Trend Micro™ TippingPoint™

Integrating SMS with Trend Vision One™

Software 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: August 2023

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.

Learn more about Service Gateway.

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.
- For sharing suspicious objects, a preconfigured Service Gateway deployed within your corporate network. After the gateway is deployed as a virtual appliance in your corporate network, it participates in handling requests between Trend Vision One and SMS.

Note

A Service Gateway connection is required for sharing suspicious objects between the SMS and Trend Vision One, but it is *not* required for:

- Sharing network intrusion prevention data
- Sharing event and filter status information
- Sending URLs to the Cloud Sandbox for analysis

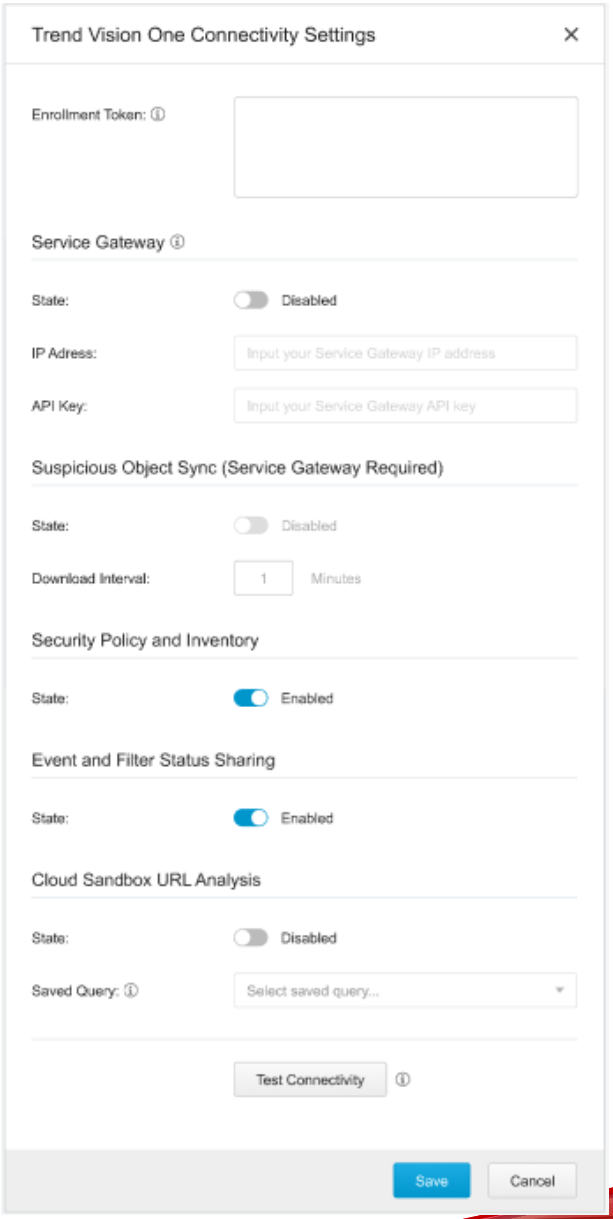
To facilitate your TippingPoint and Trend Vision One integration, consider using the Essential Access apps (valid licenses and SMS activation code required). Learn more.

For more information on deploying Service Gateway, see Deploying a Service Gateway Virtual Appliance.

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 add the required connectivity information in the Trend Vision One Connectivity Settings dialog box.



No configurations can be saved without first specifying your enrollment token. After you do, the **Security Policy and Inventory** and **Event and Filter Status Sharing** options automatically become **Enabled**.

You cannot configure the **Suspicious Object Sync** feature without first enabling and configuring the Service Gateway. Although it is not required for the rest of the feature settings, the Service Gateway will, after you configure it for **Suspicious Object Sync**, still provide Trend Vision One connectivity for those remaining settings.

Connectivity

Integrating with Trend Vision One for any of its features requires the use of an enrollment token. You must enroll your SMS using the Product Connector in Trend Vision One. Learn more.

A Service Gateway is required only for sharing suspicious objects from Trend Vision One to the SMS. Learn more about configuring your Service Gateway IP and API key. Provided that suspicious object sync remains disabled, you can bypass the Service Gateway and its hardware infrastructure maintenance and dependencies by using a direct internet connection (if your environment is set up for it) or by enabling a proxy server for internet connections through the SMS (**Admin > Server Properties > Network > HTTP Proxy**).

