

SENTINELONE

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).

The SentinelOne Integration uses SentinelOne's API to function correctly. Versions 2.0 and 2.1 of the SentinelOne API are supported.

The API request that the SentinelOne integration uses is bound by time limits. The time on the Director and Actor must be kept synchronized, or else no events will match.



This integration is remote capable.

Update SentinelOne

TO UPDATE SENTINELONE

1. Define a username that will be attached to the API key that the Validation Platform will use. The username must have at least Site Viewer access.
2. Use the SentinelOne Portal to generate an API key that can be used in the integration setup in the Director.

Update Security Validation

Prerequisites

Information to gather before you start:

- The SentinelOne API key.
- The name of the host where SentinelOne is installed.
- The Actor configured with the exact name of the host that is running SentinelOne (shown in the SentinelOne Portal).

Configuration

TO ADD THE SENTINELONE INTEGRATION

1. Go to **Settings > Integrations**.
2. Click **Add Integration > SentinelOne**.
3. Enter the **Host**.
This is the SentinelOne address given to the customer by SentinelOne.
4. Enter the **API Key**.
5. Select the **API Version**.
6. (Optional) Update the **Query**.
7. Expand **Advanced options**.
8. (Optional) Update **Query time** and **Delay time**.

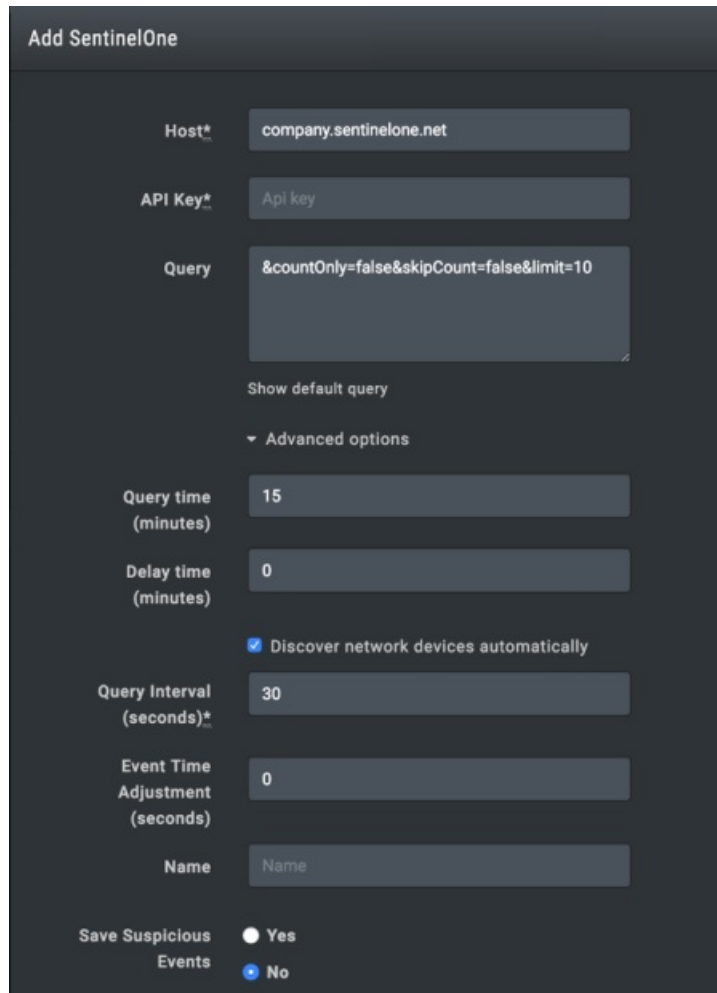


The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query 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.

- (Optional) Clear **Discover network devices automatically**.
- Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
- (Optional) Assign a **Name**.
- (Optional) Choose **Yes** to save suspicious events.
- Click **Submit**.



The screenshot shows a configuration form titled "Add SentinelOne". The form includes the following fields and options:

- Host***: company.sentinelone.net
- API Key***: Api key
- Query**: &countOnly=false&skipCount=false&limit=10
- Show default query**: (checkbox, unchecked)
- Advanced options**: (dropdown menu, expanded)
- Query time (minutes)**: 15
- Delay time (minutes)**: 0
- Discover network devices automatically**: (checkbox, checked)
- Query Interval (seconds)***: 30
- Event Time Adjustment (seconds)**: 0
- Name**: Name
- Save Suspicious Events**: (radio buttons, "Yes" selected)

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 \(https://docs.mandiant.com/home/msv-proxy-rules\)](https://docs.mandiant.com/home/msv-proxy-rules).

Verify Connectivity

TO VERIFY CONNECTIVITY TO SENTINEL ONE

Click **Test** to verify that:

- The Director can communicate with the Sentinel One IP address on the port specified.
- The API key is working and has the necessary privileges.