Mandiant

TIPPING POINT INTEGRATION WITH SECURITY VALIDATION

This integration collects security events from Tipping Point.

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

This integration uses the XML API.

API	Usage
`/dbAccess/tptDBServlet?method=GetData`	Retrieve a list events from tables provided in the query
`/dbAccess/tptDBServlet?method=Status`	Perform a check to make sure the credentials are working and the instance is reachable

Supported Versions

5.5.5.x

Before You Begin

To configure this integration, you need:

- API Key

The HTTP Authentication mechanism is deprecated and not recommended. We recommend that you authenticate by using the API key.

Create an API Key

1. Log into Tipping Point SMS.
2. Go to `https://[SMS_IP]/help/api-docs/auth.html` .
3. Follow the on screen documentation for viewing the API KEY.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Tipping Point**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)

6. For the **Host**, enter the hostname of your Tipping Point instance. The default is **httpbin.org**.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Api Key** that you generated.
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Optional: Modify **Queries**, as needed. A default value is provided.
12. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

13. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
14. Optional: Modify **Ip Fields**, which are fields in the response that require conversion from numeric IP values to dot notation IP format.
15. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

    If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events

and 10 alerts.

16. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
    - The Director can communicate with the integration host on the port and protocol specified.
    - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).

Configure Legacy Integration

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is remote capable.

Update TippingPoint

The Validation Platform requires an exclusive user account. Create an account that has, at minimum, Access SMS Web Services permissions.

API Calls

The following API Calls are used by the Validation Platform.

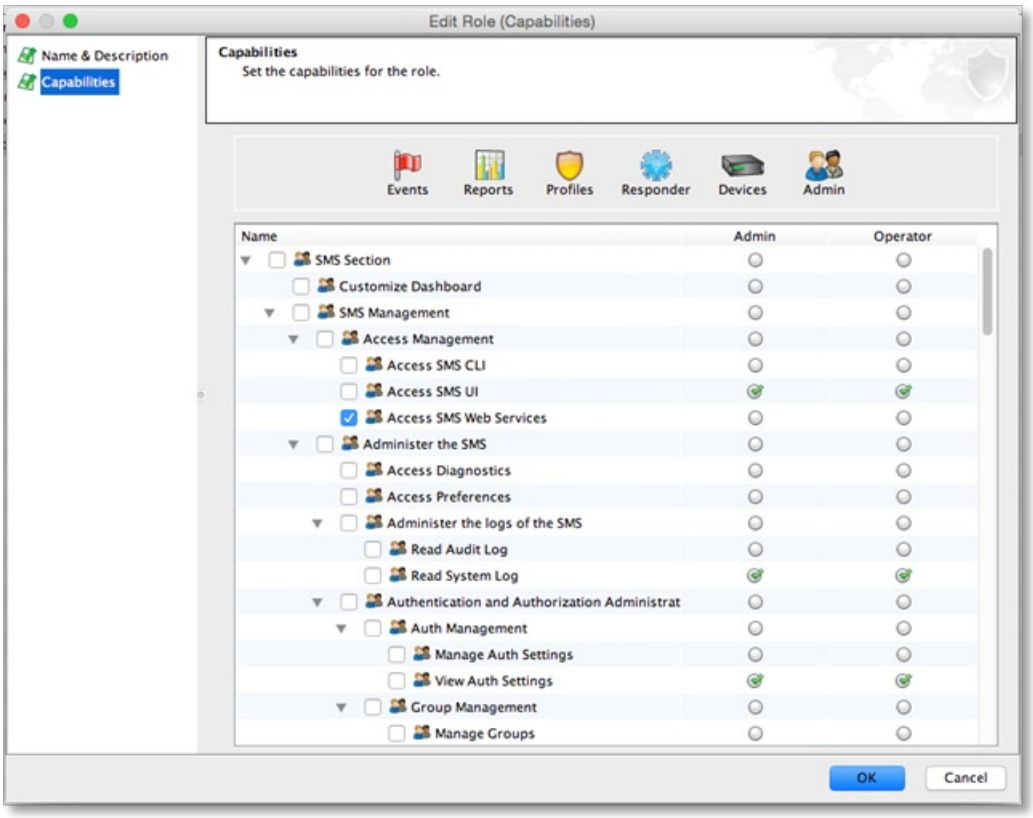
Purpose	Call
Query Alerts	`/dbAccess/tptDBServlet` with `GetData` method in the `ALERTS` table.  Uses begin_time and end_time to timebox the query.
Update signatures	`/dbAccess/tptDBServlet` with `DataDictionary` method in the `SIGNATURE` table.  This is retrieving signatures from TippingPoint to update our cache, not changing configuration on TippingPoint devices.

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the IP address used to access TippingPoint SMS host.
2. Identify the port for TippingPoint SMS host communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS for connections to the TippingPoint SMS host port.
4. Identify or create credentials to access TippingPoint.

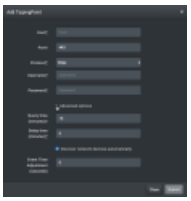


Tipping Point Credentials

Configuration

TO ADD THE TIPPING POINT INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **TippingPoint**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.
6. Click **Update Signatures** to download the TippingPoint signature set from the SMS server.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7de0/n/tippingpoint.png)

Tipping Point Integration

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules** (https://docs.mandiant.com/home/msv-proxy-rules).

Verify connectivity

TO VERIFY CONNECTIVITY TO TIPPINGPOINT

Click **Test** to verify that:

- The Director can communicate with TippingPoint using the port specified.
- User credentials are working.