# Data Connector built for Microsoft Defender for Cloud

*Last updated: Jun. 25, 2025*

## Overview

Ingest alerts from Microsoft Defender for Cloud for further analysis, threat detection and investigation.
Microsoft Defender for Cloud alerts [https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference] cover a number of security issues such as anomalous access patterns, suspicious user behaviors, malicious configurations, and so on.

> **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

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

**Default roles**:

- Falcon Administrator
- Connector Manager

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

**Additional requirements**:

- Your environment must include a functioning deployment of Microsoft Defender for Cloud
- You must have an active subscription to Microsoft Event Hubs
- Global Administrator or Security Administrator access to the Microsoft Defender for Cloud portals
- Administrator access to the Falcon console for the respective CID
- Access to the **Data Connector built for Microsoft Defender for Cloud** app in the CrowdStrike Store

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

## Setup

Set up data ingestion for Microsoft Defender for Cloud through Event Hubs and the data connector in the Falcon console. For more info, see the Microsoft Azure Event Hubs [https://learn.microsoft.com/en-us/azure/event-hubs/] documentation.

> **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

Register your Microsoft application in the administration interface for your Microsoft 365 instance and generate a client secret:

1. In the Microsoft Azure portal, go to **Microsoft Entra ID > App registrations**.
2. Click **New Registration**.
3. In **Register an application**, enter this info:
    - **Name:** Enter an application name, for example, `CrowdStrike NG-SIEM - Microsoft Defender for Cloud Event Hub Stream`. Save this **Application Name** to enter in a later step.
    - **Supported account types:** Select **Accounts in this organizational directory only (Crowdstrike only - Single tenant)**.
4. Click **Register**.
5. In **Overview**, save the **Application (client) ID** value and the **Directory (tenant) ID** values.

    > **Note:** This info is used later to configure the **Data Connector built for Microsoft Defender for Cloud**.

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

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 Defender for Cloud.

# Step 2: Create Event Hubs

Create Event Hubs in the administration interface of your Microsoft 365 instance:

1. Click **Event Hubs** in the **Services** section of the **Microsoft Azure services portal** page.
   The **Event Hubs** page opens.
2. Click **Create**.
3. In **Create Namespace (Event Hubs)**, enter the following info:
   a. In the **Basics** tab:
      i. **Subscription**: Select your Azure subscription.
      ii. **Resource Group**: Click **Create new**, enter a **Name** for this resource group, and then click **OK**.
      iii. **Namespace name**: Enter a unique name.

      > **Note:** Save this **Event Hubs Namespace** name to enter in a later step.

      iv. **Location**: Select the nearest location to you.
      v. **Pricing Tier**: Select a plan.

      > **Note:** The Microsoft **Basic** pricing tier does not allow Microsoft Defender XDR events.

      vi. **Throughput Units**: Select the number of units. For more info, see
      Throughput units [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-faq#throughput-units].
      vii. Optional. **Enable Auto-inflate:** If you want to automatically scale up the number of throughput units to meet your usage needs, select this checkbox.
   b. In the **Advanced** tab:
      i. **Minimum TLS version**: Select **Version 1.2**.
      ii. **Local Authentication**: Select **Enabled**.
   c. In the **Networking** tab:
      i. **Connectivity method:** Select **Public access**.
   d. Optional. In the **Tags** tab, add tags as needed.
   e. In the **Review + create** tab:
      i. Review the namespace details
      ii. Confirm the **Validation succeeded** message
      iii. Click **Create**.

      > **Note:** After the creation process finishes, the following message appears: `Your deployment is complete.`

