Fortinet FortiGate

Last updated: Jun. 25, 2025

Overview

Enhance Next-Gen SIEM detections with data from Fortinet FortiGate.

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.

Other requirements:

- Your environment must include a functioning deployment of Fortinet FortiGate.
- Access to a Fortinet FortiGate Administrator account.
- An on-premises syslog server with Falcon LogScale Collector installed and configured to send the data to Falcon Next-Gen SIEM.

Setup

> **Important:** Some of these steps are performed in third-party products. The CrowdStrike Falcon platform integrates the relevant settings as you configure them. However, CrowdStrike does not validate any third-party configurations. Perform the following steps with care, and validate your settings and values before finalizing configurations in Falcon.

Step 1: Configure and activate the Fortinet FortiGate 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.

   > **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:

   - Linux

     ```yaml
     dataDirectory: /var/lib/humio-log-collector
     sources:
       syslog_udp_514:
         type: syslog
         mode: udp
         port: 514
         sink: humio
     sinks:
       humio:
     ```

```
  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 the syslog settings using admin account

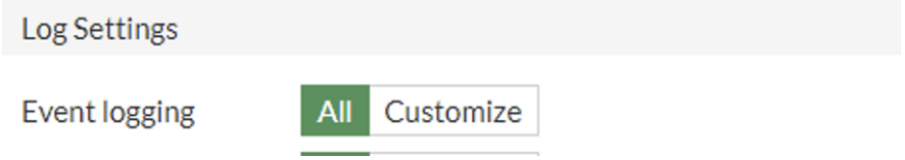
These steps are performed in the administration interface for your instance of Fortinet FortiGate. For more info, see the Fortinet product documentation.

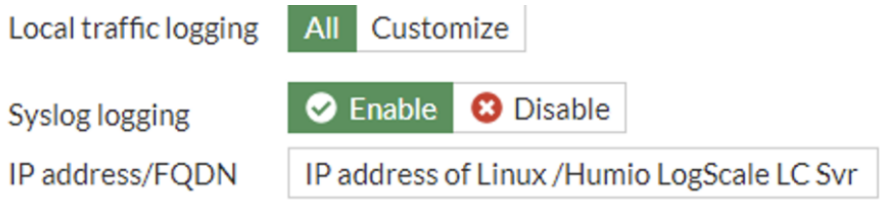
1. Log in to the FortiGate FW with Admin privileges.

2. In the FortiGate GUI, go to **Log & Report > Log Settings > Global settings**.

3. In the **Log Settings** section:

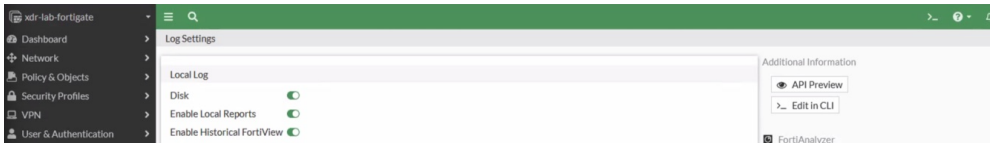
- **Event logging:** Select **All**
- **Local traffic logging:** Select **All**
- **Syslog logging:** Select **Enable**
- **IP address/FQDN:** Enter the IP address of the on-premises Linux/Humio LogScale Collector server.





4. Click **Apply** to save the changes.

5. In FortiGate CLI:



- At the # prompt, enter the following commands:

```
config log syslogd setting
set status enable
```

Note: Make sure to add the IP address of the Linux server in the command below before executing.

```
set server <Linux_server_ip_address>
```

```
set mode udp
set port 514
set facility syslog
set format default
set priority default
set max-log-rate 0
set interface-select-method auto
end
```

- At the # prompt, enter the following commands:

Note: Select a severity level that you want to configure to collect required logs. The available logs levels are: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notification**, **Information**, and **Debug**.

```
config log syslogd filter
set severity information
set forward-traffic enable
set local-traffic enable
set multicast-traffic enable
set sniffer-traffic enable
set anomaly enable
set voip enable
end
```

- Exit the CLI.

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=fortinet | #event.module=fortigate
```

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: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:Protocol:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#h6gvlrpt]
- Network:Start:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#j2mj0bj0]

- Network:Allowed:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d44jz11k]
- Network:Denied:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#o1co06s5]
- 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]
- Malware:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#r5b30nfi]
- Web:Access:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#p9vhn5jb]
- Host:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Authentication:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- 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] .

‹ ForgeRock Identity Cloud[/documentation/page/b09afdd2/forgerock-identity-clou Fortinet FortiMail › [/documentation/page/kc3d91b3/fortinet-fortimail]