CISCO FIREPOWER MANAGEMENT CENTER (FMC)

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 not remote capable.

Update Cisco FMC

TO UPDATE CISCO FMC

- Configure FMC to enable Database Access.
- Identify or create credentials to access FMC with read permissions, at minimum.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Have the JDBC Driver (see Chapter 2 of the Firepower Systems Database Guide. This file will be in the client.zip)
- Obtain the version of Java that works with FMC; this is `jre-8u181-linux-x64.rpm` and should be approximately 62MB in size.
- Identify the hostname/IP for FMC communications.
- Identify the Port used (this defaults to 2000).
- Open the Ports 1500 and 2000 to allow the system to communicate.
- Obtain a username and password.

Configuration

TO ADD THE CISCO FIREPOWER INTEGRATION

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

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12edc9cba0017c2f7ead/n/cisco-firepower-management.png)

Cisco Firepower Integration

3. If you see a message that Java is not installed, go to the **Upload Java RPM** field, click **Browse**, and select the install file; once you select it, the install will start.

   you will not be able to click **Submit** until Java has finished installing.

4. Enter information for the **Host**, **Port**, **Username**, and **Password**.
5. Review and update the **Query**.
6. Review and update the **File query**.
7. Select the **Version**.
8. Click **Browse**, then select the Client Zip file you downloaded.
9. Expand **Advanced options**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12dec9cba0017c2f7e2b/n/cisco-firepower-management-1.png)

Cisco Firepower Integration (Advanced Options)

10. (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.

11. (Optional) Change the **Java Keystore Password** and **Java Keystore Path**.

> These fields will be pre-populated with the default information and only need to be modified if you've updated the password or path.

12. (Optional) Select the check box **Enable Cisco AMP Support** and adjust the **Amp query** as needed.
13. (Optional) Select the check box **Enable the special query for Host CLI Actions** and add the query.
14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. (Optional) Select **Discover network devices automatically**.
18. Click **Submit**.

> If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

Verify connectivity

TO VERIFY CONNECTIVITY TO CISCO FMC

Click **Test** to verify that the Director can communicate with the Cisco FMC host using the provided host, port, and user credentials.