4. In **Next steps**, click **Go to resource**.
5. Click **+ Event Hub**.
6. In the **Event Hub** page, in the **Basics** tab, enter the following info:
   a. **Name**: Enter a name. Save this **Event Hub Name** to enter in a later step.
   b. **Partition count**: Select the number of partitions. For more info, see
   Partitions [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-faq#partitions].
   c. **Cleanup policy**: Select **Delete**.
   d. **Retention time (hrs)**: Enter the number of hours. For more info, see
   What is the maximum retention period for events? [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-faq#what-is-the-maximum-retention-period-for-events-]
7. Click **Review + create**.
8. After the **Validation succeeded** message appears, click **Create**.
9. In **Event hubs,** clickonthe **Event hub** that you created earlier.
10. Click **Access control (IAM)**.
11. Click **Add role assignment**.
    a. Search for **Azure Event Hubs Data Receiver**.
    b. Select **Azure Event Hubs Data Receiver**.
    c. Click **Next**.
    d. Click **+ Select Members**.
    e. Search for the **Application Name** value that you saved earlier in
    Step 1: Register Microsoft application and generate secret [/documentation/page/ze713e6a/data-connector-built-for-microsoft-defender-for-cloud#y51948d0]
    .
    f. Select the **Application Name**.

g. Click **Select**.

h. Click **Review + assign**.

i. Click **Review + assign**.

12. In the **Role assignments** tab, confirm that the new role assignment is listed.

## Step 3: Save the namespace Essentials Id value

Save the **Essentials Id** value for your new namespace in the administration interface for your Microsoft 365 instance.

1. Log in to the Microsoft Azure portal as a Global Administrator or Security Administrator, and then click **Event Hubs**.
2. Click your new Event Hubs namespace that you created in Step 2: Create Event Hubs [/documentation/page/ze713e6a/data-connector-built-for-microsoft-defender-for-cloud#z490fd70].
3. Click **Properties**.
4. Save the **Essentials Id** value to enter in a later step.

## Step 4: Verify successful data ingestion to Event Hubs

Configure Event Hubs and Microsoft Defender for Cloud in the administration interface for your instance of Microsoft Azure:

1. Click **Microsoft Defender for Cloud** in the **Services** section of the **Microsoft Azure services portal** page.
   The **Microsoft Defender for Cloud** page opens.
2. In the **Management** section of the left navigation panel, click **Environment settings**.
3. On the **Environment settings** page, **click** on your **Azure subscription**.
4. In the **Settings** section of the navigation menu, click **Continuous export**.
5. Click the **Event hub** tab.
6. Set the **Export enabled** setting to **On**.
7. In the **Exported data types** section, check **Security alerts** and select all severity levels: **Low,Medium,High,Informational**.
8. In the **Export frequency** section, check **Streaming updates**.
9. In the **Export target** section, select this information:
   - **Subscription:** Your Azure subscription
   - **Event Hub namespace** that you saved earlier.
   - **Event Hub name** that you saved earlier.
   - **Event Hub policy name** as **sender**.
10. Click **Save**.

## Step 5: Verify successful Event Hubs configuration

Verify if Microsoft Defender for Cloud is streaming data to the configured Event Hubs successfully:

1. Log in to the Microsoft Azure portal as a Global Administrator or Security Administrator, and then click **Event Hubs**.
2. Click your new Event Hubs namespace that you created in Step 2: Create Event Hubs [/documentation/page/ze713e6a/data-connector-built-for-microsoft-defender-for-cloud#z490fd70].
3. On the created **Event Hubs Namespace** page in the Azure portal, verify successful Event Hub configuration with incoming data statistics in the **Messages** chart.

## Step 6: Configure and activate the Data Connector built for Microsoft Defender for Cloud

Follow these steps to configure the **Data Connector built for Microsoft Defender for Cloud** application:

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:
   - **Name:** Enter a name for your configuration.
   - **EventHub Name:** Enter the **Event Hub Name** value that you saved earlier.
   - **EventHub Namespace:** Enter the **Event Hubs Namespace** name that you created earlier.

- **Client ID:** Enter the **Application (Client) ID** value that you saved earlier.
- **Tenant ID:** Enter the **Directory (Tenant) ID** value that you saved earlier.
- **Client Secret:** Enter the client secret **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 7: 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:

```
#repo = "msdefender-for-cloud"
```

# 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]
- Authentication:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- Process:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#p5eme1kf]
- File:Deletion:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#m2l5h6y8]

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

‹ Dat Data Connector built for Microsoft Defender for Identity › [/documentation/page/qa99cc3d/data-connector-built-for-microsoft-defender-for-identity]