



Trend Micro[™] TippingPoint[™]

Integrating SMS with Trend Vision One[™]
Software Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<https://docs.trendmicro.com/en-us/tippingpoint/security-management-system.aspx>

Trend Micro, the Trend Micro t-ball logo, Trend Vision One, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2024. Trend Micro Incorporated. All rights reserved.

Document Part No.: TP69839/230927

Release Date: January 2024

Protected by U.S. Patent No.: Pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<https://www.trendmicro.com/download/documentation/rating.asp>

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 TippingPoint 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 Notice:

<https://www.trendmicro.com/privacy>

Table of Contents

Chapter 1: Integrating SMS with Trend Vision One™

Integration prerequisites 1-2

Chapter 2: Configuring your integration

Chapter 3: Consuming Suspicious Objects

Chapter 4: Configuring reputation filters

Chapter 5: Suspicious Objects default tag values

Chapter 6: Security Policy and Inventory sharing

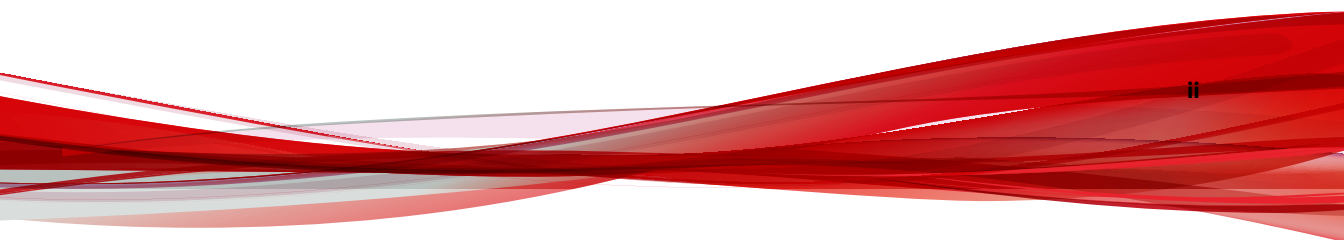
Chapter 7: Event Sharing logs

Chapter 8: Filter Status Sharing

Chapter 9: Cloud Sandbox URL analysis

Chapter 10: TLS Network Telemetry

Chapter 11: Trend Vision One certificate expiration



Chapter 1

Integrating SMS with Trend Vision One™

This guide provides information on how to elevate your organization's threat awareness and automated responsiveness by seamlessly integrating Trend Micro™ TippingPoint™ Security Management System (SMS) with Trend Vision One™.

The strategic benefits of this integration include the ability to forward detection events and intrusion prevention filter protection status to Trend Vision One for correlated detection and other advanced analytics. This enables higher quality alerts and more proactive incident discovery. Mitigate the CVE risk by selecting filters and deploying policies directly to your TippingPoint SMS profiles from Trend Vision One. Threats detected by Trend Vision One are also actionable at the network layer, enabling you to block Suspicious Objects within minutes of detection and disrupt attacks at key locations in your network. In addition, URLs detected by the SMS can be automatically sent for analysis through a Cloud Sandbox without any additional infrastructure. After the URLs are analyzed, you can view the results on the Trend Vision One Sandbox Analysis app.

[Learn more](#) about Trend Vision One.

For information on additional SMS-related enhancements, be sure to refer to the most current *SMS Release Notes* for your TippingPoint operating system (TOS).

Integration prerequisites

To get started with the integration you must have:

- An existing Trend Vision One account.
- An enrollment token that enables the SMS to connect to Trend Vision One for data sharing.



Note


Although a Service Gateway connection is supported, it is *not* required. After you deploy one as a virtual appliance in your corporate network, the Service Gateway is prioritized for communications between your SMS and Trend Vision One. However, a proxy server or direct internet connection is still required for complete integration functionality.

To facilitate your TippingPoint and Trend Vision One integration, consider using the Essential Access apps (valid licenses and SMS activation code required). [Learn more](#).

For more information on deploying Service Gateway, see [Deploying a Service Gateway Virtual Appliance](#).

Chapter 2

Configuring your integration

To configure your integration, click the ADMINISTRATION icon () on your SMS web management console dashboard, and click **Connect to Trend Vision One**. For initial configurations, the configuration status page shows all options disabled by default. Click **Configure** to open the Trend Vision One

Connectivity Settings dialog box and specify the connectivity information and settings.