Disconnecting the SMS from Trend Vision One can only be done from the Trend Vision One Product Connector (**Point Product Connections > Product Connector**). After they have been disconnected, your onboarding status changes to `False`, and the Sync Status for your connection settings will be displayed as `Failed`.

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

Suspicious Object Sync (Service Gateway Required)

After you configure a Service Gateway, set the **Suspicious Object Sync** state to **Enabled** so that the SMS can retrieve suspicious objects from Trend Vision One. The Service Gateway syncs with SMS 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 5.

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 8*.

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 11 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.

Consuming Suspicious Objects

This integration enables the SMS to pull the latest suspicious IPv4/v6 addresses, DNS entries, and URLs into the reputation database. After the gateway is enabled, the SMS can automatically consume the latest Suspicious

Objects discovered by Trend Vision One and other connected Trend products.

Suspicious Object Exceptions from 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.

The SMS initially starts a full sync from Trend Vision One through Service Gateway. After this first sync is complete, all changes on Trend Vision One are delta-synced to the SMS accordingly. The Service Gateway syncs with the SMS 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.

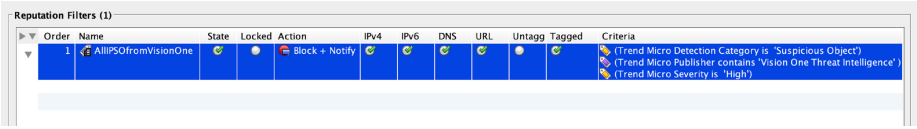
Configuring reputation filters

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



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

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.
Trend Micro Scan Action	From Trend Vision One	Suggested action: log, block.

TAG CATEGORY NAME	TAG VALUE	DESCRIPTION
Trend Micro Severity	From Trend Vision One	Applicable values: High, Medium, Low

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 devices that have been managed by the SMS are considered when sharing this data with Trend Vision One.

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.	`00000002-0002-0002-0002-000000016798`
severity	int	The event severity: • `0`: Info • `1`: Low • `2`: Minor • `3`: Major • `4`: Critical	`4`
ruleUuid	String	UUID of the triggered IPS filter.	`00000001-0001-0001-0001-000000016798`
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`

Trend Vision One Key Name	Type	Description	Eample
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`
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`

Trend Vision One Key Name	Type	Description	Eample
request	String	The URI of the http request.	`http://abc.com/solr/ admin/config?action=UPLOAD`

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:

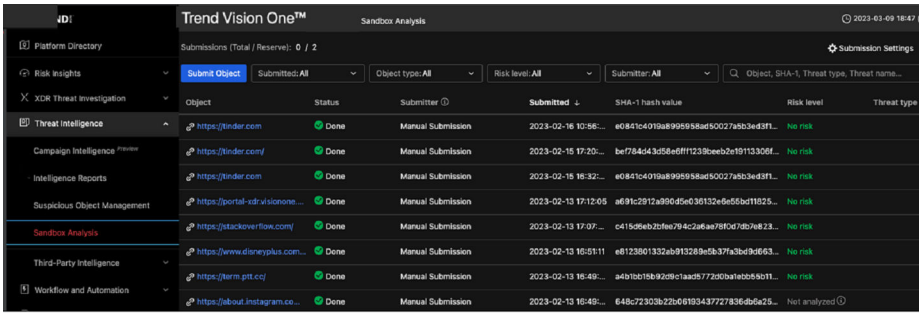
Filter Status	Description
Blocked on all profiles	The filter is enabled, and the flow control action set is set to **Block** in all inspection profiles.
Not blocked on any profile	The filter is disabled, the filter is modified without distribution, or the flow control action set is not set to **Block** in all inspection profiles.

Filter Status	Description
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.

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.



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 of 102 filters in the Filter Name field:

```
3629,3917, 4036, 4065,4111, 4531, 4691, 4714, 4761, 5056,
5381, 5426, 6069, 6300, 6377, 6382, 6383, 6435, 8273, 8447,
9221, 9577, 9578, 9895, 10565, 11105, 11112, 11867, 13310,
13316, 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,
37962, 38222, 38223, 38224, 38225, 38226, 38227, 38360,
41470, !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.

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.