Cisco Firepower Data Connector

Last updated: Jun. 25, 2025

Overview

Forward events from Cisco Firepower appliances to Falcon Next-Gen SIEM for investigation and 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:

- Administrator access to the Falcon console and a Falcon LogScale Collector (FLC) host.
- **Linux syslog server** or **Windows server** (on-premises or VM) for installing and configuring the data shipper.
- Network routing from the log source to the FLC host on TCP port 514.
- Availability of the **Cisco Firepower Data Connector** app in the CrowdStrike Store.

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

Configuring data ingestion

Set up data ingestion for Cisco Firepower using the Falcon LogScale Collector.

> **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.

Expected Log Structure

Syslog headers in one of the following formats:

- `<log.syslog.priority>timestamp: %FTD-log.level-event.code: message`
- `<log.syslog.priority>timestamp log.syslog.hostname: %FTD-log.level-event.code: message`
- `timestamp log.syslog.hostname: %FTD-log.level-event.code: message`

Timestamp Format

- `MMM dd yyyy HH:mm:ss`. For example, `Jan 29 2024 17:06:32` (UTC).

Step 1: Configure and activate the Cisco Firepower Data Connector

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors/]** or to **Data connectors > Data sources [/data-connectors/]**.
2. Click the **Cisco Firepower Data Connector** tile.
3. Enter a name and optional description to identify the connector.
4. After reading the terms and conditions, check the box to agree.
5. Click **Save**.
6. Click **Close**.
7. Click **Generate API key** to generate your API key and URL.

   > **Note:** If you don't see **Generate API key**, refresh the page.

8. Save the API key and URL values displayed in the **Connection setup** dialog. These values will be required later to set up Falcon LogScale Collector.

   > **Important:** Record your API key somewhere safe as it displayed only once during connector setup.

9. Click **Close**.

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 Cisco Firepower syslog forwarding

1. On the **Firepower Device Manager** page, under **System Settings**, select **Logging Settings**.

2. On the **System Settings** page, select **Logging Settings** in the navigation menu.

3. Enable **Data Logging** and click **+** under **Syslog Servers**.

4. Select **Add Syslog Server**. Alternatively, you can create the **Syslog Server** object in **Objects - Syslog Servers**.

5. Enter the IP address of the Falcon LogScale Collector host and the configured port number.

6. Select **Data Interface** and click **OK**.
7. Select the new Syslog server and click **OK**.
8. Select the **Severity level to filter** with the all events radio button and select your desired logging level to **Information**.
9. Click **Save**.
10. Click the deploy icon to deploy the new settings.

Fore more info, see
Configure and Verify Syslog in Firepower Device Manager [https://www.cisco.com/c/en/us/support/docs/security/firepower-2130-security-appliance/220231-configure-and-verify-syslog-in-firepower.html]
.

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:

```
#repo = "3pi_cisco_firepower_hec" | #event.module = "firepower"
```

Data reference

Next-Gen SIEM events

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

- 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]
- Network:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0vgvx1w]
- 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]
- Intrusion_detection:Denied:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#x8zazrto]
- Intrusion_detection:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#k7xn9jc3]
- Authentication:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- 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: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]
- File:Creation:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#g2in7h52]
- File:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#y4016g3a]

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

‹ Cisco Duo MFA[/documentation/page/yff4b6a2/cisco-du Cisco Identity Services Engine › [/documentation/page/i2147975/cisco-identity-services-engine]