Data Connector built for Microsoft IIS

Last updated: Jun. 24, 2025

Overview

Microsoft Internet Information Services (IIS) is a web server software package for Windows Server. The Microsoft IIS data connector allows you to collect and forward website activity data, generated by standard and advanced logging in Microsoft IIS, in both W3C and IIS log formats.

Supported log types

- **Access Logs in W3C or IIS format:** W3C logs record HTTP requests to an IIS server in a customizable text-based format, capture details like client IP, request method, response status, and user agent. They are useful in traffic analysis and troubleshooting.
- **HTTP Error Logs:** Failed requests, for example 404, and error details for troubleshooting.

Requirements

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

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

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

Server requirements: A Windows server (can be either on-premises or virtual machine) for installing and configuration of a data shipper.

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: Configure and activate the Data Connector built for Microsoft IIS

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.

   > **Tip:** This data connector's name is located in the header. For example, **Step 1: Configure and activate `<the_data_connector_name>`**.

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

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

5. In the **Add new connector** page, enter a name and optional description to identify the connector.
6. Click the **Terms and Conditions** box, then click **Save**.
7. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate the API key, go to **Data connectors > Data connectors > Data connections [/data-connectors]**, click **Open menu** ⋮ for the data connector, and click **Generate API key**.
8. Copy and safely store the API key and API URL to use during connector configuration.

   > **Important:** Record your API key somewhere safe as it displays only once during connector setup. For more information about vendor-specific connector setup, see the Third-party data source integration guides [/documentation/page/a76b8289/data-connectors#c42a73ec].

Step 2: Configure your data shipper

You can use any data shipper that supports the HEC API [https://library.humio.com/logscale-api/log-shippers-hec.html] to complete this step. We recommend using the **Falcon LogScale Collector**.

1. In the Falcon console, navigate to **Support and resources > Resources and tools > Tool downloads [/support/tool-downloads]**.
2. Install the LogScale Collector based on your operating system. For example, `LogScale Collector for Windows - X64 vx.x.x`.
3. Open the LogScale Collector configuration file in a text editor. For file location, see Create a configuration - Local [https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local].
4. Edit the `config.yaml` file. Examples of configuration files for syslog servers:

```
sources:
  access_log:
    type: file
    include: C:\inetpub\Logs\LogFiles\W3SVC*\u_ex*.log
    sink: humio

sinks:
```

```
numio:
  type: hec
  proxy: none
  token: <provided_by_CrowdStrike>
  url: <provided_by_CrowdStrike>
```

5. Verify the `sources` and `sinks` sections are correct.
   - Check that no other services are listening on port 514. For example, this command is commonly used to check for listening ports on Linux:
     ```
     sudo netstat -lpn
     ```
     - If port 514 is not available, select a different port and confirm it is not in use. Update the `port` number.
     - If you're configuring multiple sources in the same configuration file, each sink must have a distinct port. For example, you cannot have two Humio sinks listening on port 514.
   - Check the local firewall and confirm that the configured port is not being blocked.

     Important: For Windows Firewall, add the LogScale Collector to your traffic allowlist.
   - Add the `token` and `url` generated during data connector setup. Remove `/services/collector` from the end of the `url`.
6. Save and exit the `config.yaml` file.
7. Restart the Falcon LogScale Collector. For Windows, look for **Services** from the search bar, open **Services**, find **Humio Log Collector** and right-click **Restart**.

Step 3: Configure Microsoft IIS Server configuration

1. Open **IIS Manager**.
2. Select the site or server in the **Connections** pane, and then double-click **Logging**.

   Note: Enhanced logging is only available for site-level logging. If you select the server in the **Connections** pane, then the **Custom Fields** section of the **W3C Logging Fields** dialog is disabled.
3. In the **Format** field under **Log File**, select **W3C** and then click **Select Fields**.
4. Ensure only the following fields are selected:
   - Date (`date`)
   - Time (`time`)
   - Client IP Address (`c-ip`)
   - User Name (`cs-username`)
   - Server IP Address (`s-ip`)
   - Server Port (`s-port`)
   - Method (`cs-method`)
   - URI Stem (`cs-uri-stem`)
   - URI Query (`cs-uri-query`)
   - Protocol Status (`sc-status`)
   - Protocol Substatus (`sc-substatus`)
   - Win32 Status (`sc-win32-status`)
   - Time Taken (`time-taken`)
   - User Agent (`cs(User-Agent)`)
   - Referer (`cs(Referer)`)
5. Click **OK**.
6. In the **Actions** pane, click **Apply** to apply the new configuration.

Step 4: 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" | #repo = "3pi_microsoft_iis_hec" | #event.module = "iis"
```

Data reference

Next-Gen SIEM events

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

- Web:Access:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#p9vhn5jb]
- Web:Error:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#z3is1lw0]
- Network:Connection:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]
- Network:Allowed:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d44jz11k]
- Network:Access:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w0veajdl]
- Network:Denied:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#o1co06s5]

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 Mi Data Connector built for Microsoft OneDrive [/documentation/page/ibaed954/data-connector-built-for-microsoft-onedrive]