Trend Micro™ TippingPoint™

5.0.0

Security Management System (SMS)
Advanced Threat API Guide

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: February 2023

Deep Discovery integration & Reputation overview

The Trend Micro™ TippingPoint™ Security Management System (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*.

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 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: • 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 product name that discovered the threat.
Trend Micro Severity	List	Pre-defined values of: • 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 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:

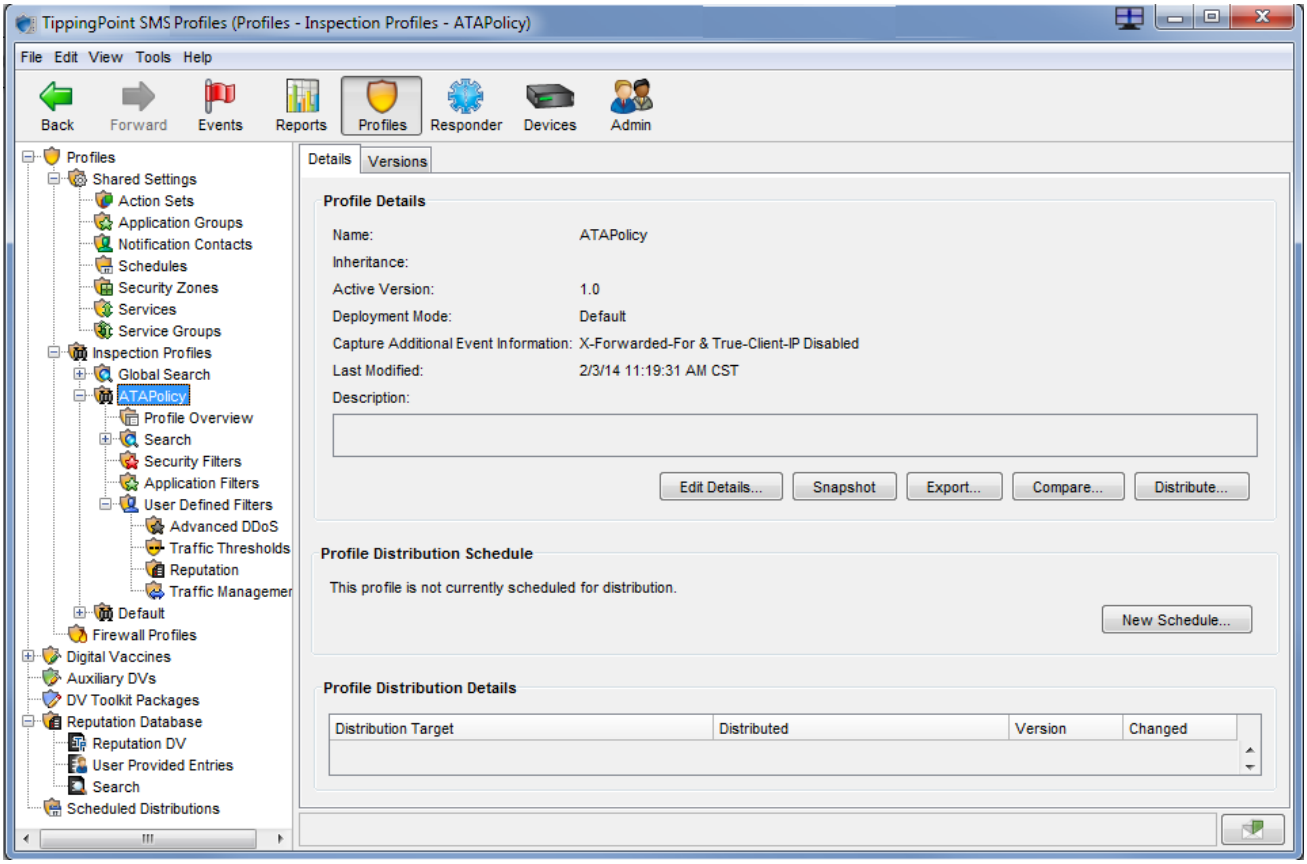
- *Block* action against the command and control network traffic and the malware source.
- *Permit + Notify* action for attempted communications from an infected host.
- *Block* or *Quarantine* an infected host.

