DEVO

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 Devo

1. In the Devo UI, navigate to Administration > Credentials > Authentication Tokens.
    a. Grant permissions for each table as needed.
2. Combine all the tables you want to validate into a single union table and name the table my.synthesis.fireeye.data.

    We ask that you do this because each Devo integration supports one table query at a time.

3. Map any relevant fields in your union table to the equivalent fields used by the Devo integration. The following table displays some default union table fields and how they map to the integration's fields.

Union Table Field	Integration Field
srcIp	Source IP
destIp	Destination IP
destPort	Destination Port
srcPort	Source Port

If you try to run a query with the name of a field that does not exist, the query will error. Verify your union table fields are properly mapped to the integration fields.

Supported Integration API Versions

- APIv2

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Query tables for events	/search/query

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify your Devo host, port, and protocol
- Identify your Devo API token

Configuration

TO ADD THE DEVO INTEGRATION

> You can create multiple Devo integrations for the same union table. If you do this, remember to always update the default queries with the correct table and field names.

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Devo**.
3. Enter the Host, Port, and Protocol.
4. Enter your API Token.
5. Update the Query as needed.
6. Expand **Advanced options**.
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) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
9. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
10. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.

    > 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.

11. Identify the field name mappings for the following (there could be multiple of each, depending on log sources and configuration):

    - Source IP

- Destination IP
- Source Port
- Destination Port
- Event Source Host
- Event Start Time (timestamp)
- Event Signature ID
- Event Description
- Email Sender
- Email Recipient
- Email Subject
- URL
- Username

12. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
13. (Optional) Assign a **Name**.
14. (Optional) Choose **Yes** to save suspicious events.
15. Click **Submit**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e9c9cba0017c2f7e87/n/devo.png)

Devo 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 DEVO

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.