F5 BIG-IP Data Connector

Last updated: Jun. 9, 2025

Overview

F5 BIG-IP is a comprehensive platform that combines software and hardware solutions to enhance application security, availability, and access control. It provides centralized management and monitoring across multiple modules, including Application Security Manager (ASM), Advanced Firewall Manager (AFM), Access Policy Manager (APM), Domain Name System (DNS), Local Traffic Manager (LTM), and system information. With its robust integration capabilities, BIG-IP enables organizations to streamline access to applications, APIs, and data while ensuring a secure and seamless user experience, regardless of location or hosting environment.

Use this connector to ingest the following log types:

- ASM logs
- AFM logs
- APM logs
- DNS logs
- LTM logs
- System & OS logs

Requirements

CrowdStrike 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 or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements:

- Administrator access to the F5 portal (MyF5)
- The default parser for this data connector requires logs in syslog format before ingestion. For more info, see **Parser**.

System requirements:

- For the Falcon LogScale Collector, see the list of supported operating system versions [https://library.humio.com/falcon-logscale-collector/log-collector-install.html#log-collector-install-compatibility].
- The size of your Falcon LogScale Collector instance depends on workload. See the LogScale Collector sizing guide [https://library.humio.com/falcon-logscale-collector/log-collector-install-sizing.html].

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 F5 BIG-IP Data Connector

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, 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 > My connectors [/data-connectors/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.

Step 2: Configure your data shipper

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:

   - Linux

```
dataDirectory: /var/lib/humio-log-collector
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

   - Windows

```
dataDirectory: C:\ProgramData\LogScale Collector\
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

   - Mac

```
dataDirectory: /var/local/logscale-collector
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio

sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

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 Linux, run this command in your terminal:

```
sudo systemctl start humio-log-collector
```

   - For Windows, look for **Services** from the search bar, open **Services**, find **Humio Log Collector** and right-click **Restart**.

   - For Mac, run this command in your terminal:

