Data Connector built for Microsoft Defender XDR Events

Last updated: Jun. 25, 2025

Overview

Ingest Advanced Hunting Events [https://learn.microsoft.com/en-us/microsoft-365/security/defender/supported-event-types?view=o365-worldwide] from Microsoft Defender XDR for analysis, threat detection, and investigation with the Data Connector built for Microsoft Defender XDR. Advanced Hunting Events from Microsoft Defender XDR allow you to proactively search for and investigate potential threats across your organization using information from a suite of Microsoft security products.

> **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.

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

CrowdStrike access and permissions: Administrator or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements

- You must have an active subscription to Microsoft Event Hubs.
- Global Administrator or Security Administrator role to register an application and validate an event hub.
- Owner or User Access Administrator role to add a role assignment. For more info, see Create a Microsoft Entra app & service principal in the portal [https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal].
- Your environment must include a functioning deployment of Microsoft Defender XDR.

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.

Set up data ingestion for Microsoft Defender XDR 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:** Read this information before setup.

- If you are configuring multiple Microsoft data connectors, each data connector should connect to its own dedicated Event Hub.
- You can use a single Event Hub Namespace to host multiple Event Hubs. The number of Event Hubs permitted per namespace depends on your subscription tier. To learn more about how many Event Hubs you can host per namespace, see Basic vs. standard vs. premium vs. dedicated tiers [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-quotas#basic-vs-standard-vs-premium-vs-dedicated-tiers].
- Microsoft Entra ID application credentials are required for data connector configuration in Step 8 of this guide. If you already have an Microsoft Entra ID application and Event Hub set up that you wish to configure with this data connector, you can begin at setup at Step 4.

Step 1: Register Microsoft application and generate secret

1. In the Microsoft Azure portal, search and select **Microsoft Entra ID**.
2. In the Microsoft Entra ID **Overview** page, click **+ Add > App registration**.
   The **Register an application** page opens.
3. On the **Register an application** page, enter this info:
   a. **Name:** Enter an application name. Save this name to enter in a later step.
   b. **Supported account types:** Choose the account type based on your organization's requirements. We recommend choosing **Accounts in this organizational directory only** based on least privilege access. For more info, see Identity and account types for single- and multitenant apps [https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types].
   c. Click **Register**. The **Application** page opens with a **Successfully created application** notification.
4. In the **Essentials** section on the **Application** page, copy and save the **Application (client) ID** and the **Directory (tenant) ID** values to use in a later step.
5. In the navigation menu, click **Manage > Certificates & secrets**.
   The **Certificates & secrets** page appears.
6. Click the **Client secrets** tab and click **+ New client secret**.
   The **Add a client secret** dialog opens.
7. Enter a description for the client secret and a client secret expiration time. The expiration interval is based on your environment and determines how often the client secret needs to be regenerated.
8. Click **Add**. Your new client is now listed in the **Client secrets** tab with a **Successfully updated application credentials** notification.
9. Copy the **Value** field and save it somewhere safe to enter in a later step.

   > **Note:** This sensitive info is displayed only once and is required for data connector configuration in a later step.

Step 2: Create an Event Hub Namespace

> **Note:** If you already have an Event Hub Namespace and Event Hub created, skip to Step 4: Add role assignment [/documentation/page/j06b4388/data-connector-built-for-microsoft-defender-xdr#tda0cfb9].

1. In the Microsoft Azure portal, search for and select **Event Hubs**.
   The **Event Hub** page opens.

2. Click **+ Create**.
   The **Create Namespace** page opens.

3. In the **Basics** tab, set or input the **Project** and **Instance Details**:

   - **Subscription:** Select your Azure subscription.
   - **Resource Group:** Choose an existing resource group or click **Create new**, enter a **Name** for this resource group, and then click **OK**.

     > **Note:** Only choose an existing resource group if that group hosts resources that share the same lifecycle, access controls, environment, or location as the resources in your Namespace.

   - **Namespace name:** Enter a unique name. Save this Event Hub Namespace name to enter in a later step.
   - **Location:** Select a region to support availability zones for this namespace. For more info, see What are Azure availability zones? [https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview?tabs=azure-cli#configuring-resources-for-availability-zone-support]
   - **Pricing Tier:** Select a plan. Minimum required plan is the **Standard** tier. Based on your tier, select additional configuration options:
     - **Throughput Units:** Select the number of units. Default is 1.

       > **Important:** Sending data from Event Hubs to this connector is limited to a maximum of 2MB per second. You can purchase additional throughput units and set this to a higher number to scale up to 2MB per second. For more info about selecting throughput units, see Scaling with Event Hubs [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability].

     - Optional. **Enable auto-inflate:** Check the box if you want throughput units to automatically increase based on your usage. For more info about auto-inflate, see Automatically scale up Azure Event Hubs throughput units (standard tier) [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-auto-inflate].

