# Fortinet FortiMail

*Last updated: Jun. 16, 2025*

## Overview

FortiMail is Fortinet's secure email gateway that protects against spam, phishing, and malware. It offers multi-layered filtering, encryption, DLP, and advanced threat protection with FortiGuard integration.

Use this connector to ingest the following log types:

- Email encryption events
- Email spam
- Statistics
- System events
- Virus scanning

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

**Vendor requirements:** FortiMail GUI administrative access.

**Parser:** The default parser for this data connector requires logs in Syslog format. For more info, see Parser [/documentation/page/kc3d91b3/fortinet-fortimail#cfaf676e].

**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 HEC/HTTP 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 by connector name to find and select the **HEC / HTTP Event Connector.**
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 or select these details:
   - **Data source:** Enter a name for the data source to display on the connection's **Details** page.
   - **Connector name:** Enter a name to identify the connector. This name displays in the **Connections** list.
   - **Description:** Optional. Enter a description of the connector.
   - **Parsers:** Select a parser to use for this connection. In the **Parsers** dropdown menu, select **fortinet-fortimail**.
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,** 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

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

   - Windows

     ```yaml
     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

     ```yaml
     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 Fortinet FortiMail log settings

1. Sign in to the FortiMail GUI.
2. Go to **Log & Report > Log Setting > Remote**, then click **New**.
3. Configure these settings:
    a. Click **Enable** and enter a **Profile Name**.
    b. **Address:** Enter the IP address of the Falcon LogScale Collector.
    c. **Port:** Enter the port the Falcon LogScale Collector is listening on. The default port is 514.
    d. **Protocol:** Select **Syslog**.
    e. **Mode:** Select **UDP.**
    f. **Severity Level:** Select **6**.
    g. **Facility:** Select **local7**.
    h. **Logging Policy Configuration:** Enable the types of logs you want to forward to Falcon Next-Gen SIEM.
4. Click **Create**.

## 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 = "fortimail"
```

# Data reference

## Parser

The default parser recommended to parse incoming data for this data connector is **fortinet-fortimail**. This parser requires logs in **Syslog** format.

**Supported timestamp format**: `date=yyyy-MM-dd time=HH:mm:ss`, assuming UTC.

**Example**: `date=2024-07-17 time=12:26:41`

## Structure

Syslog priority with a key-value pair message body

```
<190>date=2023-01-30,time=16:09:15.246,device_id=FEVM02TM23000064,log_id=0400003064,type=virus,subtype=infec
ted,pri=information,from="syntax@www.example.com",to="user2@1.example",src=192.0.2.28,session_id="q6OL7fsQ01
8870-q6OL7fsR018870",msg="The file inline16-69.dat is infected with EICAR_TEST_FILE."
```

## Next-Gen SIEM events

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

- Authentication:Start:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#v3639xkr]
- Configuration:Access:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w71kufuj]
- Configuration:Change:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vkl]
- Configuration:Creation:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#n9xgygup]
- Configuration:Deletion:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#v267j0ck]
- Email:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#f5yqjx4f]
- Host:Change:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#t9lb07j6]
- Host:End:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#m0caqh4x]
- Host:Info:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Host:Start:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#j89ajtvy]
- Iam:Change:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#w2o4xy4u]
- Iam:Creation:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#r6v4uftm]
- Iam:Deletion:{failure,success,unknown} [/documentation/page/q1f14b54/next-gen-siem-data#v1nlikck]

- Iam:Group:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#l716zkv7]
- Iam:User:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#u8x1u9jm]
- Malware:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#r5b30nfi]
- Network:Connection:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]
- 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]
- Process:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#b1nwxnx3]

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

< Fortinet FortiGate[/documentation/page/e001559f/fortine GCP Pub/Sub Data Connector > [/documentation/page/tf022cab/gcp-pub-sub-data-connector]