Trend Vision One Connectivity Settings

Enrollment Token: ⓘ

Service Gateway ⓘ

State:

☐ Disabled

IP Address:

Input your Service Gateway IP address

API Key:

Input your Service Gateway API key

Suspicious Object Sync

State:

☐ Disabled

Download Interval:

1

 Minutes

Security Policy and Inventory

State:

☐ Disabled

Event and Filter Status Sharing

State:

☐ Disabled

Cloud Sandbox URL Analysis ⓘ

State:

☐ Disabled

✖ To send URLs to the Cloud Sandbox Analysis app, you must first use the SMS Java client to create at least one saved query.

Saved Query:

Select saved query...

TLS Network Telemetry ⓘ

State:

☒ Enabled

Test Connectivity ⓘ

Save

Cancel

Enrollment token

Integrating with Trend Vision One for any of its features requires the use of an enrollment token; otherwise, no configurations can be saved. This token registers your SMS with Trend Vision One. Depending on your Trend Vision One version, use the Product Connector or the Product Instance page (the most current version) to enroll your SMS. [Learn more](#).

After you specify the token, all the available configuration options, which are disabled by default, automatically become **Enabled** except for **Cloud Sandbox URL Analysis**.



Note

Each enrollment token is used one time only. After the initial connection is made, the token expires shortly thereafter. If you disconnect SMS from Trend Vision One, a new enrollment token will be required to reconnect.

[Learn more](#) about generating an enrollment token.

Connectivity

Although you can enable and configure a Service Gateway connection, it is not required for any of the feature settings. [Learn more](#) about configuring your Service Gateway IP and API key. If you do enable the Service Gateway, it will, after you configure it, be prioritized for communications between your SMS and Trend Vision One. However, you must still configure a proxy server through the SMS (**Admin > Server Properties > Network > HTTP Proxy**) or use a direct internet connection for complete integration functionality. These options enable you to bypass the Service Gateway and its hardware infrastructure maintenance and dependencies.

To disconnect your SMS from Trend Vision One, click the **Disconnect** button on the Connect to Trend Vision One status page. Alternatively, you can disconnect by clicking the three vertical dots on the right side of the Trend Vision One Product Instance page (**Point Product Connections > Product Instance**), or Product Connector page (if you have an older version). After the SMS has been disconnected, your onboarding status changes to `False`,

and the Sync Status for your connection settings will be displayed as **Out of sync**.

**Note**

You can always reconnect with your previous settings by clicking the **Configure** button and entering a new enrollment token.

Click **Test Connectivity** to confirm your connectivity status for all of your integration settings.

Suspicious Object Sync

Set the **Suspicious Object Sync** state to **Enabled** so that the SMS can pull the latest suspicious IPv4/IPv6 addresses, DNS entries, and URLs from Trend Vision One into the SMS reputation database. A sync is performed every 60 seconds by default. You can change this time interval setting.

**Note**

Resyncing might be required in some cases. For example, if you are switching to another Trend Vision One account to fetch a different Threat Intelligence feed, then you will need to disable the integration, change the gateway IP address or API key, and then enable it again. Any Suspicious Objects in the reputation database from a previous account are still retained.

[Learn more on page 3-1.](#)

Security Policy and Inventory

Turn on this setting to enable the SMS to share Network Intrusion Prevention policy and inventory information with Trend Vision One, and to set and deploy filter policies from Trend Vision One. *[Learn more on page 6-1.](#)*

Event and Filter Status Sharing

Turn on this setting to enable the SMS to share IPS and TPS detection events and intrusion prevention filter protection status with Trend Vision One. The event data gives you insight into the network events of your environment so you can determine whether suspicious activity or incidents are occurring.

When an SMS-managed device detects an event, the event is forwarded to Trend Vision One where the logs can be searched and correlated.

[Learn more on page 8-1](#) about Filter Status Sharing.

[Learn more](#) about Trend Vision One Zero Trust Risk Insights.

Cloud Sandbox URL Analysis

Turn on this setting to enable the SMS to submit URLs for analysis in a secure virtual environment using the Sandbox Analysis app. You can submit up to 10 URLs to the sandbox. Each URL counts as a separate object toward the daily reserve. [Learn more](#).

TLS Network Telemetry

Enables the SMS to send real-time network data it collects from the TippingPoint devices it manages to Trend Vision One for analysis. [Learn more on page 10-1](#).

Chapter 3

Consuming Suspicious Objects

This integration enables the SMS to pull the latest suspicious IPv4/v6 addresses, DNS entries, and URLs into the reputation database. The SMS can automatically consume the latest Suspicious Objects discovered by Trend Vision One and other connected Trend products.

Suspicious Object Exceptions from Trend Vision One are not implemented on the SMS, but individual exceptions can be added on a per-customer basis by the customer directly on the SMS.