4. In the **Advanced** tab, select **Security** measures:

   - **Minimum TLS version:** Select a minimum TLS version. We recommend Version 1.2. For more info, see Configure the minimum TLS version for an Event Hubs namespace [https://learn.microsoft.com/en-us/azure/event-hubs/transport-layer-security-configure-minimum-version]
     .
   - **Local Authentication:** Select **Enabled** or **Disabled** based on your requirements. For more info about local authentication, see Authenticating Event Hubs Consumers with SAS. [https://learn.microsoft.com/en-us/azure/event-hubs/authenticate-shared-access-signature#authenticating-event-hubs-consumers-with-sas]

5. In the **Networking** tab, choose a **Connectivity method**. For more info about connectivity methods, see Allow access to Azure Event Hubs namespaces from specific IP addresses or ranges [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-ip-filtering].

6. Optional. In the **Tags** tab, add tags as needed.

7. In the **Review + create** tab, complete these tasks:

   a. Review the namespace details.

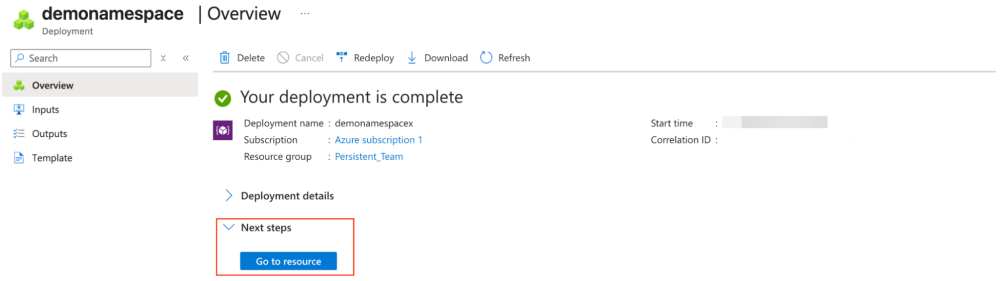
   b. Confirm the **Validation succeeded** message.

   c. Click **Create**.

   d. The deployment **Overview** page opens. Confirm successful namespace creation with the **Your deployment is complete** message on screen.

Step 3: Create an Event Hub

1. In the **Next steps** section, click **Go to resource**.



   The namespace **Overview** page opens.

2. Click **+ Event Hub**.
   The **Create Event Hub** page opens.

3. In the **Basics** tab, enter **Event Hub Details** and set **Retention** settings:

   - **Name:** Enter a name. Save this event hub name to enter in a later step.

     > **Note:** Avoid using the same name for both the Event Hub and Event Hub Namespace.

   - **Partition count:** Select the number of partitions. For more info, see Partitions [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability#partitions].

     > **Note:** As a best practice for processing large volumes of data, we recommended using the highest number of partitions. For more info, see Advantages of using partitions [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability#advantages-of-using-partitions].

   - **Cleanup policy:** Select **Delete** or **Compact** based on your requirements. If you choose **Compact**, complete these tasks.
     - Select **Infinite retention time.**
     - Set a **Tombstone retention time** in hours. For more info, see Configure cleanup policy [https://learn.microsoft.com/en-us/azure/event-hubs/configure-event-hub-properties#configure-cleanup-policy].
   - **Retention time (hrs):** As events are sent to the connector for consumption when they are created, we recommend selecting the default 1 hour retention time. You can increase the number as needed. For more info, see Configure retention time [https://learn.microsoft.com/en-us/azure/event-hubs/configure-event-hub-properties#configure-cleanup-policy].

4. In the **Capture** tab, turn Capture **On** or **Off**. For more info, see Capture events through Azure Event Hubs in Azure Blob Storage or Azure Data Lake Storage [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-capture-overview]

.

5. In the **Review + Create** tab, complete these tasks:

    a. Review the instance details.

    b. Confirm the **Validation succeeded** message.

    c. Click **Create**.

    d. The Even Hubs Namespace **Overview** page opens. Confirm successful Event Hub creation with the **Successfully created Event Hub message** notification.

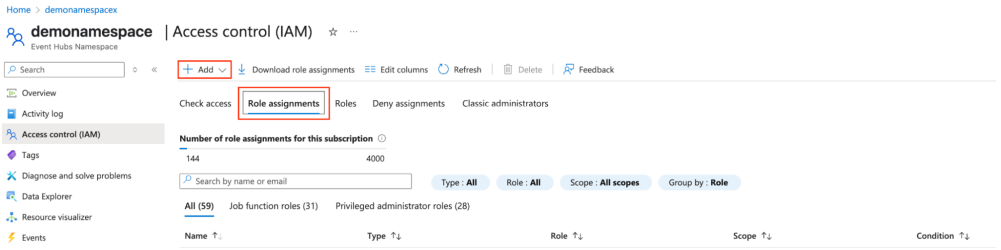
Step 4: Add role assignment

1. In the main menu of the Event Hub Namespace page, click **Access control (IAM)**.

    > **Tip:** If you're using an existing Event Hub and the Event Hub Namespace contains other Event Hubs that you do not wish to give this role assignment, you can create the role assignment in the Event Hub instead. Go to the Event Hub page and click **Access control (IAM)**.

