Mandiant

MICROSOFT AZURE LOG ANALYTICS

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)**.

Update Azure Log Analytics

- Identify or create credentials to access Log Analytics with read access, at minimum.
- Verify you have access to the Log Analytics API with Data.Read permission.
- Identify the following values:
  - Client ID
  - Client Secret
  - Tenant ID
  - Workspace ID

These values are generated when you configure Log Analytics. If you have not yet registered Log Analytics as an application in Azure, refer to the **Microsoft documentation** **(https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-register-applications?tabs=app-reg-ga)** for further assistance .

- Set up Tables in Log Analytics.

Queries in the Azure Log Analytics integration will error if corresponding Tables are not configured in Log Analytics. For example, the default Malicious DNS Action Query in the integration needs the DnsEvents table in Log Analytics to be configured.

TO ACCESS THE CLIENT ID, CLIENT SECRET, TENANT ID, AND WORKSPACE ID

If you do not already know the values required to add the Azure Log Analytics integration, you must locate them in the Azure portal.

Refer to the **Microsoft documentation** **(https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-register-applications?tabs=app-reg-ga)** for further assistance identifying these values.

1. In the Azure Log Analytics portal, take note of your **Workspace ID**.
2. In the Azure Active Directory portal, take note of your **Tenant ID**.
3. In the Azure Active Directory portal, navigate to **App registrations** > **New registration**.
4. Enter the required registration information.
   a. Take note of the **Client ID**.
   b. The required **Redirect URI** field can be set to your Director's URL.
5. Navigate to the **Certificates & Secrets** page.
6. Create a new client secret and take note of the value.

TO ADD THE DATA.READ API PERMISSION

1. In the Azure Log Analytics portal, navigate to the **API Permissions** page.
2. Add Log Analytics **Data.Read** permission.
3. Get administrator approval for the application.

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Auth	https://login.microsoftonline.com/{tenent_id}/oauth2/token For Azure Government (GovCloud): https://login.microsoftonline.us/{tenent_id}/oauth2/token
Query Log Analytics	https://api.loganalytics.io/v1/workspaces/{workspace_id}/query For Azure Government (GovCloud): https://api.loganalytics.us/v1/workspaces/{workspace_id}/query

Update the Validation Platform

Prerequisites

This integration requires the Cloud Validation Module.

Information to gather before you start:

- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Tenant ID.
- Identify the Workspace ID.

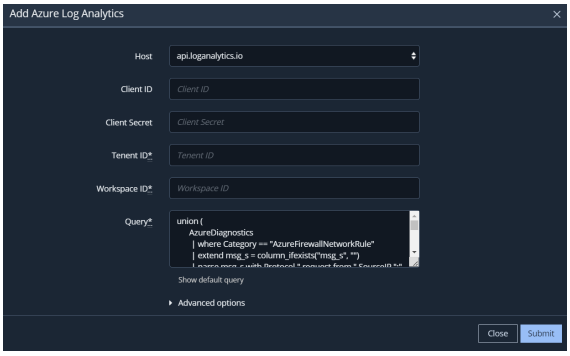
Configuration

TO ADD THE AZURE LOG ANALYTICS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Azure Log Analytics**.

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

3. From the **Host** drop-down list, select the appropriate value depending on your Azure Log Analytics environment:
   - The entry ending in **.io** for standard Azure environments
   - The entry ending in **.us** for Azure Government (GovCloud) environments
4. Enter **Client ID** and **Client Secret**.
5. Enter **Tenant ID** and **Workspace ID**.
6. Modify the **Query**, as necessary.



Microsoft Azure Log Analytics Integration

7. Expand **Advanced options**.
    a. (Optional) Update **Query time (minutes)** and **Delay time (minutes)**.

> 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.

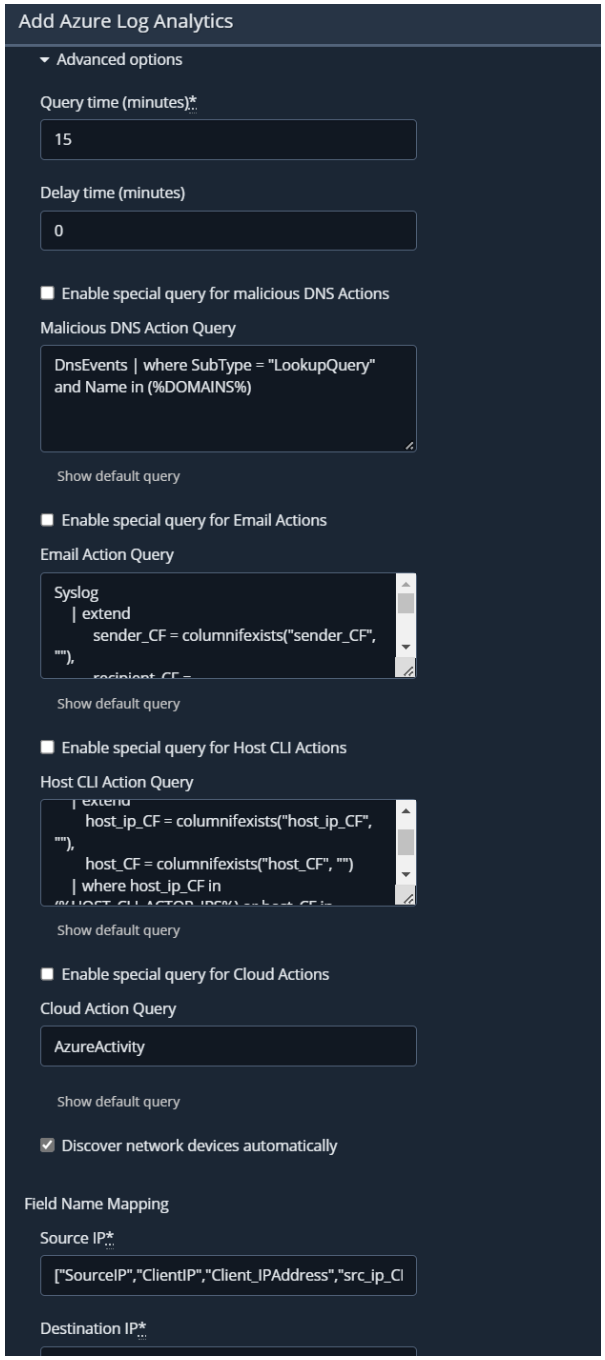
> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