```
sudo launchctl kickstart -k system/com.crowdstrike.logscale-collector
```

Step 3: Configure F5 Networks BIG-IP Syslog Forwarding

The BIG-IP system allows you to log process-related information and send log messages to remote high-speed log servers. You can also filter the logged data based on alert level and source. To set up the F5 BIG-IP environment, you can use either the browser-based Configuration Utility or command-line tools.

Follow the steps below to configure BIG-IP system logging using the browser-based Configuration Utility:

1. Open `https://BIG_IP_SERVER_IP`

   > **Note:** Replace `BIG_IP_SERVER_IP` with the IP address of your device.

2. Log in to your BIG-IP Management Interface.
3. Continue with the next configuration steps.

Step 3.1: Create a pool of remote logging servers

Create a pool of remote log servers to which the BIG-IP system can send log messages.

A logging pool allows you to define a pool of servers that receive syslog events. The pool contains the IP address, port, and a node name that you provide.

1. At the top of the screen, click **Configuration**.
2. On the Main tab, click **Local Traffic > Pools**.
3. Click **Create**.
4. In the **Name** field, enter a unique name for the pool.
5. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   - Type an IP address in the **Address** field, or select a node address from the **Node List**.
   - Type a service number in the **Service Port** field, or select a service name from the list.

     > **Note:** Remote logging servers require port 514.

   - Click **Add**.
6. Click **Finished**.

Step 3.2: Create a remote high-speed log destination

Create a log destination of the Remote High-Speed Log type to specify that log messages are sent to a pool of remote log servers.

> **Note:** Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP system.

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**.
2. Click **Create**.
3. In the **Name** field, enter a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.
   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers which was created in
   Step 3.1: Create a pool of remote logging servers [/documentation/page/ob38708b/f5-big-ip-data-connector#p69857ab].
6. From the **Protocol** list, select the UDP protocol (default protocol used by the high-speed logging pool members).
7. Click **Finished**.

Step 3.3: Create a formatted remote high-speed log destination

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog server.

> **Note:** Ensure that at least one remote high-speed log destination exists on the BIG-IP system. The formatted log destination allows you to specify any special formatting required on the events forwarded to the high-speed logging destination.

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**.
2. Click **Create**.
3. In the **Name** field, enter a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote Syslog**.
   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. From the **Syslog Format** list, select a format for the logs.
6. From the **Forward To** list, select the High-Speed Log Destination created in
   Step 3.2: Create a remote high-speed log destination [/documentation/page/ob38708b/f5-big-ip-data-connector#m2415275].

   > **Important:** For logs coming from Access Policy Manager (APM), only the BSD Syslog format is supported.

7. Click **Finished**.

Step 3.4: Create a publisher

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

> **Note:** Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP system. It allows the BIG-IP appliance to publish the formatted log message to the local syslog database.

1. On the Main tab, click **System > Logs > Configuration > Log Publishers**.

2. Click **Create**.

3. In the **Name** field, enter a unique, identifiable name for this publisher.

4. From the available list of **Destinations** setting, select the formatted remote high-speed log destination which was created in Step 3.3: Create a formatted remote high-speed log destination [/documentation/page/ob38708b/f5-big-ip-data-connector#kc324b95] and click << to move the destination to the **Selected** list.

5. Click **Finished**.

Step 3.5: Creating a logging filter

Create a custom log filter to specify the system log messages that you want to publish to a particular log.

> **Note:** Ensure that at least one log publisher is configured on the BIG-IP system.

1. On the Main tab, click **System > Logs > Configuration > Log Filters**.

2. In the **Name** field, enter a unique, identifiable name for this filter.

3. From the **Severity** list, select the level of alerts that you want the system to use for this filter.

   > **Note:** The severity level that you select includes all of the severity levels that display above your selection in the list. For example, if you select **Emergency**, the system publishes only emergency messages to the log. If you select **Critical**, the system publishes critical, alert, and emergency-level messages in the log.

4. From the **Source** list, select "All system processes" from the available list of event log sources.

5. In the **Message ID** field, enter the first eight hex-digits of the specific message ID that you want the system to include in the log. Use this field when you want a log to contain only each instance of one specific log message.

   > **Note:** BIG-IP system log messages contain message ID strings in the format: xxxxxxxx:x:. For example, in this log message: Oct 31 11:06:27 olgavmmgmt notice mcpd[5641]: 01070410:5: Removed subscription with subscriber id lind, the message ID string is: 01070410:5:. You enter only the first eight hex-digits: 01070410.

6. From the **Log Publisher** list, identify the publisher created in step 4 that contains the destinations you wish to send log messages to.

7. Click **Finished**.

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 = f5networks | #repo = "3pi_f5_bigip" | #event.module = "bigip"
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **f5networks-bigip**. This parser requires logs in syslog format before using this data connector.

Timestamp

Timestamp Format: `MMM [ ]d HH:mm:ss`

Example: `Feb 10 05:35:26`

Structure

F5 Networks BIG-IP LTM sample event messages. The following sample event message shows a Pool member's monitor status.

```
<133>Nov  5 14:01:50 f5networks.bigip.test notice mcpd[5281]: 01070638:5: Pool member
2001:20:5004:1606::89:8790 monitor status down.
```

Next-Gen SIEM events

Next-Gen SIEM events

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

- Network:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx]
- Network:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j2mj0bj0]
- Network:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0vgvx1w]
- Network:Connection:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]
- Network:Denied:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#o1co06s5]
- Iam:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e3wbhf1h]
- Iam:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w2o4xy4u]
- Iam:User:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#u8x1u9jm]
- 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]
- 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]
- Process:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#b1nwxnx3]
- Process:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m7os2kgj]
- File:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i2xbijpg]
- File:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#y4016g3a]
- Configuration:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vkl]
- Configuration:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Host:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Session:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#n0esexy6]
- Session:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p03v6mbn]
- Session:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#x0113sk8]
- 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] .

‹ ExtraHop RevealX 360[/documentation/page/d724e73b/extrahop- Falcon LogScale Collector › [/documentation/page/u496e28e/falcon-logscale-collector]