



5.0.0 TippingPoint™ Security Management System (SMS)

Advanced Threat API Guide

Legal and notice information

© Copyright 2017 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.

Contents

- About this guide..... 1**
 - Target audience..... 1
 - Related documentation..... 1
 - Conventions..... 1
 - Product support..... 3
- Deep Discovery integration & Reputation overview..... 4**
 - SMS integration..... 4
 - Reputation databases..... 4
 - Predefined Reputation tag categories..... 4
 - Reputation filters..... 6
 - Profiles..... 6
- SMS Reputation Management API..... 7**
 - Integrated environment..... 7
- Network enforcement & policy management using Deep Discovery device data..... 8**
 - Transforming Reputation entries into distributed policy..... 8

About this guide

This guide provides integration information for Deep Discovery devices with the TippingPoint Security Management System (SMS) alongside one or more inline TippingPoint Intrusion Prevention System (IPS) and Threat Protection System (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 3

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


The following typographic conventions for structuring information are used.

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

Deep Discovery integration & Reputation overview

The SMS Reputation Management API uses intelligence from Deep Discovery devices to provide in-line blocking at wire speed with TippingPoint IPS and 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

A Deep Discovery 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 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 Deep Discovery Analyzer uses the SMS Reputation Management API to connect with the SMS, enabling the device to trigger Reputation events.

Reputation databases

The TippingPoint ThreatDV Reputation feed is a collection of malicious IP addresses and DNS names. The Threat DV URL Reputation feed is a collection of malicious URL entries. For more information on URL Reputation entries, see the *URL Reputation Filtering Deployment and Best Practices Guide*.

These Reputation feeds are predefined on the SMS. Users can also create a database with their own list of malicious entries. The entries in the Reputation database are used to create Reputation filters that target specific network security needs. See [Reputation filters](#) on page 6.

Predefined Reputation tag categories

The SMS incorporates predefined tag categories from Deep Discovery devices. The 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 Deep Discovery 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 Deep Discovery device, refer to the 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 *SMS 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"> Suspicious Object C&C Callback Address 	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"> High Medium Low 	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 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, all the Reputation entries that match the filters within that profile are also distributed. If a Deep Discovery device sends Reputation entries to the SMS, those entries are distributed to the IPS and TPS devices where a matching filter is already present (as a result of a previous profile distribution).

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 *SMS Web API Guide* included in the latest SMS release.

Integrated environment

In the proposed integrated environment, an out-of-line Deep Discovery 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 Deep Discovery device.

The SMS Reputation Management API enables a Deep Discovery device to connect with the SMS through a secure Web interface, enabling the Deep Discovery 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 Deep Discovery 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 Deep Discovery Analyzer device data in an integrated environment and to set up the following responses to Reputation event triggers:

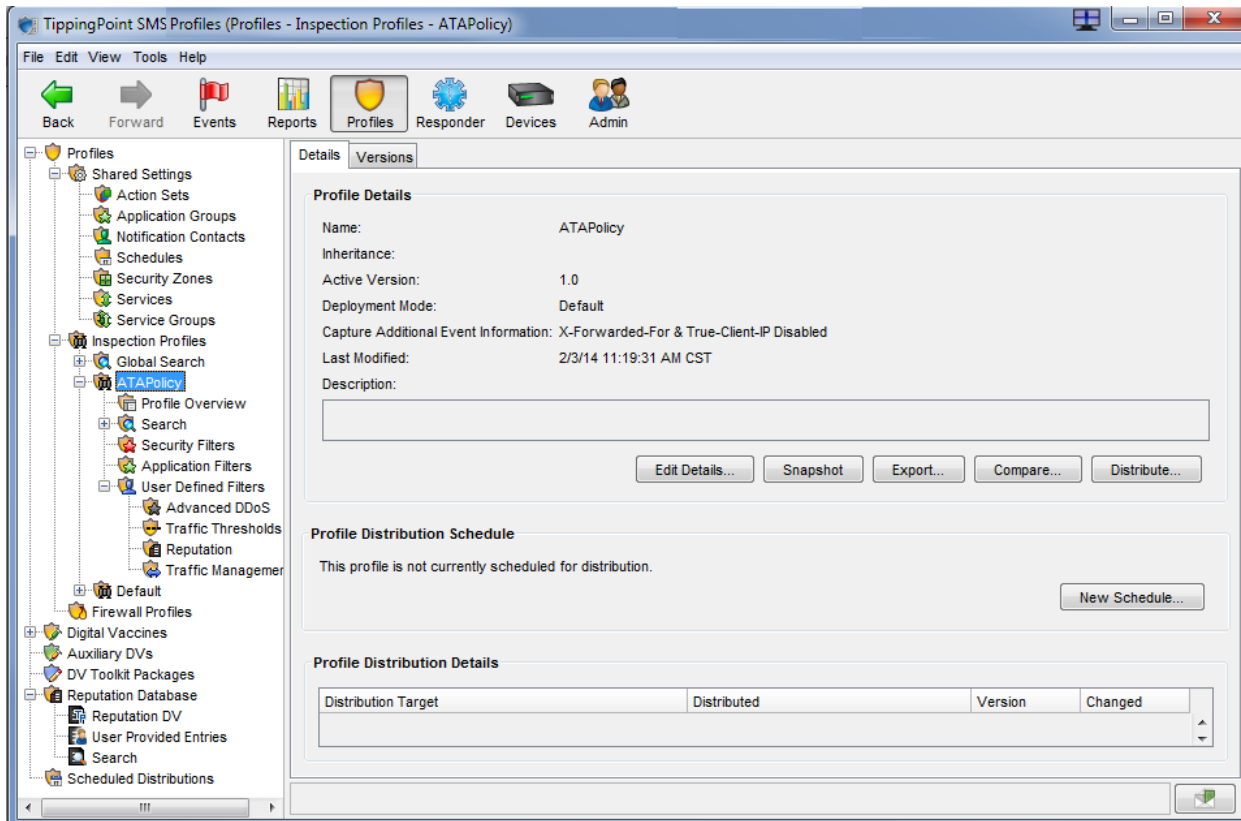
- *Block* action against the command and control network traffic and the malware source.
- *Permit + Notify* action for attempted communications from an infected host.
- *Block* or *Quarantine* an infected host.

