

ALERTLOGIC

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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).



This integration is remote capable.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- AlertLogic Host.
- AlertLogic API key.

Configuration

TO ADD THE ALERTLOGIC INTEGRATION

1. Go to **Settings > Integrations**.
2. Click **Add Integration > AlertLogic**.
3. Enter the **Host** and the **API Key**.
4. Expand **Advanced options** and update the information if necessary.
5. Click **Submit**.

Add AlertLogic ✕

Host

API Key

▼ Advanced options

Query time (minutes)

Delay time (minutes)*

Query Interval (seconds)*

Event Time Adjustment (seconds)*

Name

Save Suspicious Events Yes No

Verify connectivity

TO VERIFY CONNECTIVITY TO ALERTLOGIC

Click **Test** to verify that the Director can communicate with AlertLogic using the host and API information.