# Data Connector built for Microsoft Graph API

*Last updated: Jun. 25, 2025*

## Overview

Enhance Next-Gen SIEM detections with Microsoft Graph API data for Microsoft Defender for Office 365 and Azure Active Directory.

> **Note:** This connector uses Microsoft Graph API v1.0 endpoints, which only return interactive logins and successful federated sign-ins. Non-interactive sign-ins are not supported as they are only available in beta endpoints. For more details, see Microsoft Graph API v1.0 [https://learn.microsoft.com/en-us/graph/api/signin-list?view=graph-rest-1.0&tabs=http] and Microsoft Graph API Beta [https://learn.microsoft.com/en-us/graph/api/signin-list?view=graph-rest-beta&tabs=http].

> **Tip:** If you need to configure multiple Microsoft connectors, you can use the Microsoft connector reference table to help with set up and configuration. For more info, see Microsoft connectors [/documentation/page/a76b8289/data-connectors#g7ff80b6].

### Requirements

**Subscriptions:** Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB.

**CrowdStrike clouds:** Available in US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.

**CrowdStrike access and permissions**: Administrator access to the Falcon console for the respective CID.

**Vendor requirements:**

- A **Microsoft Entra ID P1 or P2 license** is required to obtain data from Microsoft Defender.
- Global Administrator access to the Microsoft 365 portal.
- Your environment must include a functioning deployment of one or both of these solutions:
  - Microsoft Defender for Office 365
  - Microsoft Azure Active Directory

## Setup

Set up data ingestion for Microsoft Graph API for Microsoft Defender for Office 365 and Azure Active Directory through the associated app in the CrowdStrike Store.

> **Important:** Some of these steps are performed in third-party products. The CrowdStrike Falcon platform integrates the relevant settings as you configure them. However, CrowdStrike does not validate any third-party configurations. Perform the following steps with care, and validate your settings and values before finalizing configurations in Falcon.

### Configuration summary

Step 1: Register Microsoft application, generate secret, and add permissions [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#r325a0d8]

> **Note:** The Client Secret received from Microsoft Azure AD requires periodic rotation according to the expiration duration that you select.

Step 2: Add permissions for Microsoft Azure AD [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#ca6c4295]

Step 3: Add permissions for Microsoft Defender for O365 [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#dfd90ec0]

Step 4: Configure and activate the Data Connector built for Microsoft Graph API [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#s7d69a74]

Step 5: Set up data connector [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#r803dc31]

Step 6: Verify successful data ingestion [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#bbc3a3c5]

### Step 1: Register Microsoft application, generate secret, and add permissions

These steps are performed in the administration interfaces of your Microsoft Azure and Microsoft Graph API instances. For more detailed info, see Get access without a user [https://learn.microsoft.com/en-us/graph/auth-v2-service] and additional Microsoft product documentation for managing API applications.

1. Login as Global Administrator, and go to **Microsoft Azure Active Directory > Application > App registrations**.
2. Click **New Registration**.
3. In **Register an application**, enter the following details:
   - **Name:** Example, Falcon Next-Gen SIEM.
   - **Supported account types:** Select **Accounts in this organizational directory only ("Organization's Name" only - Single tenant)**.
   - Click **Register**.
4. In **Overview**, save the **Application (Client) ID** value and the **Directory (Tenant) ID** value. These are used later in the Falcon Microsoft application configuration.

5. In **Client credentials**, click **Add a certificate or secret**.

6. Click **Client secrets**.

7. Click **New client secret**.

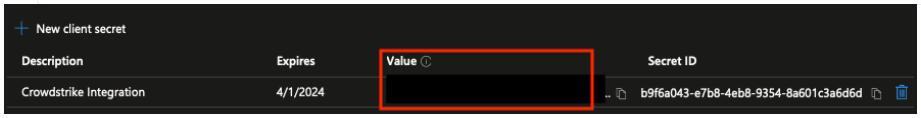
8. Provide a description (name) and the expiration interval.

> **Note:** The expiration interval is based on your environment, and determines how often the client secret needs to be regenerated.

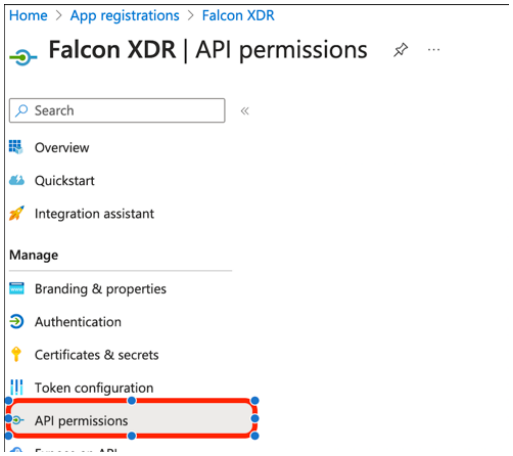
9. Click **Add**.

