Mandiant

DEVO INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Darktrace to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Darktrace to test the efficacy and configuration of security controls 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

API Calls

API	Usage
`/search/query`	Query for events in Devo
`/search/jobs`	Used to test connectivity and authentication settings

Supported Versions

- Devo API v2

Preparation

To configure this integration, you need the API Key of your Devo domain.

Retrieve API Key

1. Sign into Devo.
2. Navigate to **Administration > Credentials**.
3. Select the **Tokens** tab, then click **New Token**.
4. Configure the token as required, then click **Apply**.
5. Click the name of the new token in the table, then copy the token from the window that appears.

Update Devo

1. In the Devo UI, navigate to **Administration > Credentials > Authentication Tokens**.
2. Grant permissions for each table as needed.
3. Combine all the tables you want to validate into a single union table and name the table `my.synthesis.fireeye.data`
4. 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

Configure Security Validation

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

   You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. 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).
5. Enter the **Host** value for the Darktrace instance as a hostname or IP address. The default is **apiv2-us.devo.com**.
6. Enter a **Port** value. The default is **443**.
7. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Http** or **Https**).
8. Enter the **Api Token**.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. 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.

12. Optional: Add or remove **Queries**. Defaults are provided: **IP Query**, **Domains Query**, **Email Query**, and **Hostname Query**.
13. Optional: Change the **Page Size** for upstream server requests. 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 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.