TippingPoint™

Integrating SMS with Trend Micro 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: February 2022

Integrating SMS with Trend Micro Vision One™

Elevate your organization's threat awareness and automated responsiveness by integrating Trend Micro™ TippingPoint™ Security Management System (SMS) with Trend Micro Vision One™.

The strategic benefits of this integration include the ability to forward detection events and intrusion prevention filter protection status to Trend Micro Vision One for correlated detection and other advanced analytics. This enables higher quality alerts and more proactive incident discovery. In addition, threats detected by Trend Micro 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.

The ServiceGateway seamlessly integrates your TippingPoint security hardware appliances with Trend Micro Vision One for greater threat visibility and responsiveness. Beginning with version 1.0.0.10051 of Service Gateway, you can also enable Event and Filter Status Sharing to share IPS and TPS detection events and filter protection status with your SMS (version 5.5.2.1 or later) for correlation.

This guide provides information on how to use the Service Gateway so that the SMS can retrieve Suspicious Objects from Trend Micro Vision One. It also provides information on enabling Event and Filter Status Sharing so that the Service Gateway can share IPS and TPS detection events and filter protection status with your SMS for correlation.

Learn more about Trend Micro Vision One.

Learn more about Service Gateway.

Integration prerequisites

Initiate Vision One integration on your SMS web management console by configuring and enabling Service Gateway. After the gateway is deployed as a virtual appliance in your corporate network, it handles requests between Trend Micro Vision One and SMS.

To get started with the integration you must have:

- An existing Trend Micro Vision One account.
- A preconfigured Service Gateway deployed within your corporate network.

Note

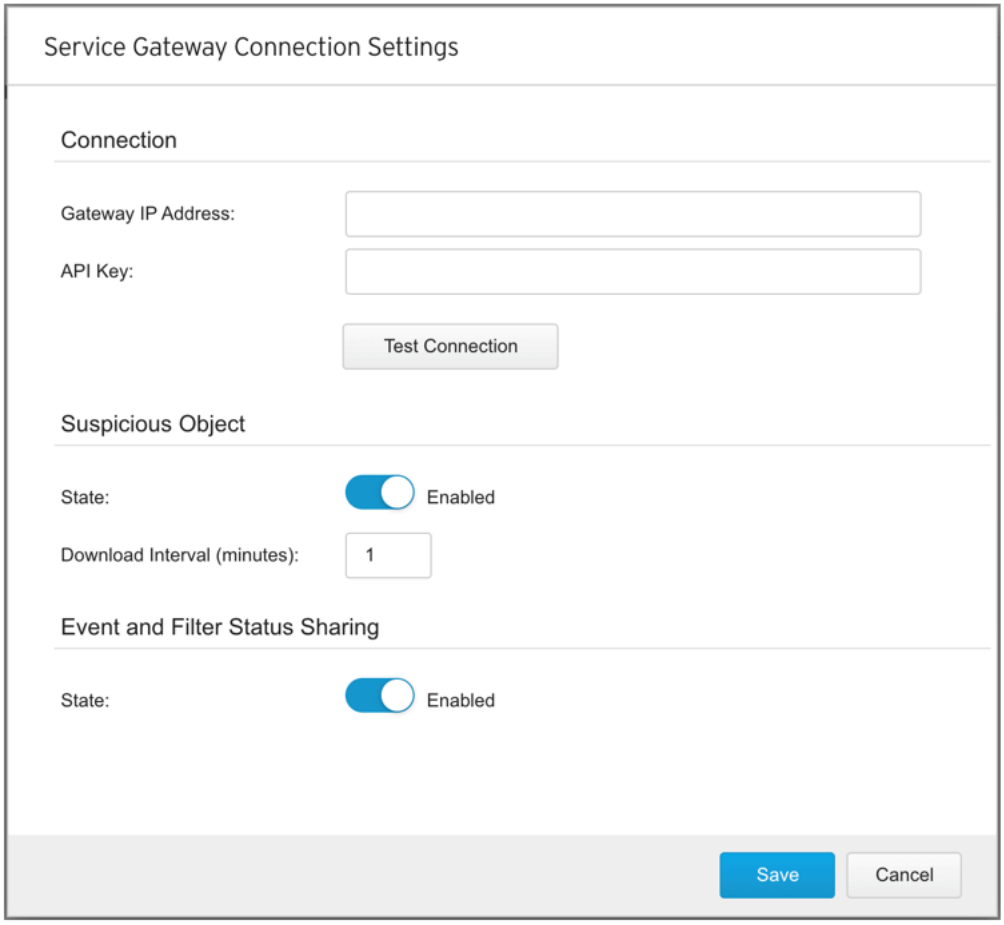
To use Event and Filter Status Sharing, your Trend Micro Vision One account must have a valid XDR Add-on license for TippingPoint software. To request this license, contact your sales representative.

