CISCO ADVANCED MALWARE PROTECTION (CISCO AMP) INTEGRATION WITH SECURITY VALIDATION

This integration collect events that are generated by Cisco AMP to test the efficacy and configuration of the security control using Security Validation jobs.

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 feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.** **(https://docs.mandiant.com/home/mandiant-support-cases)**

API calls

API	Usage
`/v1/events`	Returns a list of events from Cisco AMP.
`/v1/version`	Returns information about the API version. Used for check health.

Supported Versions

- Cisco AMP API v1

Before You Begin

To configure this integration, you need the following:

- API Key
- Client ID

Generating the API Key and Client ID

1. Log into the Cisco AMP for Endpoints Console
2. Navigate to Accounts -> API Credentials
3. Click New API Credential to generate a new API Key and Client ID.

Configure Security Validation

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

   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. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **Host** for the Trellix ePO instance.
7. Enter a **Port** value. The default is **443.**

8. Enter the **Username** and **Password** for the account that has permissions to use the API endpoints.
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 **FieldMapModel** 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: 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. If supported by your integration, configure correlation queries:
        i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
        ii. Modify the **Correlation Query Interval**, if necessary (minutes).
    d. 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.

    e. Select **Save Suspicious Events**.
    f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    g. 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.

14. 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 Cisco AMP

Verify that the Director can resolve and communicate to AMP's API, located at **https://api.amp.cisco.com (https://api.amp.cisco.com/)**.

Update the Validation Platform

Prerequisites

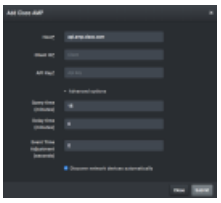
Information to gather before you start:

1. Identify the client ID for AMP communications.
2. Identify the API Key for AMP communications.
    a. Log in to https://console.amp.sourcefire.com (NA) or https://console.eu.amp.sourcefire.com (EU).
    b. From the **Accounts** menu, navigate to the Business Page.
    c. Click **Edit**.
    d. Click **Regenerate** to generate the Client ID and API Key (this button is located under "Features" next to"3rd Party API Access") .

Configuration

TO ADD THE CISCO AMP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** and choose **Cisco AMP**.
3. Enter information for the **Host**, **Client ID**, and **API Key**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12d8c9cba0017c2f7dda/n/cisco-amp.png)

Add Cisco AMP 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 CISCO AMP

Click **Test** to verify that the Director can communicate with the Cisco host using the provided client ID and API key.