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*.

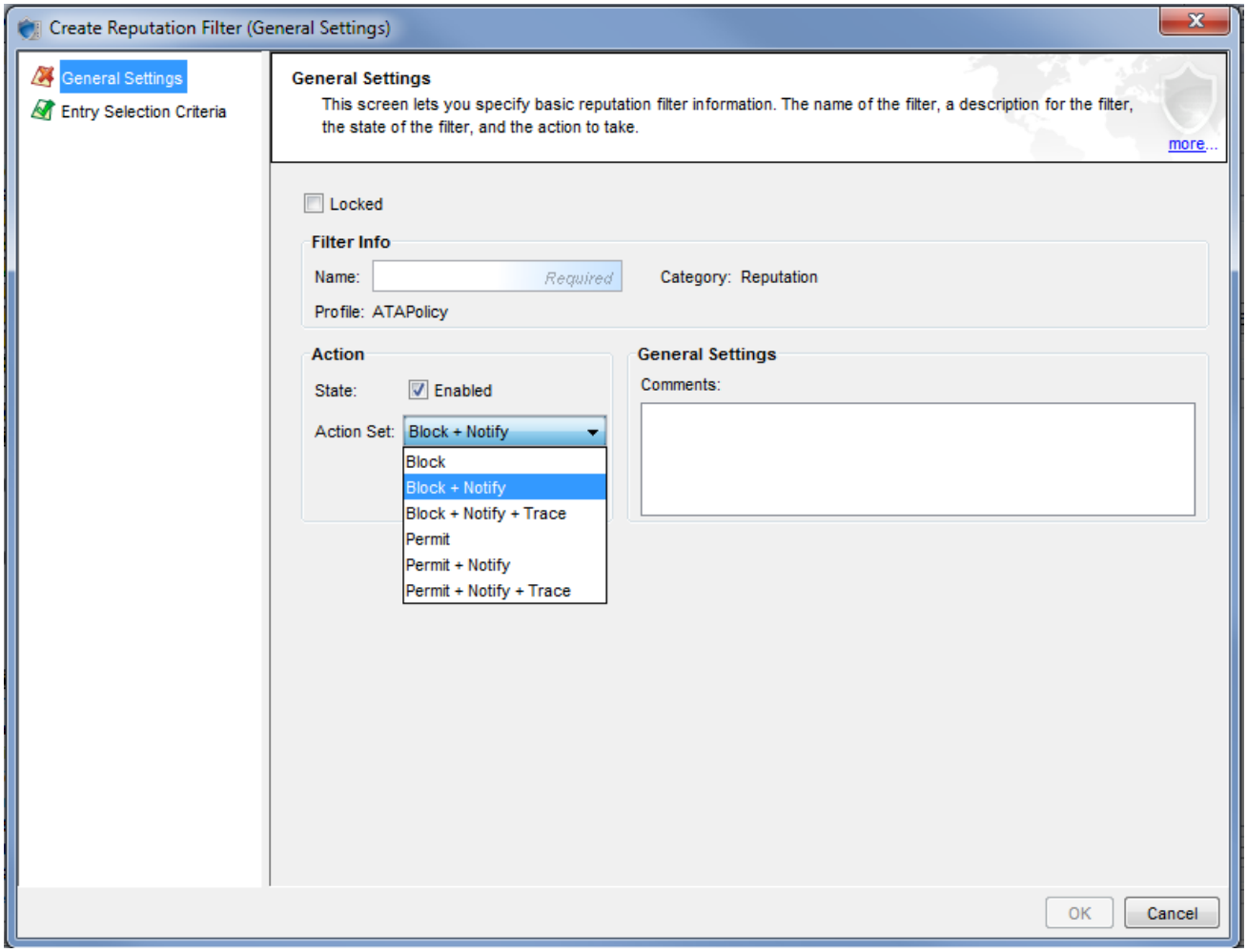
The SMS uses profiles to distribute filters, filter setting modifications, and associated actions to managed devices. For more information about profiles, see *Profiles*. Before creating Reputation filters, an SMS administrator typically creates an inspection profile, which becomes the vehicle for distributing 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.

