DARKTRACE

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 integration

Identify or create an API key for use with the Validation Platform. This is done by signing into Darktrace and going to Admin > Config > API Token Generate.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Verify we can read devices	`/devices?seensince=7days`
Get Device Specific Details by IP	`/devices?ip=:ip`
Get Events for Device within specific timeframe	`/details?did=:did&starttime=:start_time&endtime=:end_time`

Update the Validation Platform

Prerequisites

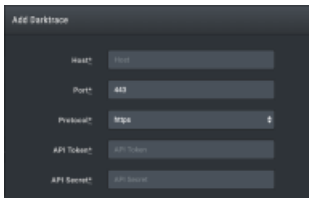
Information to gather before you start:

- Hostname
- Port
- API Key
- API Secret

Configuration

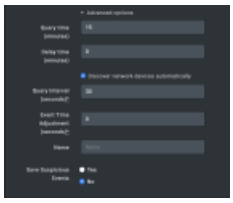
TO ADD THE INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Darktrace**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e9c9cba0017c2f7e8d/n/darktrace1.png)
Darktrace Integration

3. Enter the **Host** and **Port**.
4. Select the **Protocol**.
5. Enter the **API Token** and **API Secret**.
6. Expand **Advanced options**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e7c9cba0017c2f7e7a/n/darktrace-adv.png)
Advanced section of Darktrace Integration

7. (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.

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

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 INTEGRATION

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.

If you see the following error, either the API Key or the API Secret is incorrect or there is a time mismatch:

```
Api signature Error
```

Requests to API are signed with a timestamp. If the requesting machine (Director or Remote Actor) is out of time sync more than a few minutes, the requests will fail.