Mandiant

CISCO FIREPOWER INTEGRATION WITH SECURITY VALIDATION

This integration collects generated events to test the efficacy and configuration of the security control using Security Validation jobs.

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

Configure Cisco FirePower

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

Information to gather before you start:

- Identify the hostname/IP for Cisco FirePower 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.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Cisco FirePower**.

   - Mandiant Security Validation (MSV): You can add this as either a Direct or Remote Integration for on-prem.
   - Mandiant Advantage Security Validation (MA-SV): Because of required dependencies, this can only be added as a Remote Integration for SaaS.

3. Optional. Click the drop-down next to the integration name if you need to change the version.
4. Enter a meaningful **Integration Name**.
5. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
6. Optional: Change the **Protocol** value to determine what protocol is used for requests. The default is **jdbc:vjdbc:rmi**.
7. Enter the **Host** value (hostname or IP address) that you identified for Cisco FirePower communications.
8. Enter a **Port** value. The default is **2000**.
9. Enter the **Username** and **Password** for the account with permissions to access Cisco FirePower.

10. Optional: Enter the **Expected Certificate**. If provided, the certificate is used to verify SSL.

    The certificate, provided as a string value, is checked against the public certificate of the server. If they do not match, an error appears. If omitted, no verification occurs any public certificate from the server is accepted.

11. Add or remove **Query** values.

    - Version 7.2.4 and later: Use the queries labeled `(supports >= v7.2.4)` instead of the equivalents without version numbers. For example, use **IP Intrusion Query (supports >= v7.2.4)** and remove **IP Intrusion Query**.
    - Versions earlier than 7.2.4: remove the queries labeled `(supports >= v7.2.4)` .

12. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

13. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.
14. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. 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, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.

h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

15. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, 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.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

> 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

- Mandiant Security Validation (MSV): You can add this as either a Direct or Remote Integration for on-prem.
- Mandiant Advantage Security Validation (MA-SV): Because of required dependencies, this can only be added as a Remote Integration for SaaS.

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.