Mandiant

TRELLIX EMAIL SECURITY - CLOUD (ETP)

> 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).

To validate the effectiveness of Trellix Email Security - Cloud (ETP), this integration uses the Trellix Email Security - Cloud (ETP) API. When you run email Actions, the Trellix Email Security - Cloud (ETP) API will use a verdict (Antispam, Antivirus, Advanced Threat, or Clean) and an action (Delivered, Rejected, or Quarantined) to determine whether the Action has passed or failed.

This integration is remote capable.

Update Trellix Email Security - Cloud (ETP)

Using your IAM account, create an API key for use with the Validation Platform. Verify your key has the same Email Security entitlements used in other API keys.

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Get email metadata	`/api/v1/messages/trace`
Get alert info	`/api/v1/alerts`

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify your Trellix Email Security - Cloud (ETP) host, which is dependent on the region associated with your instance.
- Identify your API key.

Configuration

TO ADD THE TRELLIX EMAIL SECURITY - CLOUD (ETP) INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Trellix Email Security - Cloud (ETP)**.

   You can add this as either a Local or Remote Integration.

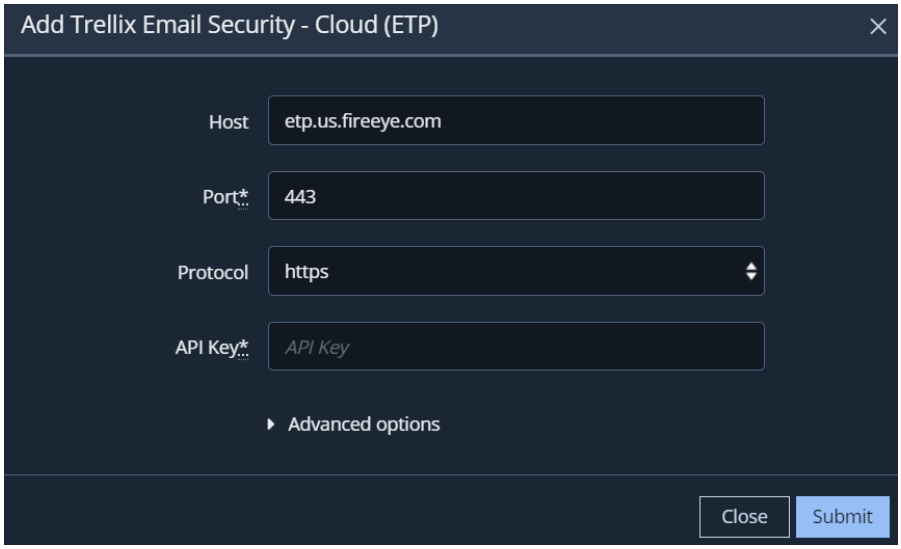
3. Enter information for the **Host**, **Port**, and **Protocol**.
4. Enter your API key.
5. Expand **Advanced options**.

6. (Optional) Update **Query time** and **Delay time**.

> The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. 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.

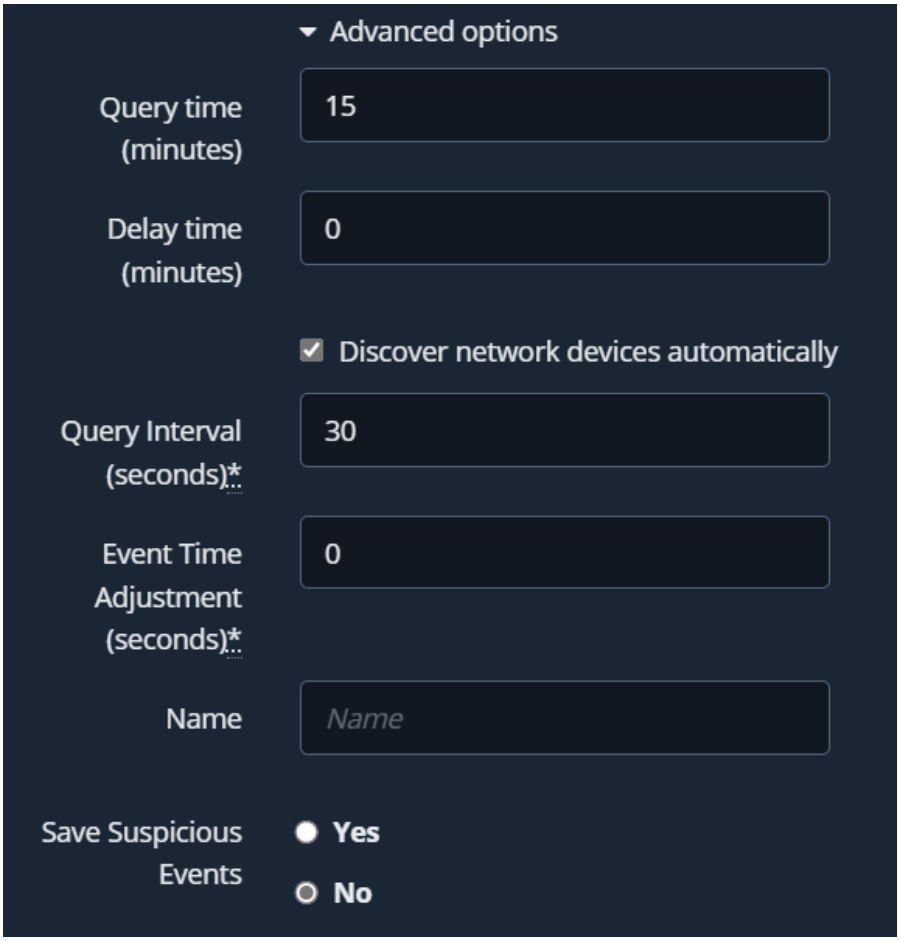
> If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

7. (Optional) Select **Discover network devices automatically**.
8. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
9. (Optional) Assign a **Name**.
10. (Optional) Choose **Yes** to save suspicious events.
11. Click **Submit**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ebf6fa0846174d1601ecf8/n/trellix-email-security-cloud-etp.png)

Trellix Email Security - Cloud (ETP) Integration



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/63ecf35c8cd1f37fec0fe5da/n/trellix-email-security-cloud-etp-advanced-options.png)

Trellix Email Security - Cloud (ETP) Integration - Advanced options

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 TRELLIX EMAIL SECURITY - CLOUD (ETP)

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.