Mandiant

MICROSOFT AZURE SENTINEL

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).

If you're looking for raw event data, you should implement the **Microsoft Azure Log Analytics** (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics) integration. The integration described here, for Microsoft Azure Sentinel, addresses alerts associated with that event data.

This integration is remote-capable.

Update Microsoft Azure Sentinel

- Identify or create credentials to access Sentinel with read access, at minimum.
- Add the Microsoft Sentinel Reader role to the app that you are creating and registering.
- Verify you have access to the Log Analytics API with Data.Read permission.
- Identify the following values in the Azure Web portal:

  These values are generated when you configure Azure Log Analytics.

  - Client ID
  - Client Secret
  - Tenant ID
  - Workspace ID

- Set up Tables in Log Analytics.

  Queries in the Azure Sentinel 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.

Access the Client ID, Client Secret, Tenant ID, and Workspace ID

If you do not already know the values required to add the Azure Sentinel 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.
- If you have already noted the Client ID, Client Secret, Tenant ID, and Workspace ID for the **Microsoft Azure Log Analytics** (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics) Integration, you can reuse those values for the Azure Sentinel Integration.

1. In the Azure Log Analytics portal, take note of your **Workspace ID**.

2. In the Active Directory portal, take note of your **Tenant ID**.
3. In the 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.

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.

Grant Access to Log Analytics Workspace

1. From your **Log Analytics workspace** overview page, select **Access control (IAM)**.
2. Select **Add role assignment**.
3. Select the **Reader** role and then select **Members**.
4. On the **Members** tab, choose **Select members**.
5. Enter the name of your app in the **Select** box.
6. Select your app and choose **Select**.
7. Select **Review + assign**.

API Calls

The following API calls are used by the Validation Platform.

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

Update the Validation Platform

Prerequisites

Information to gather before you start:

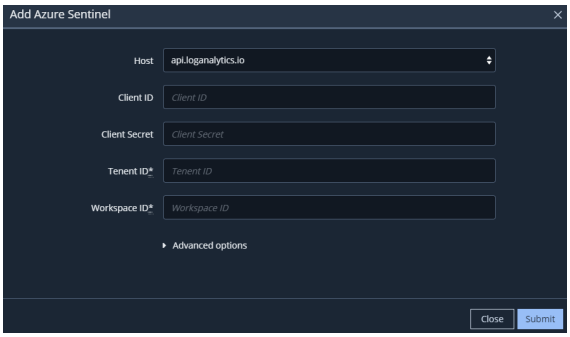
- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Tenant ID.
- Identify the Workspace ID.

Configure the Azure Sentinel Integration

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

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 Sentinel 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**.



Microsoft Azure Sentinel Integration

6. Expand **Advanced options** and update the information as necessary.
   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 **Discover network devices automatically**.
   c. 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**

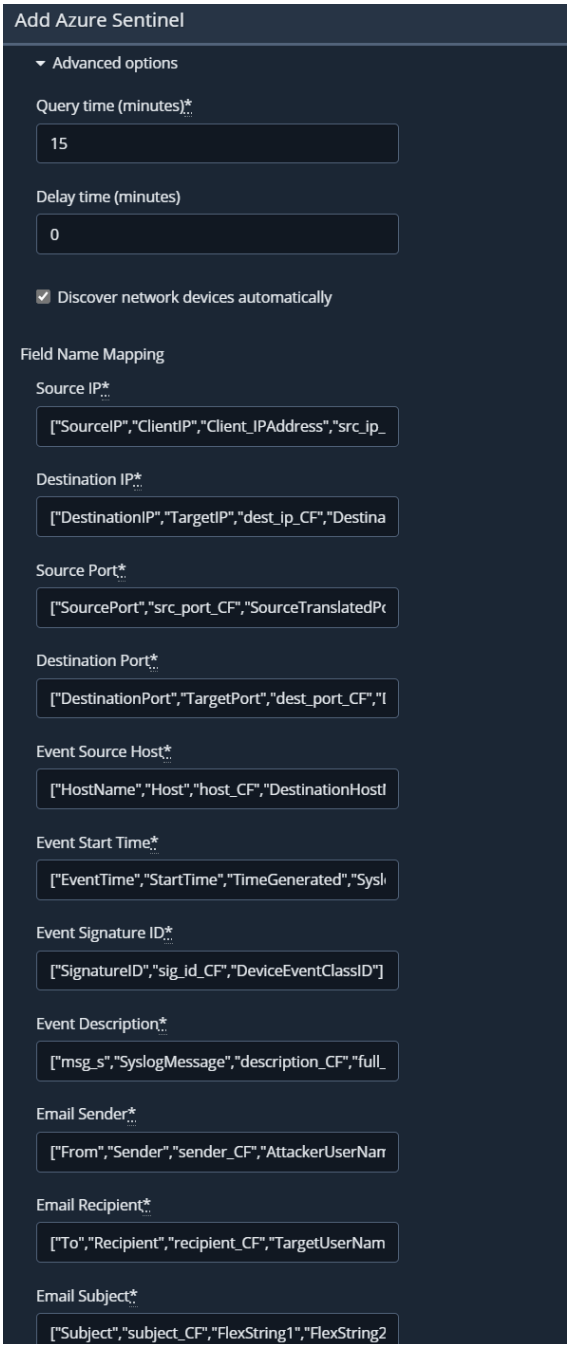
- **Email Subject**
- **URL**
- **Username**
- **File hashes**

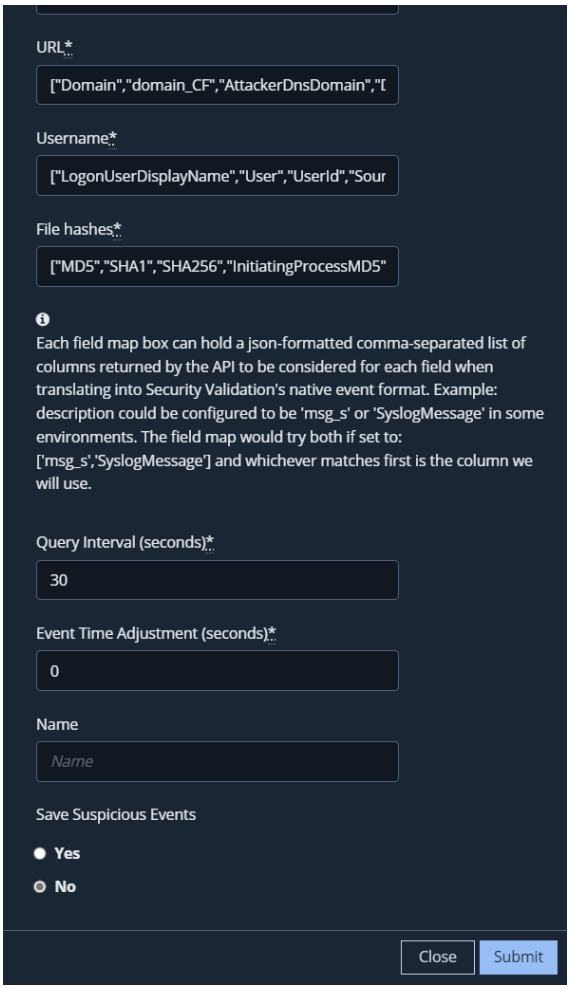
d. Modify the **Query Interval (seconds)** and **Event Time Adjustment (seconds)**, if necessary.

e. (Optional) Assign a **Name**.

f. (Optional) Choose **Yes** to **Save Suspicious Events**.

7. Click **Submit**.





Microsoft Azure Sentinel 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

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.