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 6.

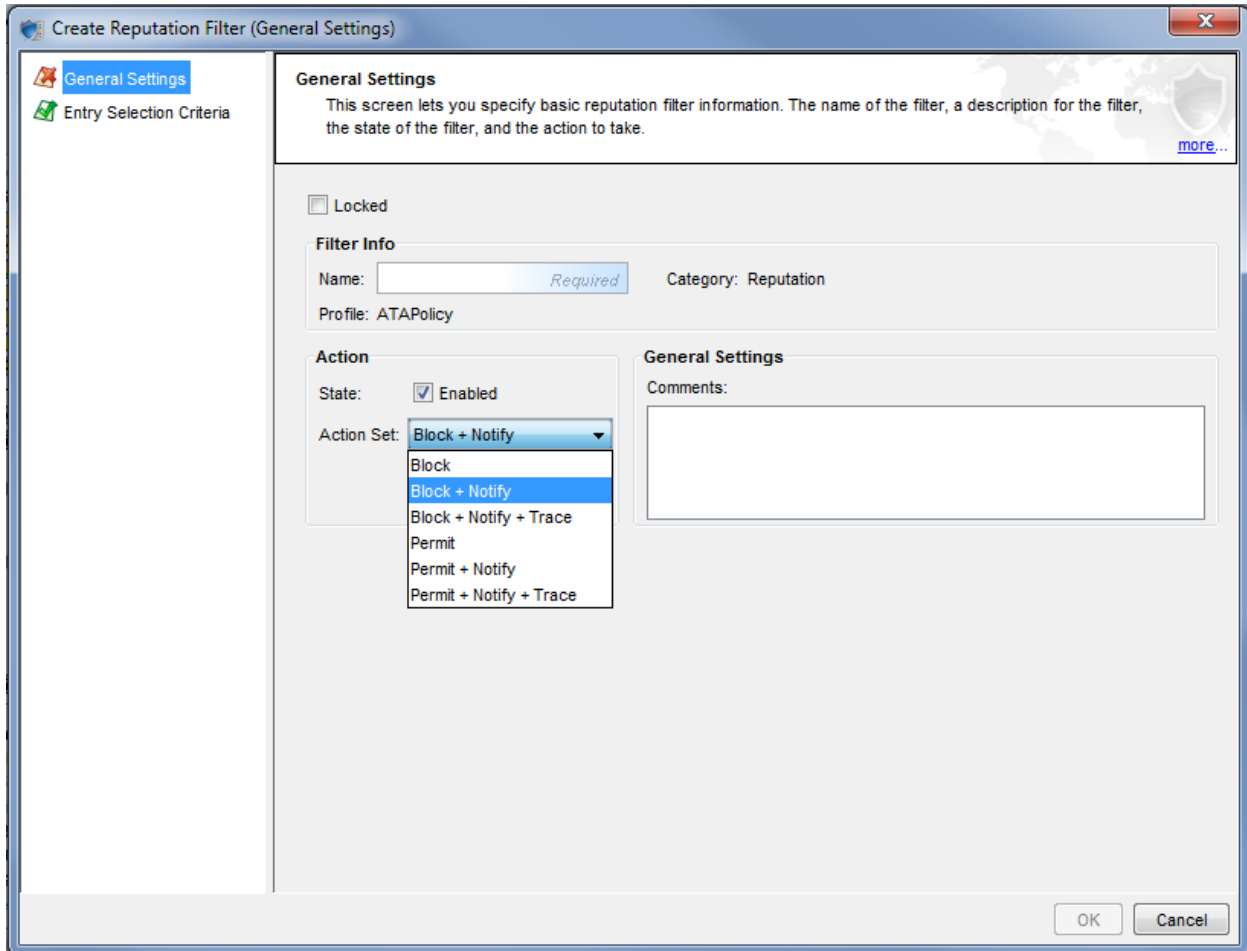
The SMS uses profiles to distribute filters, filter setting modifications, and associated actions to managed devices. For more information about profiles, see [Profiles](#) on page 6. Before creating Reputation filters, an SMS administrator typically creates an inspection profile, which becomes the vehicle 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.

