Data Connector built for Microsoft DLP

Last updated: Jun. 25, 2025

Overview

Ingest Microsoft data loss prevention (DLP) logs into Falcon Next-Gen SIEM using the Office 365 Management Activity API for threat detection, investigation, and further analysis.

Requirements

Subscription: 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.

Additional requirements:

- Global Administrator access to the Microsoft 365 portal.
- An active Office 365 subscription.
- An active Azure subscription associated with your Office 365 subscription.
- Office 365 unified auditing is enabled for your organization to pull records through the Management Activity API. For instructions, see Turn audit log search on or off [https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?tabs=microsoft-purview-portal].
- Administrator access to the Falcon console.
- Availability of the **Data Connector built for Microsoft DLP** app in the CrowdStrike Store

  > **Note:** If the app is not available, contact your sales engineer to have it enabled or provisioned.

Setup

> **Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Step 1: Register Microsoft application and generate secret

These steps are performed in the administration interface of the Microsoft Azure portal.

1. In the Microsoft Azure portal, go to **App registrations**.
2. Click **New registration**.
3. In **Register an application**, enter this info:
   a. **Name**: Enter an application name, for example, `CrowdStrike NG-SIEM - Microsoft DLP`. Save this **Application Name** to enter in a later step.
   b. **Supported account types**: Select **Accounts in this organizational directory only ("Organization's Name" only - Single tenant)**
4. Click **Register**.
5. In **Overview**, save the **Application (Client) ID** value and the **Directory (Tenant) ID** value.

   > **Note:** These values are used in a later step to set up the data connector in the Falcon console.

6. In the **Manage** section, click **Certificates & secrets**.
7. Click **Client secrets**.
8. Click **New client secret**.
9. Enter a description and the expiration interval.

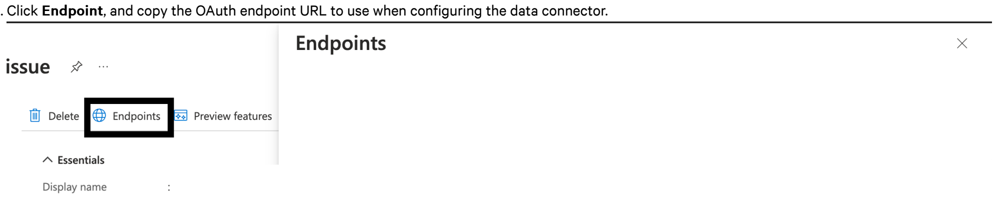
   > **Note:** The expiration interval is based on your environment and determines how often the client secret needs to be regenerated.

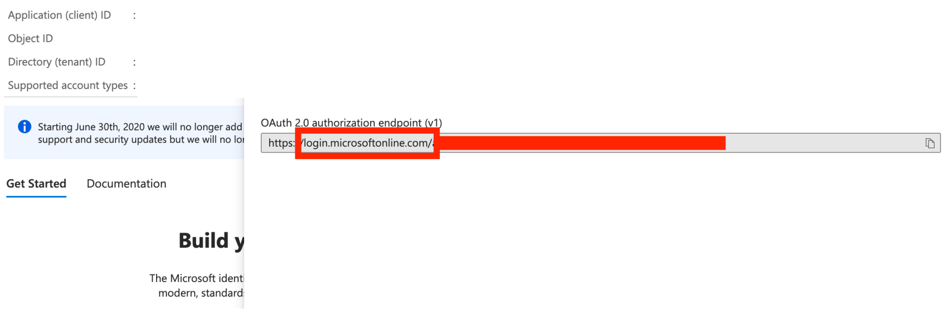
   > **Important:** The data connector will stop ingestion once client secret expires.

10. Click **Add**.

    > **Important:** Save the client secret in the **Value** field somewhere safe as it is sensitive info displayed only once and required later to configure the Data Connector built for Microsoft DLP.

