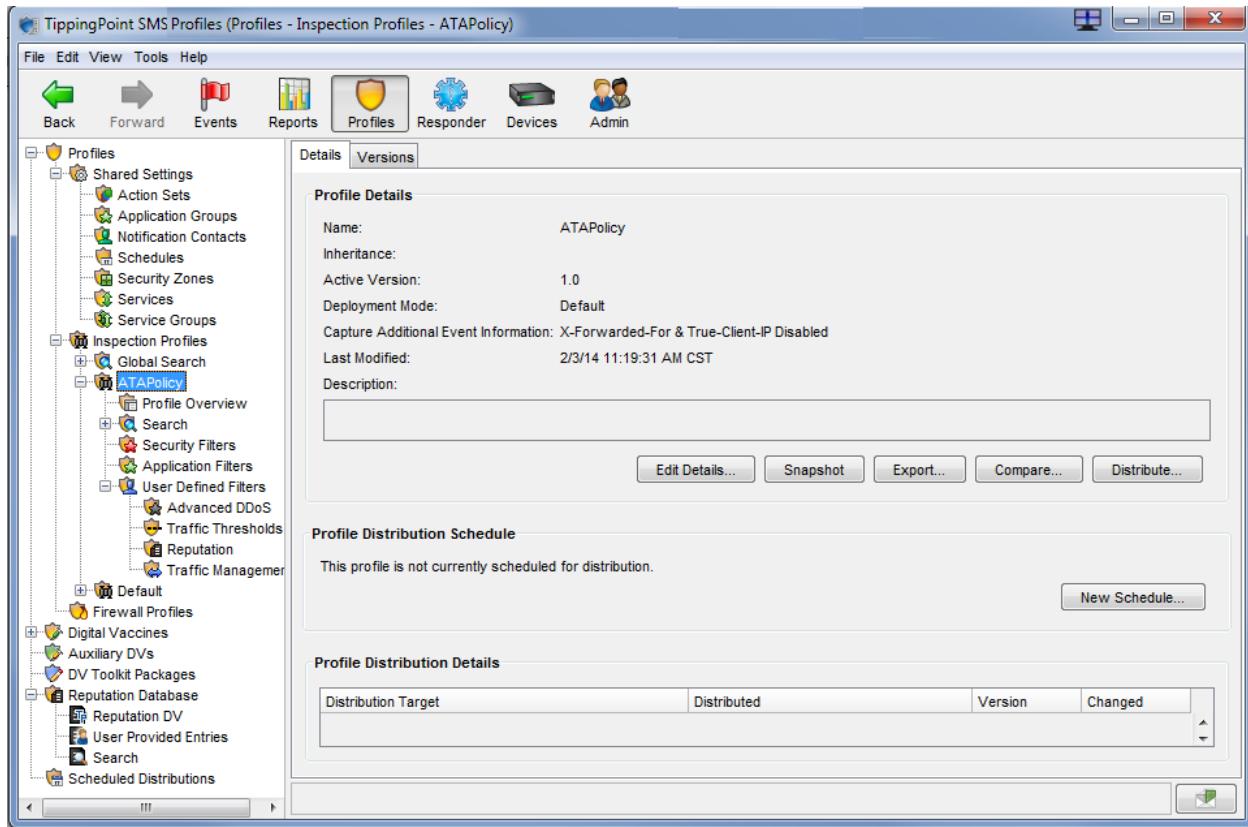
- *Block* action against the command and control network traffic and the malware source.
- *Permit + Notify* action for attempted communications from an infected host.
- *Block* or *Quarantine* an infected host.

## Transforming reputation entries into distributed policy

Use reputation entries to create reputation filters associated with specific action sets. For more information on *reputation filters* and *action sets*, see [Reputation filters](#) on page 5.