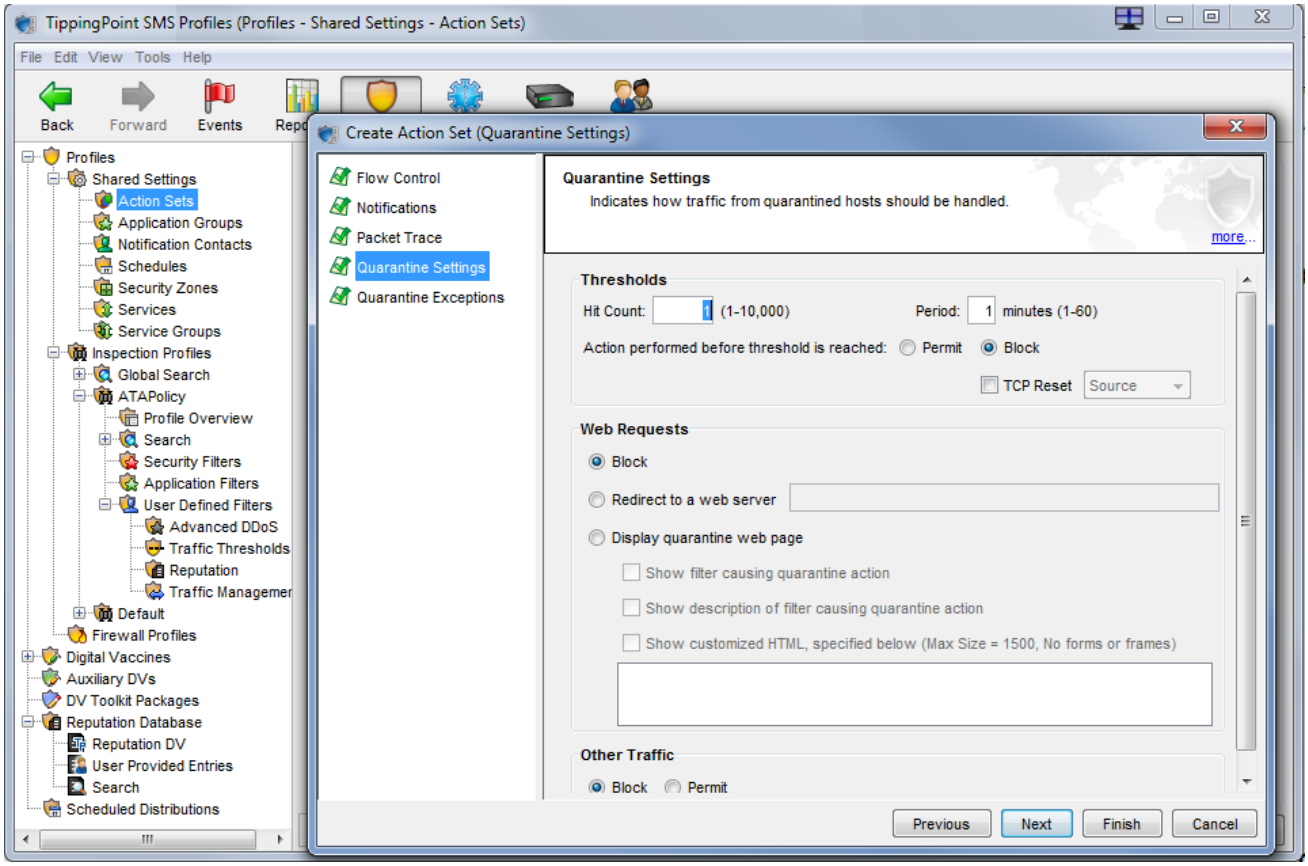


The inspection profile enables you to manage your distribution (all devices, some devices, or specific segments), and it allows you to track where the filters you create will be distributed.

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).