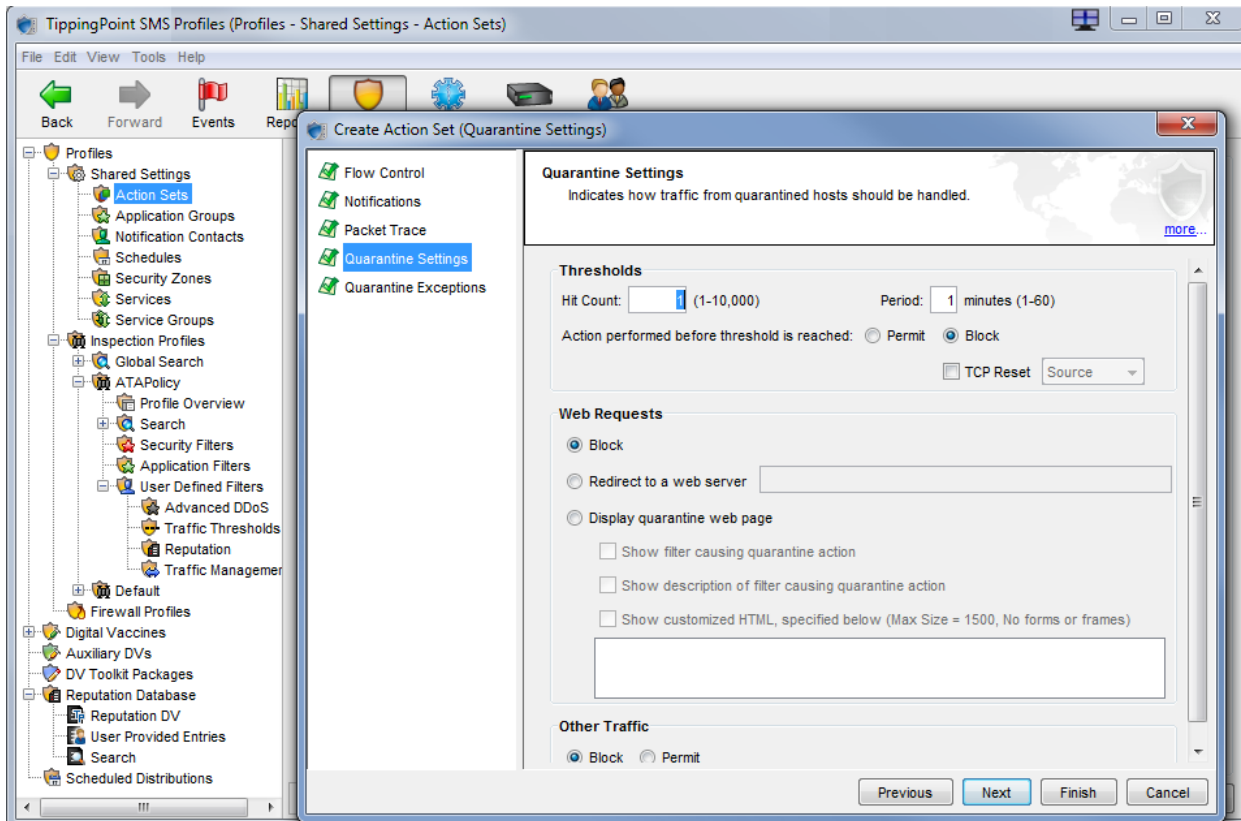


The inspection profile enables you to manage your distribution (all devices, some devices, or specific segments), and it allows you to track where the filters you create will be distributed.

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.

When a profile is distributed, all the Reputation entries that match the filters within that profile are also distributed. If a Deep Discovery device sends Reputation entries to the SMS, those entries are distributed to the IPS and TPS devices where a matching filter is already present (as a result of a previous profile distribution).



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

Item Code: APEM57895/170801