Cisco Identity Services Engine

Last updated: Jun. 24, 2025

Overview

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure network access to end users and devices. Cisco ISE enables the creation and enforcement of security and access policies for endpoint devices that are connected to an organization's routers and switches. Use this guide to set up data ingestion for **Cisco ISE** using a data shipper, such as the Falcon LogScale Collector.

Types of logs generated by this data connector:

- `CISE_Alarm`

- `CISE_MONITORING_DATA_PURGE_AUDIT`

- `CISE_RADIUS_Diagnostics`

- `CISE_Administrative_and_Operational_Audit`

- `CISE_logging`

- `CISE_System_Statistics`

- `CISE_Passed_Authentications`

- `CISE_Failed_Attempts`

- `CISE_Administrator_Authentication_and_Authorization`

- `CISE_Authentication_Flow_Diagnostics`

- `CISE_Identity_Stores_Diagnostics`

- `CISE_AD_Connector`

- `CISE_Internal_Operations_Diagnostics`

- `CISE_Threat_Centric_NAC`

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 requirement: Cisco ISE Portal Administrative privileges.

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 Cisco Identity Services Engine 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:
       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 Cisco ISE administrative settings

1. Log in to the Cisco ISE Portal with Admin privileges.

2. Go to **Administration** > **System** > **Logging** > **Remote Logging Targets.**

3. Click **Add** and enter these details:

- **Name:** Enter a unique name for the remote target.

- **Description:** Enter a description for the remote target.

- **Host / IP Address:** Enter the IP address of the Falcon LogScale Collector.

- **Port:** Enter the port number used by the Falcon LogScale Collector.

- **Facility Code:** Select the syslog facility to use for logging events. For example, LOCAL6.

- **Target Type:** Select **TCP Syslog.**

- **Maximum Length:** Enter **8192.**

4. Click **Save**. Verify the creation of the new target in the **Logging Targets** page.

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 = "cisco" | #repo = "3pi_cisco_ise" | #event.module = "ise"
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **cisco-ise**.

Timestamp

Timestamp Format: yyyy-MM-dd HH:mm:ss.SSSSSS Z

Example: 2020-04-27 11:11:47.028075 -08:00

Timestamp Format: yyyy-MM-dd HH:mm:ss,SSS Z

Example: 2021-02-23 21:44:54.276 +00:00

Timestamp Format: MMM dd HH:mm:ss Z

Example: Mar 3 10:42:25 +00:00

Timestamp Format: MMM dd HH:mm:ss

> **Important:** This timestamp format assumes UTC.

Example: Mar 28 11:46:57

Structure

CISE_Alarm syslog with the following header format:

```
<log.syslog.priority>log.syslog.version @timestamp log.syslog.hostname log.syslog.appname log.syslog.procid
log.syslog.msgid syslog.structured_data
```

Other events syslog with the following header format:

```
<log.syslog.priority>timestamp log.syslog.hostname eventCategory eventId segmentTotal segmentNumber message
```

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]

- Authentication:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]

- Authentication:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v9a3adya]

- Iam:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e3wbhf1h]

- Iam:Admin:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w0uja3kq]

- 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]

- Iam:Group:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#l716zkv7]

- 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]

- 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:Allowed:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d44jz11k]

- Network:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0vgvx1w]

- Network:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j2mj0bj0]

- Network:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx]

- 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]

- Configuration:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]

- 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]

- File:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t3em9j85]

- File:Deletion:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m2l5h6y8]

- 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]

- Process:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m7os2kgj]

- Process:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#b1nwxnx3]

- Process:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p5eme1kf]

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