2. Click the **Role assignments** tab to see the role assignments for this subscription.

3. To add a new role assignment, click **+ Add > Add role assignment**.For more info about assigning roles, see
Assign Azure roles using the Azure portal [https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal].



4. In the **Role** tab, select the **Azure Event Hub Data Receiver** role, then click **Next**.

5. In the **Members** tab, click **+ Select Members**.

6. In the **Select Members** dialog, search and select the application name value that you saved in Step 1, then click **Select**.

7. In the **Review + assign** tab, review the role assignment details.

8. Click **Review + assign**. The resource group **Access IAM** page opens with the role assigned to the selected scope.

Step 5: Create a consumer group

As a best practice, if multiple applications are reading the same data in your Event Hub, we recommend creating a Consumer Group for each application or purpose. Each consumer group allows up to 5 concurrent readers with different processing requirements. For more info, see
Consumer Groups [https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-features#consumer-groups].

Create a Consumer Group within your Event Hub:

1. Go to the Event Hub Namespace.

2. Select your Event Hub.

3. In the main menu, click **Consumer Groups**.

4. Click **+ Consumer Group**.

5. Enter a name for your consumer group. For example, `ngsiem-audit-logs`.

    > **Important:** Do not use this consumer group anywhere else other than with Next-Gen SIEM connectors.

6. Click **Create**.

Step 6: Configure data forwarding to your Event Hub

Configure Event Hubs and Microsoft Defender XDR in the administration interface for your instance of Microsoft 365:

1. In the
Microsoft 365 Defender portal [https://login.microsoftonline.com/common/oauth2/authorize?client_id=80ccca67-54bd-44ab-8625-4b79c4dc7775&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DejRd2rxDWyX07TPdCOBBdAZIS8iAZvwii_OZwn3LFtb6DI9s7vJeVRfE5_-QNG01qlQqOwYkfnfipromHbhlyjNbXw19pA62o3j4_63Iq9h3Y2XWlyUh4AsdoAZgACwJGiUxo-cnRMQtEBp3JH-Vew&response_mode=form_post&nonce=638325839959963774.N2FiZWMwOWYtMGI3YS00ZjkxLWJlYjYtYmY1MjkwOTE4OWI2ZjI2OTAzOTAtN2IyOC00NDJmLTk0ODQtNWMzNzlkNWMyNjll&client-request-id=ba2b0754-610e-4fcf-bbe6-32a20e71e809&redirect_uri=https%3A%2F%2Fsecurity.microsoft.com%2F&x-client-SKU=ID_NET461&x-client-ver=6.22.1.0]
, go to **Settings > Microsoft Defender XDR > Streaming API**.

2. Click **+ Add**.

3. In **Add new Streaming API settings**, enter the following info:

    - **Name:** Enter a name for the Streaming API service.
    - **Forward events to Event Hub:** Enable this setting.
    - **Event Hub Resource ID:** To get your **Event Hub Namespace resource ID**, go to your Azure Event Hubs namespace page. In the **Properties** tab, copy the **Resource ID**.
      For more info, see Enable raw data streaming [https://learn.microsoft.com/en-us/defender-xdr/streaming-api-event-hub#enable-raw-data-streaming].
    - **Event Hub name:** Enter the **Event Hubs Namespace** name that you saved earlier.
    - **Events Types**: Select **Alerts**, **Email**, and **Apps & Identities**.

4. Click **Save**.

Step 7: Verify successful Event Hub configuration

Verify data is successfully streaming to your event hub:

1. In the Azure Portal, search for and select **Event Hub**.

2. Click the new Event Hub namespace that you created in Step 2.
3. In the **Overview** page, look at the **Messages** chart and verify incoming messages.

Step 8: Configure and activate the Data Connector built for Microsoft Defender XDR Events

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 dialogue appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.
6. Enter the following information:
   - **Name:** Enter a name for your configuration.
   - **Event Hub Consumer Group:** Enter the name of the Event Hub Consumer Group you created in Step 5.
   - **EventHub Name:** Enter the name of your existing Event Hub or the name that you saved in Step 3.
   - **EventHub Namespace:** Enter the name of your existing Event Hubs Namespace or the Namespace name that you saved in Step 2.
   - **Client ID:** Enter the Application (Client) ID value that you saved in Step 1.
   - **Tenant ID:** Enter the Directory (Tenant) ID value that you saved in Step 1.
   - **Client Secret:** Enter the client secret value that you saved Step 1.
   - **Cloud:** Select **Public**, **Government**, or **China**.
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**.

    > **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 9: 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 = "microsoft_defender_xdr"
```

Data reference

Next-Gen SIEM events

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

- Process:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#p5eme1kf]
- Authentication:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- Configuration:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Iam:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#e3wbhf1h]
- Email:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#f5yqjx4f]
- File:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#y4016g3a]
- Host:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Library:Start:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#s0dfb8yk]
- Network:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx]
- Registry:Creation:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#x6l9dpbt]
- Registry:Change:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#i91q6llu]
- 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] .