> **Note:** Save the client secret, which appears in the **Value** field. This is the only opportunity to save it as it isn't displayed again.

> **Important:** The client secret **Value** poses a security risk if compromised. We recommend deleting it after you enter it in a later step.

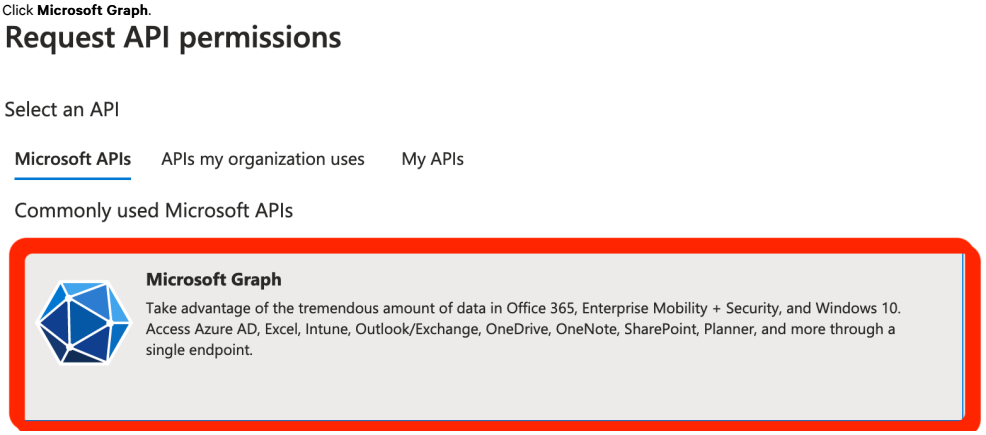



10. Click **API Permissions**.




11. Click **Add a Permission**.

12. Click **Microsoft Graph**.




13. Click **Application permissions**.

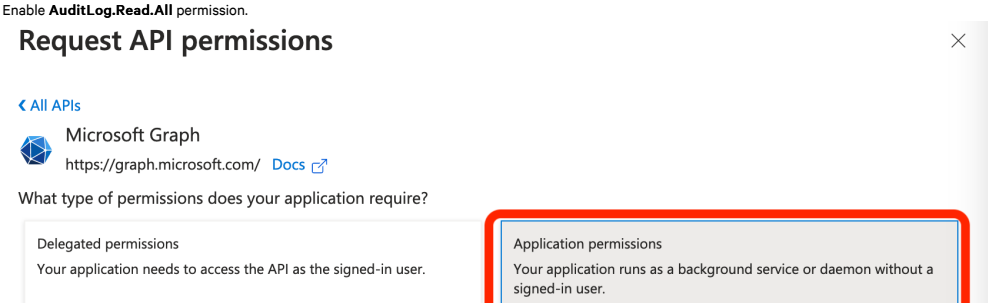
## Step 2: Add permissions for Microsoft Azure AD

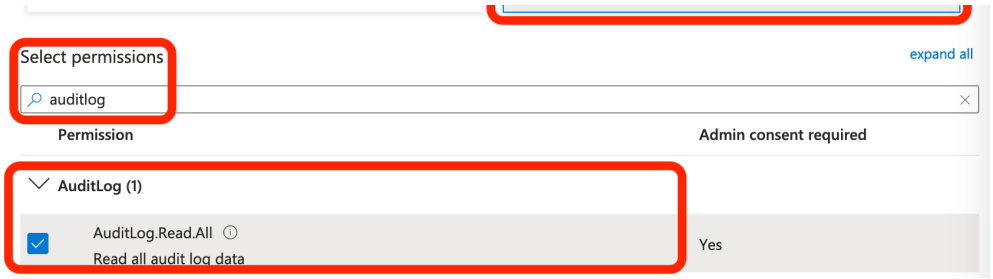
In the administration interfaces for your instance of Microsoft Azure and Microsoft Graph API, configure Microsoft API application settings. For more detailed info, see Get access without a user [https://learn.microsoft.com/en-us/graph/auth-v2-service] and additional Microsoft product documentation for managing API applications.

> **Note:** The following steps show parameters for Azure AD. If you are not configuring Azure AD, move on to step 3 for Defender for Office 365 Alerts permissions.