After the SMS completes its first full sync from Trend Vision One, all changes on Trend Vision One are delta-synced to the SMS accordingly. The syncs with the SMS occur every minute and with Trend Vision One every five minutes.



Note

It might take a maximum of six minutes for objects to be synced to the SMS from Trend Vision One. If any objects match the blocking criteria in the preconfigured reputation filter, device sync takes immediate effect.

Chapter 4

Configuring reputation filters

To start blocking Suspicious Objects, you will need to set up criteria in the Reputation Filters table and distribute the filters to your TippingPoint security devices. Reputation filters are configured in the SMS Java client. To install the Java client, navigate to **Help > Install Client**. Learn more about the Java client and reputation filters in the *SMS User Guide*.

After the reputation filters are configured, be sure to distribute the profiles to your devices. All Suspicious Objects that match the criteria in the filter are automatically synced to your devices. For example, if you need to block all objects of high severity from Trend Vision One, the reputation filter criteria should be:

- Trend Micro Detection Category = Suspicious Object
- Trend Micro Publisher = Vision One Threat Intelligence
- Trend Micro Severity = High

Reputation Filters (1)											
Order	Name	State	Locked	Action	IPv4	IPv6	DNS	URL	Untagg	Tagged	Criteria
1	AllIPSOfromVisionOne			Block + Notify							(Trend Micro Detection Category is 'Suspicious Object') (Trend Micro Publisher contains 'Vision One Threat Intelligence') (Trend Micro Severity is 'High')

These devices will keep blocking the objects unless you remove them or you change the blocking criteria.

Chapter 5

Suspicious Objects default tag values

All Suspicious Objects from Trend Vision One are tagged with the default values indicated in the following table. Every object contains a *Reputation Entries TTL* tag value to track expired time. You can configure an object's expired time value on the SMS or on Trend Vision One.

The SMS periodically cleans up these objects based on the expired time value. For more guidance on managing Suspicious Objects in Trend Vision One, see [Suspicious Object](#) lists.

TAG CATEGORY NAME	TAG VALUE	DESCRIPTION
Trend Micro Detection Category	Suspicious Object	All Trend Vision One objects are assigned these values
Trend Micro Publisher	Trend Vision One Threat Intelligence	
Trend Micro Source	Trend Vision One Threat Intelligence	
Trend Micro Suspicious Object Source	From Trend Vision One	Possible value: UDSO, VASO
Reputation Entries TTL	From Trend Vision One	The expiration of the object. If it never expires, a default TTL of 10 years TTL from sync time is assigned.

TAG CATEGORY NAME	TAG VALUE	DESCRIPTION
Trend Micro Scan Action	From Trend Vision One	Suggested action: log, block.
Trend Micro Severity	From Trend Vision One	Applicable values: High, Medium, Low

Chapter 6

Security Policy and Inventory sharing

This enables the SMS to share Network Intrusion Prevention information with Trend Vision One. This shared data includes device inventory information (name, IP address, model, software version, device health, digital vaccine version, management console), policy recommendation information (action sets, profiles, distributions), and policy enforcement information (policy configuration and deployment). Mitigate the CVE risk by selecting filters and deploying policies directly to your TippingPoint SMS profiles from Trend Vision One. You can monitor all this information using Trend Vision One without having to use separate consoles.

The SMS sends the data to Trend Vision One every 5 minutes.

With this functionality, you can view and monitor the security status of your device.



Note

Only one SMS can be configured for sharing this data. Only devices that have been managed by that SMS are considered when sharing this data with Trend Vision One.

Chapter 7

Event Sharing logs

With Event Sharing, you can enable the SMS to share detection events with Trend Vision One. The SMS will send these events to Trend Vision One every 60 seconds.

You can use Trend Vision One search functionality to view the shared events, which provide the following information:

TREND VISION ONE KEY NAME	TYPE	DESCRIPTION	EAMPLE
rt	String	UNIX timestamps in milliseconds.	1595326567163
dvchost	String	Hostname of the managed appliance.	device185
ruleName	String	The name of the triggered IPS filter.	HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability
policyId	String	The policy UUID.	00000002-0002-00 02-0002- 000000016798