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

Configuring Service Gateway Integration

To configure Service Gateway Integration, navigate to the **Administration** icon on your SMS web management console dashboard. Select **Service Gateway** under the Administration tab. Add the required

information from your Trend Micro Vision One instance in the Service Gateway Connections dialog box as shown below:



Connection

Configure your Gateway IP and API key so that the SMS can connect to the Service Gateway. You can use the **Test Connection** button to preview gateway integration. Click **Save** to save your connection settings.

Suspicious Object

Be sure to set the state to **Enabled** so that the SMS can retrieve Suspicious Objects from Trend Micro 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 Micro 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.

Event and Filter Status Sharing

Event and Filter Status Sharing enables SMS to share IPS and TPS detection events and intrusion prevention filter protection status with Trend Micro Vision One using the Service Gateway. 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 appliance detects an event, the event is forwarded to Trend Micro Vision One where the logs can be searched and correlated.

The filter protection status data helps produce a risk score of your environment based on a Trend Micro Vision One Risk Insights vulnerability assessment. Part of the assessment includes recommendations for virtual patching using TippingPoint intrusion prevention filters.

Learn more about Trend Micro Vision One Zero Trust Risk Insights.

Consuming Suspicious Objects

This integration enables SMS to pull the latest suspicious IPv4/v6 addresses, DNS entries, and URLs into the reputation database. After the gateway is enabled, SMS can automatically consume the latest Suspicious Objects discovered by Trend Micro Vision One and other connected Trend Micro products. SMS initially starts a full sync from Trend Micro Vision One through Service Gateway. After this first sync is complete, all changes on Trend Micro Vision One are delta-synced to SMS accordingly. The Service Gateway syncs with SMS every minute and with Trend Micro Vision One every five minutes.

Note

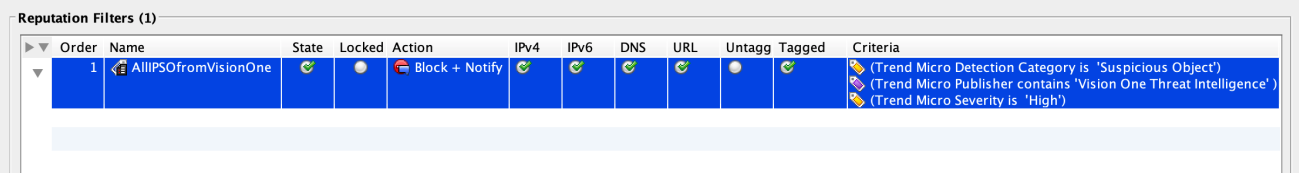
It might take a maximum of six minutes for objects to be synced to SMS from Trend Micro Vision One. If any objects match the blocking criteria in the preconfigured reputation filter, device sync takes immediate effect.

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, 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 Micro 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 Micro 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 SMS or Trend Micro Vision One.

SMS periodically cleans up these objects based on the expired time value. For more guidance on managing Suspicious Objects in Trend Micro Vision One, see Suspicious Object lists.

Tag category name	Tag value	Description
Trend Micro Detection Category	Suspicious Object	All Trend Micro Vision One objects are assigned these values
Trend Micro Publisher	Trend Micro Vision One Threat Intelligence	
Trend Micro Source	Trend Micro Vision One Threat Intelligence	
Trend Micro Suspicious Object Source	From Trend Micro Vision One	Possible value: UDSO, VASO
Reputation Entries TTL	From Trend Micro 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 Micro Vision One	Suggested action: log, block.
Trend Micro Severity	From Trend Micro Vision One	Applicable values: High, Medium, Low

Event Sharing logs

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

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

Trend Micro 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`

Trend Micro Vision One Key Name	Type	Description	Eample
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`
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 Micro 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`

Filter Status Sharing

With Filter Status Sharing, you can enable the SMS to share your intrusion prevention filter protection status with Trend Micro Vision One. The SMS will send the data to Trend Micro Vision One every hour, 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 Micro Vision One Zero Trust Risk Insights functionality to view filter protection status with vulnerability detection results. 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.
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.