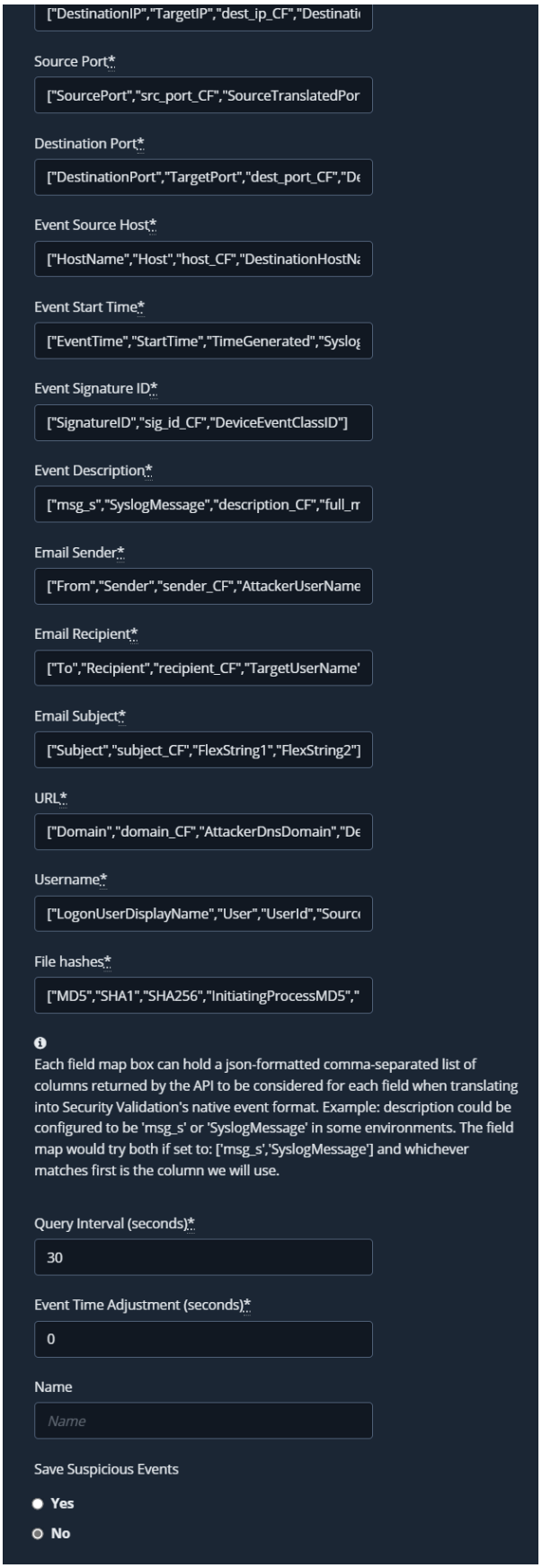
    b. (Optional) Select **Enable query for Malicious DNS Actions** and configure the **Query**. This query will only be used when you run Malicious DNS Actions or Captive DNS Actions.
    c. (Optional) Select **Enable query for Email Actions** and configure the **Query**. This query will be only be used when you run Email Actions.
    d. (Optional) Select **Enable query for Host CLI Actions** and configure the **Query**. This query will only be used when you run Host CLI Actions.
    e. If applicable, select **Enable special query for Cloud Actions** and configure the **Query**.
    f. (Optional) Select **Discover network devices automatically**.
    g. Modify **Field Name Mapping** for the following, as necessary:
        - **Source IP**
        - **Destination IP**
        - **Source Port**
        - **Destination Port**
        - **Event Source Host**
        - **Event Start Time**
        - **Event Signature ID**
        - **Event Description**
        - **Email Sender**
        - **Email Recipient**

- **Email Subject**
- **URL**
- **Username**
- **File hashes**

h. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.
i. (Optional) Assign a **Name**.
j. (Optional) Choose **Yes** to **Save Suspicious Events**.

8. Click **Submit**.





Azure Log Analytics Integration - Advanced Options

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 AZURE LOG ANALYTICS

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.