TREND VISION ONE KEY NAME	TYPE	DESCRIPTION	EXAMPLE
severity	int	The event severity: <ul style="list-style-type: none"> • 0: Info • 1: Low • 2: Minor • 3: Major • 4: Critical 	4
ruleUuid	String	UUID of the triggered IPS filter.	00000001-0001-0001-0001-00000016798
app	String	Protocol of the alert. For example: HTTP, IP, or TCP	http
src	String	Source IP address.	192.0.2.0
spt	String	Source port number	36654
dst	String	Destination IP address	198.51.100.0
dpt	String	Destination port number.	80
aggregatedCount	String	The aggregated number of messages received.	1
act	String	The action set.	Block
endpointIp	String	Client IP address. Supplied by X-Forwarded-For & True-Client-IP header.	203.0.113.0

TREND VISION ONE KEY NAME	TYPE	DESCRIPTION	EXAMPLE
overSsl	String	Whether or not the event is triggered by an SSL decryption stream. This string is displayed only when SSL inspection is supported.	0
mpname	String	Management product name.	Trend TippingPoint Security Management System
cves	List (String)	The corresponding CVEs of the filter for this event.	CVE-2019-12264, CVE-2019- 12259
techniqueId	List (String)	The corresponding MITRE technique IDs of the filter for this event.	T1021, T1078
interestedIp	String	Interested IP of the attack of this event.	203.0.113.0
request	String	The URI of the http request.	http://abc.com/ solr/ admin/ config? action=UPLOAD

Chapter 8

Filter Status Sharing

With Filter Status Sharing, you can enable the SMS to share your intrusion prevention filter protection status with Trend Vision One. The SMS will send the data to Trend Vision One every 3 hours, in addition to whenever inspection profile configurations are distributed and applied to devices successfully.

**Note**

Only the profiles that have been distributed to devices are considered when evaluating protection status.

You can use Trend Vision One Zero Trust Risk Insights functionality to view filter protection status with vulnerability detection results. The filter protection status data helps produce a risk score of your environment based on a Trend Vision One Risk Insights vulnerability assessment. Part of the assessment includes recommendations for virtual patching using TippingPoint intrusion prevention filters.

The following table defines each status:

FILTER STATUS	DESCRIPTION
Blocked on all profiles	The filter is enabled, and the flow control action set is set to Block in all inspection profiles.

FILTER STATUS	DESCRIPTION
Not blocked on any profile	The filter is disabled, the filter is modified without distribution, or the flow control action set is not set to Block in all inspection profiles.
Blocked on some profiles	The filter status is protected in only some inspection profiles.

[Learn more](#) about viewing filter protection status with vulnerability detection results.

Chapter 9

Cloud Sandbox URL analysis

This integration enables the SMS to send URLs for analysis without any additional infrastructure. The Cloud Sandbox Analysis app performs the analysis. You can also use the Cloud Sandbox Analysis app to view the analysis results.

JDI	Trend Vision One™ Sandbox Analysis							2023-03-09 18:47
Platform Directory	Submissions (Total / Reserve): 0 / 2							Submission Settings
Risk Insights	Submit Object	Submitted: All	Object type: All	Risk level: All	Submitter: All	Object, SHA-1, Threat type, Threat name...		
XDR Threat Investigation	Object	Status	Submitter	Submitted	SHA-1 hash value	Risk level	Threat type	
Threat Intelligence	https://tinder.com	Done	Manual Submission	2023-02-16 10:56...	e0841c4019a8995958ad50027a5b3e43f1...	No risk		
Campaign Intelligence	https://tinder.com/	Done	Manual Submission	2023-02-15 17:20...	be7f84d43d58e0ff112339eeb2e1911330df...	No risk		
Intelligence Reports	https://tinder.com	Done	Manual Submission	2023-02-15 16:32...	e0841c4019a8995958ad50027a5b3e43f1...	No risk		
Suspicious Object Management	https://portal-xdr.visionone...	Done	Manual Submission	2023-02-13 12:12:05	a691c2912a99d05e036132e6e56cd11025...	No risk		
Sandbox Analysis	https://stackoverflow.com/	Done	Manual Submission	2023-02-13 17:07...	c41595eb2bfe794c2a6aa78f0d7db76823...	No risk		
Third-Party Intelligence	https://www.disneyplus.com...	Done	Manual Submission	2023-02-13 16:51:11	e6123801332ab913288e5b37fa3bd9d663...	No risk		
Workflow and Automation	https://term.pit.co/	Done	Manual Submission	2023-02-13 16:49...	a4b1b1b09209c1a2b7729cbat0b08b011...	No risk		
	https://tiktok.instagram.co...	Done	Manual Submission	2023-02-13 16:49...	648c72303b22b06103437727836db0a26...	Not analyzed		

Enabling Cloud Sandbox URL analysis requires the following:

- Valid Trend Vision One license.
- At least 1 daily reserve (50 credits) on Trend Vision One. [Learn more.](#)
- At least one saved query.
- At least one profile with **HTTP Context** enabled.