1. In the Select Permissions field, enter **auditlog**.

2. Enable **AuditLog.Read.All** permission.






3. Click **Add permissions**.

4. In the API permissions window click **Grant admin consent**.

5. In the Grant admin consent confirmation window, click **Yes**.

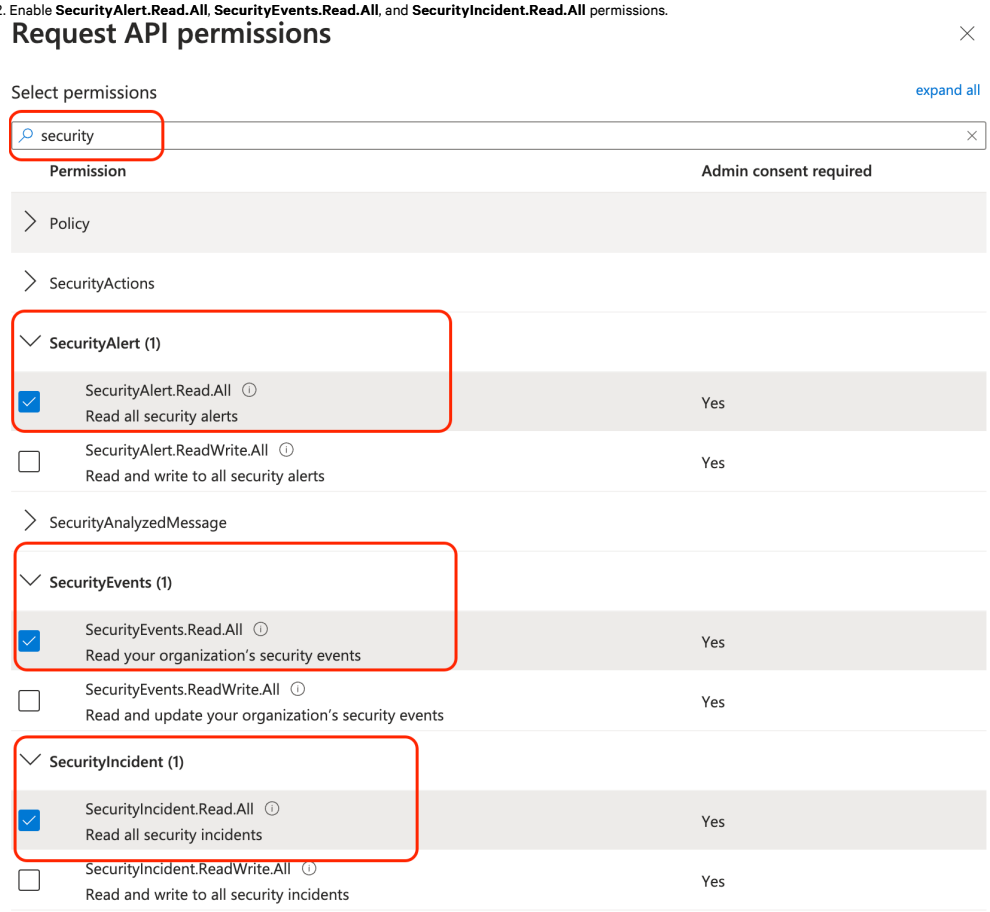
## Step 3: Add permissions for Microsoft Defender for O365

In the administration interfaces for your instance of Microsoft Azure and Microsoft Graph API, configure Microsoft API application settings. For more detailed info, see Get access without a user [https://learn.microsoft.com/en-us/graph/auth-v2-service] and additional Microsoft product documentation for managing API applications.

> **Note:** These steps show parameters for Defender for Office 365 Alerts. If you are not integrating this product data, skip Step 3.

1. In the Select Permissions field, enter **security**.

2. Enable **SecurityAlert.Read.All**, **SecurityEvents.Read.All**, and **SecurityIncident.Read.All** permissions.




3. Click **Add permissions**.

4. In the API permissions window, click **Grant admin consent**.

5. In the Grant admin consent confirmation window, click **Yes**.

## Step 4: Configure and activate the Data Connector built for Microsoft Graph API

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.