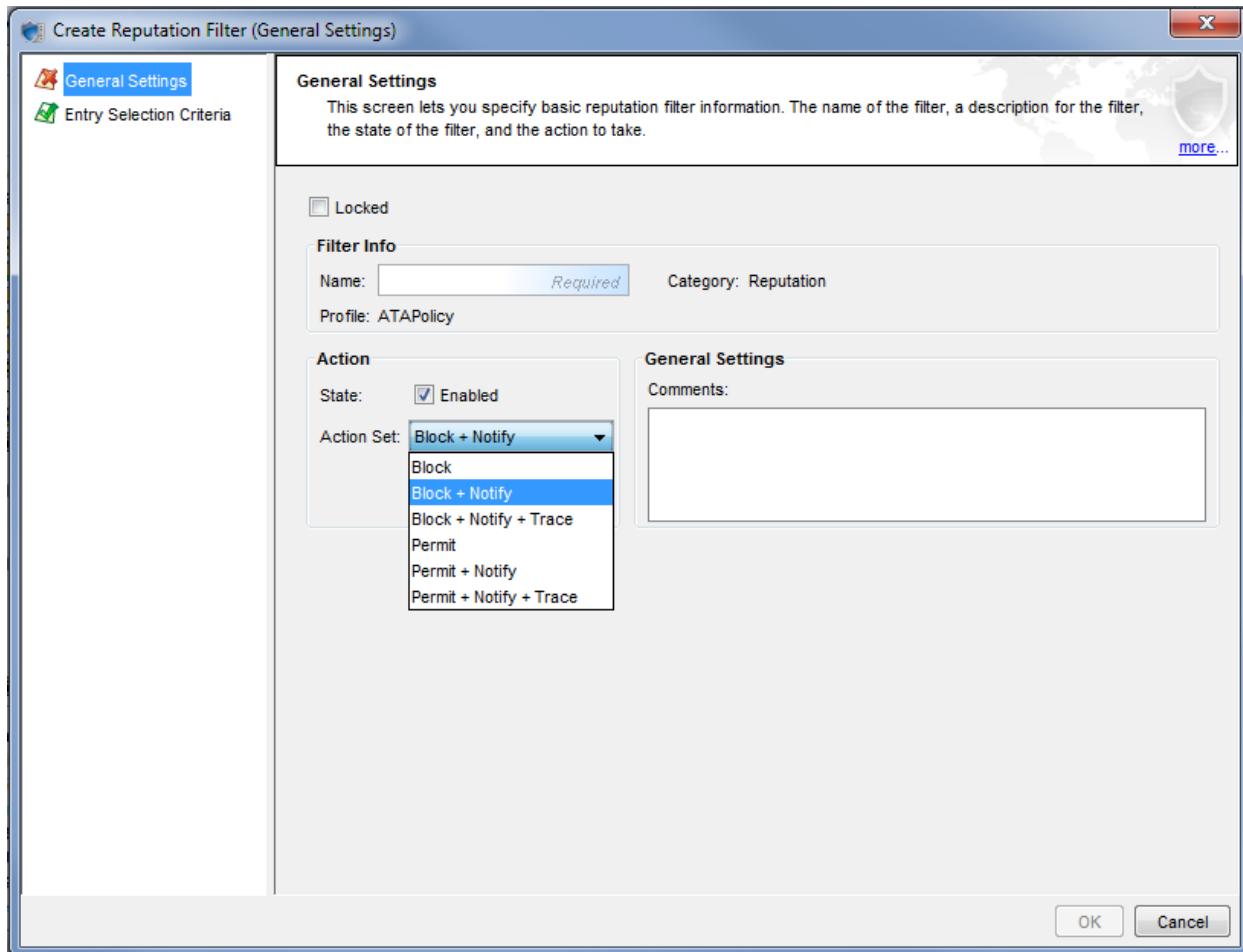
The SMS uses profiles to distribute filters, filter setting modifications, and associated actions to managed devices. For more information about profiles, see [Profiles](#) on page 5. Before creating reputation filters, an SMS administrator typically creates an inspection profile, which becomes the vehicle for distributing the security policy.

In the following example, an SMS administrator has created an inspection profile called *ATAPolicy* in which reputation filters will be created and distributed.

