VMWARE APPDEFENSE

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 uses HTTPS and Port 443.

This integration is remote capable.

Update VMware AppDefense

You must create a new integration in the integrations section of AppDefense. If the Validation Platform is not listed in the dropdown list, you can use the Splunk option since it generates a normal API key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Your VMware AppDefense Organization ID.
- API Key.

Configuration

TO ADD THE VMWARE APPDEFENSE INTEGRATION

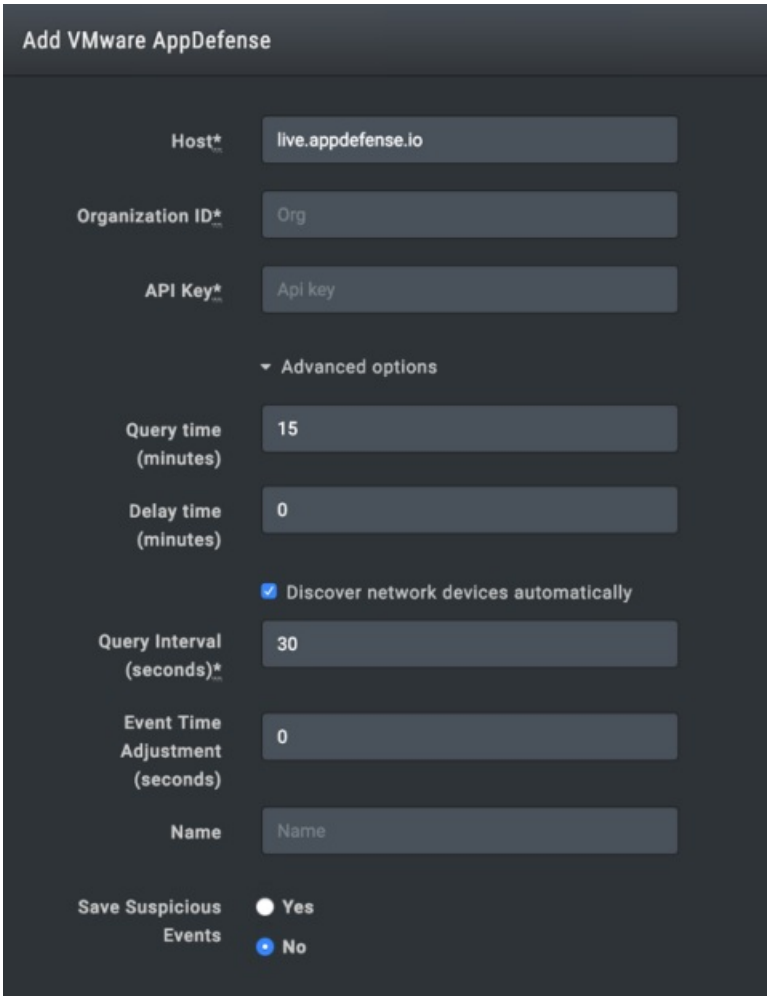
1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **VMware AppDefense**.
3. Enter the **Organization ID**.
4. Enter the **API Key.**
5. Expand **Advanced options**.
6. (Optional) Update **Query time** and **Delay time**.

   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) Clear **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**.



VMware AppDefense Integration

Verify Connectivity

TO VERIFY CONNECTIVITY TO VMWARE APPDEFENSE

Click **Test** to verify that:

- The Director can communicate with VMware AppDefense using the Organization ID specified on the port specified.
- The API key is valid and working.