- Ability to connect to the Cloud Sandbox Analysis app.

Learn more about creating a saved query and enabling HTTP context for a profile in the *TippingPoint Security Management System (SMS) User Guide* at the [Online Help Center](#).

By enabling the Suspicious Object Sync in conjunction with this integration, you can sync the high-risk URLs back to the SMS for profile filtering. In order for the SMS to detect suspicious URLs, you must manually create a profile with the relevant filters enabled. Currently, there are 102 filters that you must enable and set to Block. To find and enable these filters:

1. In the SMS Client, navigate to **Profiles > Inspection Profiles > Default > Search**, and input the following query in the Filter Name field:



Note

In order to preserve your Default profile and prevent the local IPS default profiles from remaining active on unused segments, create a copy of the Default profile and make any configuration changes to that copy instead.

```
^3316: , ^13645: , ^13719: , ^13786: , ^16480: , ^19428: , ^19611: ,  
  
^19616: , ^19620: , ^20356: , ^20357: , ^20359: ,  
  
^21187: , ^21333: , ^22379: , ^22662: , ^24042: ,  
  
^24492: , ^24594: , ^24837: , ^24884: , ^24932: , ^24971: ,  
  
^27819: , ^29217: , ^29454: , ^29455: , ^29456: , ^29457: , ^29458: , ^29459: , ^29460: , ^29461: ,  
  
^29462: , ^29463: , ^29464: , ^29465: , ^29466: , ^29467: , ^29468: , ^: , ^29469: , ^29470: ,  
  
^29471: , ^29472: , ^29473: , ^29474: , ^29740: , ^29798: ,  
  
^30117: , ^30192: , ^30264: , ^30301: , ^31283: , ^31570: , ^32902: , ^34248: ,
```

```

^35781: , ^35783: , ^35785: , ^36578: , ^37896: , ^37940: , ^37959: , ^37960: ,
^3629: , ^3917: , ^4036: , ^4065: , ^4111: , ^4531: , ^4691: , ^4714: , ^4761: , ^5056: ,
^37962: , ^38222: , ^38223: , ^38224: , ^38225: , ^38226: , ^38227: , ^38360: ,
^41470: , ^5381: , ^5426: , ^6069: , ^6300: , ^6377: , ^6382: , ^6383: , ^6435: , ^8273: , ^8447: ,
^9221: , ^9577: , ^9578: , ^9895: , ^10565: , ^11105: , ^11112: , ^11867: , ^13310: , !13629, !24036,

!34036, !40360, !40361, !40362,
!40363, !40369, !40650, !40651, !40652, !40653, !40655,
!40656, !40657, !40658, !40659, !41110, !41111, !41112,
!41114, !41115, !41116, !41117, !41118, !41119, !24531,
!34691, !24761, !34761, !36069, !16300, !19221, !39221,
!19577, !29577, !19578, !29578, !19895, !39895, !13917,
!34111, !34065, !25381

```

2. In the Search Results output, select all the filters and click **Edit**.
3. In the Action panel of the Edit Multiple Filters dialog, select **Enabled** for the state and **Block** for the Action Set.
4. Click **OK**.
5. Click **Distribute** to distribute the profile of enabled filters to your managed devices.

When you update your Trend Vision One enrollment token, the index of sandbox URLs is also automatically updated to the latest alert record, even if there are records that have not been uploaded to the Sandbox Analysis app yet.

[Learn more](#) about sandbox analysis.

Chapter 10

TLS Network Telemetry

This enables the SMS to send and collect real-time network data from its managed devices to Trend Vision One for timely and thorough analysis. In contrast to other resource-intensive polling methods, TLS Network Telemetry automatically collects and sends data more efficiently and in real time. Because it is modeled for scalability, you can grow your network without seeing diminished monitoring of time-sensitive data.



Note

For collection to occur, the devices must have FIPS mode disabled.

Analysis of the data by Trend Vision One enables you to assess and prioritizes your network risks alongside other XDR sensor data.

Chapter 11

Trend Vision One certificate expiration

When you integrate your SMS with Trend Vision One for the first time using the Enrollment Token, you are automatically provided with a Trend Vision One certificate that expires after one year.

Because configurations that involve event, filter, or data sharing require a current and valid certificate, your Trend Vision One certificate automatically renews 30 days before its expiration so that you avoid any gap in security protection. This also circumvents having to monitor the certificate's expiration date and having to take extra manual steps to renew it.



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: TP6M69839/230927