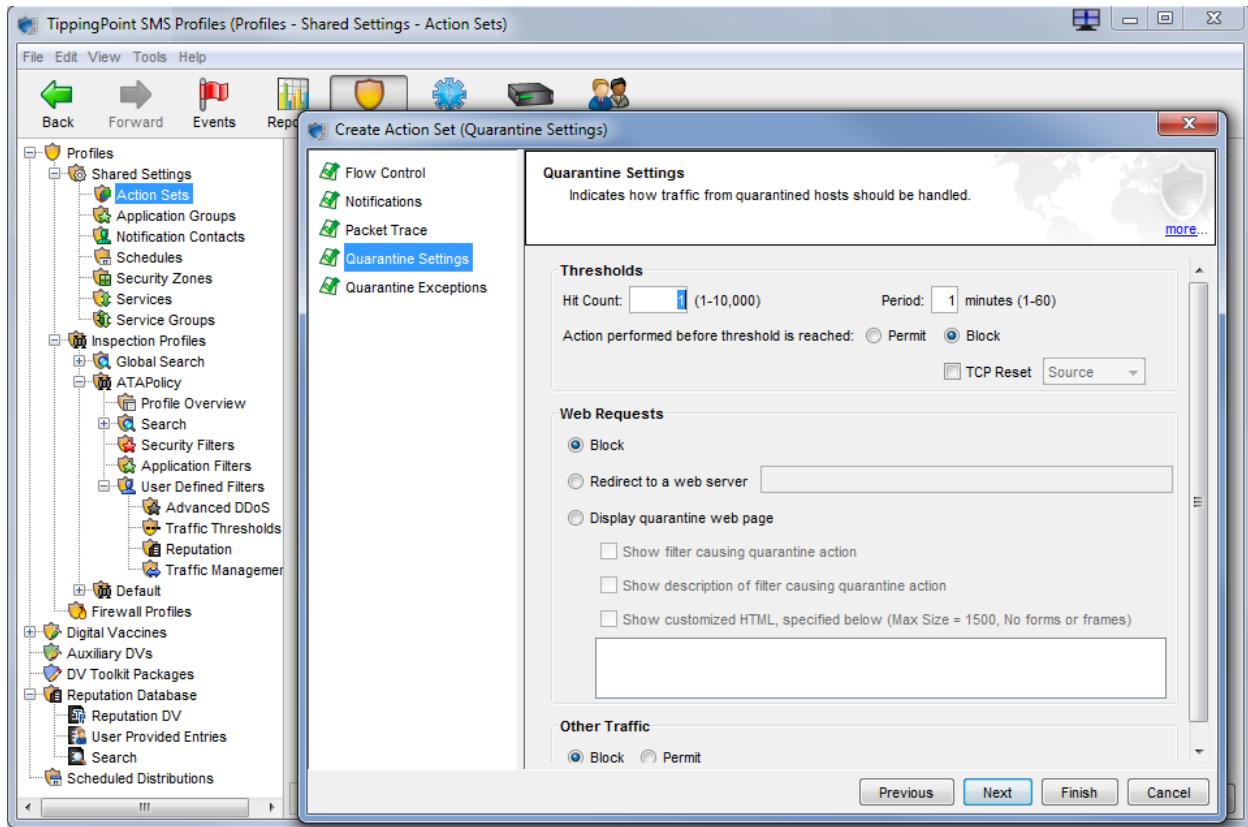


The inspection profile enables you to manage your distribution (all devices, some devices, or specific segments), and it allows you to track where the filters you create will be distributed.

The SMS administrator uses the Create Reputation Filter wizard to create reputation filters. The General Settings screen prompts for basic filter information: Name, State, Action Set, and Comments.



*Block*, *Permit*, and *Notify* actions are available by default. For a *Quarantine* response, the SMS administrator can create a custom action set under Shared Settings in the SMS client (see the image below). Creating a custom action set for Quarantine response allows you to set packet trace options, specify options to handle traffic from quarantined hosts, and to configure exceptions.



In the SMS Create Reputation Filter wizard, the Entry Selection Criteria screen enables the administrator to specify criteria to use for selecting entries from the reputation database. The administrator uses this screen to specify the reputation tag categories for the filter.

After adding reputation filters to the profile, the administrator distributes the profile to the appropriate devices or segments. Once the profile is distributed, any updates to the reputation database entries from the ATP device will automatically update the profile and cause it to be redistributed.

**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A.  
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736  
Email: support@trendmicro.com

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: APEM47851/170502