11. Click **Endpoint**, and copy the OAuth endpoint URL to use when configuring the data connector.





Application (client) ID :

Object ID

Directory (tenant) ID :

Supported account types :

Starting June 30th, 2020 we will no longer add
support and security updates but we will no lo

Get Started

Documentation

Build y

The Microsoft ident
modern, standard

OAuth 2.0 authorization endpoint (v1)

https://login.microsoftonline.com/[redacted]

For example, in this instance the Auth URL is `login.microsoftonline.com`.

Step 2: Add permissions for Microsoft DLP

These steps are performed in the administration interface of the Microsoft Azure portal.

1. In the **Manage** section, click **API permissions**.
2. Click **Add a permission**.
3. Click **Office 365 Management APIs**.
4. Click **Application permissions**.
5. In the **Select Permissions** field, enter `ActivityFeed.ReadDlp` and enable the **ActivityFeed.ReadDlp** permission.
6. Click **Add permissions**.
   The **ActivityFeed.ReadDlp** permission appears in the **Configured permissions** section.
7. In **API permissions**, click **Grant admin consent**.
8. In the **Grant admin consent** confirmation, click **Yes**.

Step 3: Configure and activate the Data Connector built for Microsoft DLP

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**.
5. **Note:** For connectors that are in a **Pre-production** state, a warning dialog appears. Click **Accept** to continue configuration.
6. In the **Add new connector** page, click **Manage configurations**.
7. 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**: Choose the Base URL by Office 365 subscription plan for your organization.
     - **Enterprise plan:** `manage.office.com`
     - **GCC government plan:** `manage-gcc.office.com`
     - **GCC High government plan:** `manage.office365.us`
     - **DoD government plan:** `manage.protection.apps.mil`
   - **Tenant ID**: Enter the Tenant ID value that you saved earlier.
   - **Auth URL:** Enter the Auth URL value that you saved earlier.
8. Click **Save configuration**.
9. In the **Data connector configuration** field, select the configuration you just created.
10. In the **Connector name** field, enter a name for your connector.
11. Optional. Enter a **Description** for the connector.
12. Review and agree to the terms and conditions.
13. Click **Save**.

Step 4: Verify successful data ingestion

> **Tip:** Wait at least 15 minutes after setup to allow initial event data to be generated. If you do not see the raw data after 15 minutes, the product might need more time. Search results aren't generated until an applicable event occurs.

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

1. Go to Data connectors > Data connectors > My connectors [/data-connectors/connectors] and click your connector's name to view the connector details.
2. Verify that the status of the data connector is **Active**.
3. After a few minutes, refresh the page to confirm that data ingestion is successful by verifying numerical values in **Last ingested (UTC)** timestamp and the **Last ingested amount**.
4. Go to Next-Gen SIEM > Log management > Advanced event search [/investigate/search].
5. On the **Search** tab, select **Third Party** as your data source.
6. Run a search for the data you ingested with this query: `#repo = "3pi_microsoft_dlp"`

Data reference

Next-Gen SIEM events

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

- Email:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#f5yqjx4f]
- File:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i2xbijpg]
- File:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t3em9j85]
- File:Creation:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#g2in7h52]
- File:Deletion:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m2l5h6y8]
- File:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#y4016g3a]
- Iam:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w2o4xy4u]
- Iam:Creation:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#r6v4uftm]
- Iam:Deletion:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v1nlikck]
- Iam:User:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#u8x1u9jm]
- Iam:Group:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#l716zkv7]
- Authentication:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v3639xkr]
- Authentication:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v9a3adya]
- Configuration:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w71kufuj]
- Configuration:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vkl]
- Configuration:Creation:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#n9xgygup]
- Configuration:Deletion:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v267j0ck]
- Configuration:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Api:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#q01fldxq]
- Database:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#u7cc7mhg]
- Web:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p9vhn5jb]

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 Micr Data Connector built for Microsoft Entra ID > [/documentation/page/zd4ca92c/data-connector-built-for-microsoft-entra-id]