2. Click **+ Add connection**.

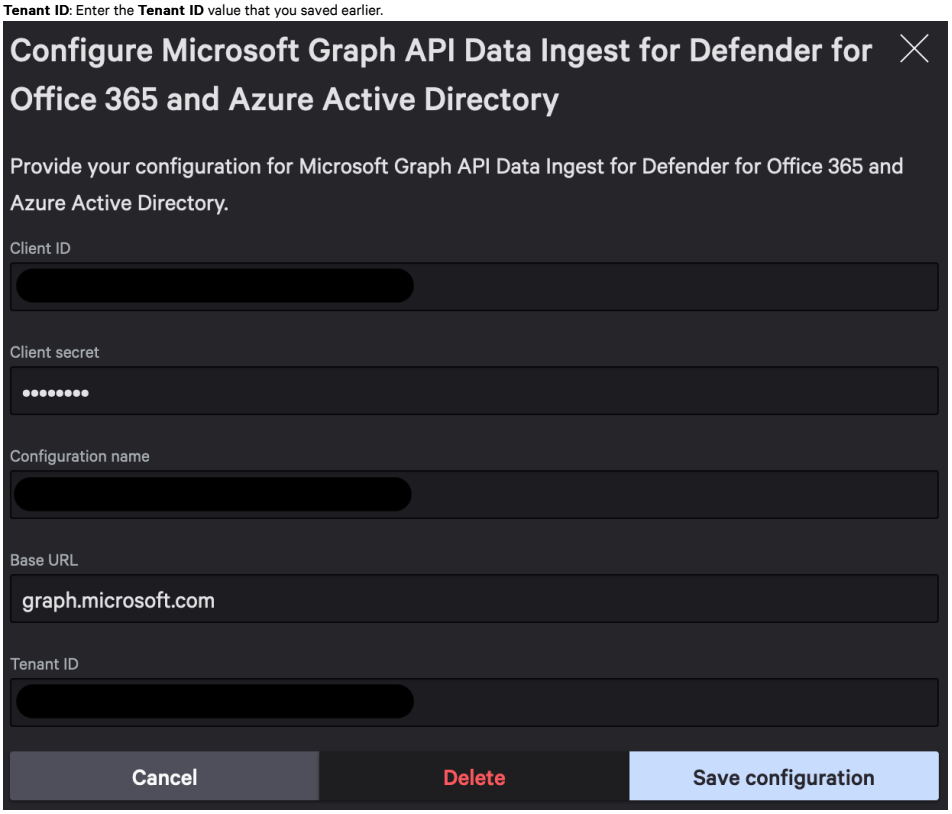
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.

4. In the **New connection** dialog, review connector metadata, version, and description. Click **Configure**.

   > **Note:** For connectors that are in a **Pre-production** state, a warning dialog appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.

6. Enter the following values:
    - **Client ID**: Enter the **Client ID** value that you saved earlier.
    - **Client Secret**: Enter the client secret **Value** that you saved earlier.
    - **Configuration name**: Enter a name for your configuration.
    - **Base URL**: Enter **graph.microsoft.com**
    - **Tenant ID**: Enter the **Tenant ID** value that you saved earlier.




7. Click **Save configuration**.
8. In the **Data connector configuration** field, select the configuration you just created.
9. Enter a name and an optional description to identify the connector.
10. Click the **Terms and Conditions** box, then click **Save**.

## Step 5: Set up data connector

Set up your data connector to ingest data from Microsoft.

1. In the Falcon console, go to **Data connectors > Data connectors > Data sources [/data-connectors/]**.
2. Select the **Data Connector built for Microsoft Graph API** app.
   The **Add new connector** page opens.
3. In the **Data souce configuration** field, select the configuration you created in
   Step 4: Configure and activate the Data Connector built for Microsoft Graph API [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#s7d69a74]
   .
   Optional. To add, edit, or delete a configuration, click **Manage configurations** and follow the steps in
   Step 4: Configure and activate the Data Connector built for Microsoft Graph API [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api#s7d69a74]
   .
4. In the **Connector name** field, enter a name for your connector.
   Optional. In the **Description** field, enter a description for your connector.
5. Select the box to agree the Terms and Conditions [https://www.crowdstrike.com/terms-conditions/].
6. Click **Save**.

> **Note:** Configuring a data source with multiple products creates a new data connector for each product supported by the data source. A confirmation message displays the names of your new connectors.

## Step 6: Verify successful data ingestion

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.

2. In the **Status** column, verify data connection status is **Active**.

3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.

4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#Vendor=microsoft | #event.module=defender
```

or

```
#Vendor=microsoft | #event.module=azure
```

# Data reference

## Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Threat:Indicator:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#s455fd5m]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

< Data Connector built for Microsoft Exchan Data Connector built for Microsoft IIS > [/documentation/page/l5e17e69/data-connector-built-for-microsoft-iis]