CARBON BLACK CLOUD

> 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.

Since the API used is the same, the Carbon Black Cloud integration enables the Validation Platform Director to pull events from many of Carbon Black's products, including:

- Carbon Black Cloud
- Carbon Black Defense
- Carbon Black Threat Hunter

Update Carbon Black Cloud

Identify or create credentials to access Carbon Black Cloud with read access, at minimum.

API tokens are tied to user accounts and inherit the user's privileges. When capturing the API key, use an account with the necessary privileges.

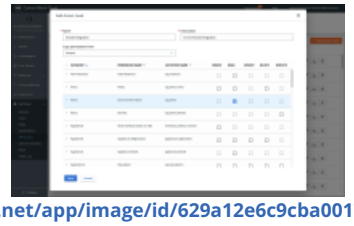
TO IDENTIFY THE API AND ORGANIZATION KEYS

1. Sign into Carbon Black using the appropriate credentials.
2. Navigate in the Carbon Black Cloud console to **Settings > API Access**.
3. Select **Access Levels** and click **+ Add Access Level**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dec9cba0017c2f7e1f/n/cb-api-access.png)

Carbon Black API Access

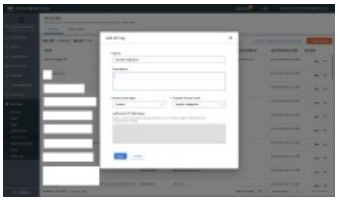
4. Fill in the details for the Access Level and select the **Alerts - General Information - org.alerts - READ permission** and click **Save**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e6c9cba0017c2f7e75/n/cb-add-access-level.png)

Carbon Black Add Access Level

5. Click **API Keys** at the top of the window and click **+ Add API Key**.
6. Name the key and select **Custom** in the **Access Level type** drop-down list; then, select the Access Level you created in step **Select Access Levels and click + Add Access Level.Carbon Black API Access** .



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e2c9cba0017c2f7e4f/n/cb-add-api-key.png)

Carbon Black Add API Key

7. Click **Save** and copy/paste your credentials into the integration.

The Org Key displays in the upper-left of the window.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
default query	/alert/_search

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Port info
- Host info

> Look at the web address of your Carbon Black Cloud console to identify the Host. For more information, see the **Carbon Black documentation (https://developer.carbonblack.com/reference/carbon-black-cloud/authentication/#building-your-base-urls)**.

- Organization Key
- API ID and API Secret Key

Configuration

TO ADD CARBON BLACK CLOUD

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Carbon Black Cloud**.
3. (Optional) Replace the default **Host** value with the host from your Carbon Black Cloud console.
4. Enter the **Port**.
5. Enter the **Organization Key**.
6. Enter the **API ID** and **API Secret Key**.
7. Review and update the **Query**.

8. Expand **Advanced options**.
9. (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.

10. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
11. (Optional) Assign a **Name**.
12. (Optional) Select **Discover network devices automatically**.
13. Click **Submit**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dec9cba0017c2f7e27/n/cb-cloud.png)

Carbon Black Cloud 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 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.