Veeam Data Platform

Last updated: Jun. 24, 2025

Overview

Use this connector to ingest syslog messages sent by Veeam Data Platform servers to monitor various Veeam security activities, including early threat detection, four-eyes authorization events, or multi-factor authentication issues. Veeam Data Platform events help you understand the health status of your data protection for unified security across endpoint and network domains.

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 access to the Falcon console for the respective CID.

Vendor requirements:

- Veeam Data Platform Advanced or Premium edition
- Veeam Data Platform version 12.1 or later

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 Veeam Data Platform 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:
     ```

```
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 syslog settings in Veeam

Configure the syslog server for **Veeam Backup & Replication** and/or **Veeam ONE**.

Configure the syslog server in Veeam Backup & Replication

1. From the main menu, select **Options > Event Forwarding**.

2. In the **Syslog servers** section, click **Add.**

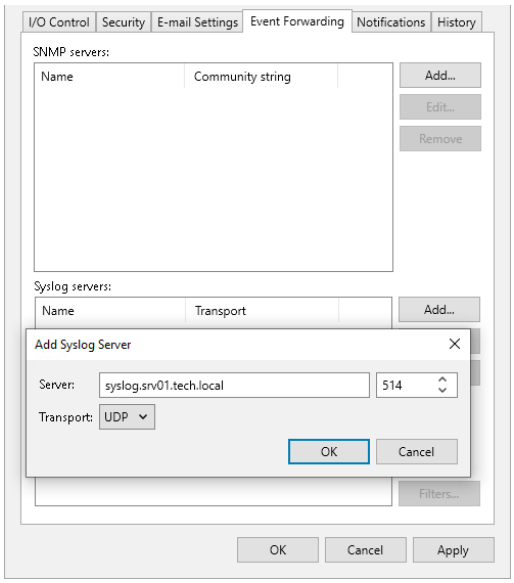
3. In the **Server** field, specify the FQDN or IPv4 address of the Falcon LogScale Collector.

   Note: You cannot specify the IPv6 address in this field.

4. In the **Transport** field, specify the transport protocol: **TCP** or **UDP**.

   Note: It is recommended to use the default port 514 unless you changed it during LogScale Collector setup.

5. Click **OK**.

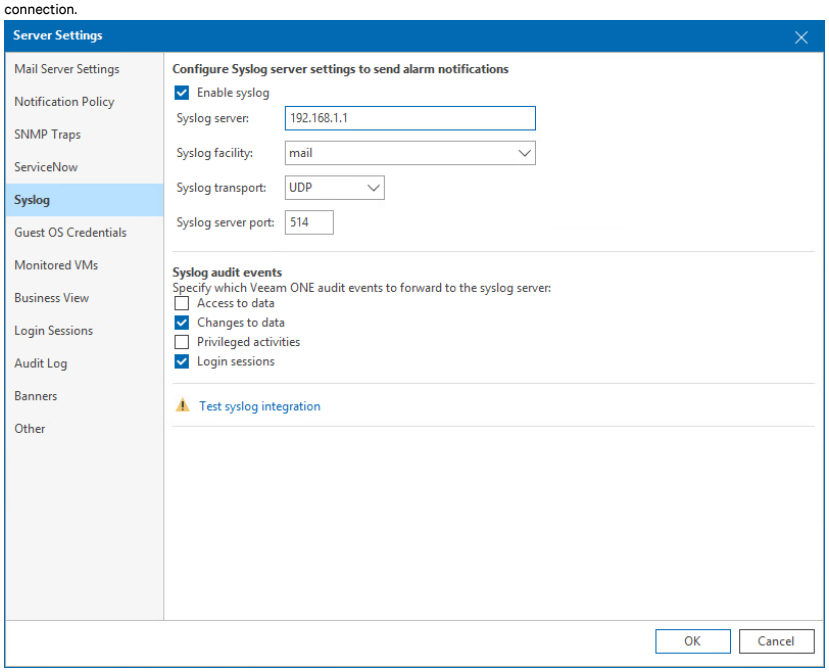


Note: If the syslog server is unavailable, an error message is displayed.

Configure the syslog server in Veeam ONE

1. Navigate to the Veeam ONE Server settings.
2. At the Syslog step of the wizard, click the **Enable syslog** check box.
3. Enter syslog server details:
   - **Syslog server:** Define the IPv4 or IPv6 address of the Falcon LogScale Collector.
   - **Syslog facility:** Define the value used to identify the source of the alarm. By default, this is set to mail.
   - **Syslog transport:** Define TCP or UDP. By default, this is UDP.
   - **Syslog server port:** The port used to connect to your syslog integration instance. By default, this is 514. It is recommended to use the default port 514 unless you changed it during the Falcon LogScale Collector setup.
4. Select syslog audit events that you want to send to your syslog integration:
   - Access to data
   - Changes to data
   - Privileged activities
   - Login sessions

   Note: It is recommended to send all syslog audit events for full visibility in Falcon Next-Gen SIEM.
5. To test the connection settings, click **Test syslog integration**. This creates a test connection to syslog and returns a signal confirming a successful connection.



Note: If you select the **Enable syslog** check box and do not test the connection, Veeam ONE will verify it before saving the server settings. Additionally, the connection is checked when each **Server Settings** item, for example mail server settings or email notifications, changes.

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 ="Veeam" | #repo = "3pi_veeam_data_platform"
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **veeam-veeamdataplatform**.

Structure

This is how the Veeam Backup & Replication output looks like before parsing:

```
<14>1 2025-01-20T09:00:16.365505-08:00 xxyyzz Veeam_MP - - [origin
      enterpriseId="31023"] [categoryId=0 instanceId=31400 ID="00000000-0000-0000-0000-000000000000"
      Name="N\asja2" ChangesXML="<changes><object id="12c6fc3a-fd11-45e5-8f4b-63a758f88b48"
      name="N\asja2" assignedRoleName="Veeam Restore Operator" /></changes>" UserName="N\asja"
      UserFullInfo="<ModifiedUserInfo fullName="N\asja" loginType="0" />" VbrHostName="xxyyzz.n.local"
      VbrVersion="12.3.0.288" Version="1" Description="User or group N\asja2 has been
      deleted."]
```

This is how the Veeam Backup & Replication output looks like after parsing:

```
#Cps.version: 1.0.0
#ecs.version: 8.17.0
#event.kind:event
#event.module:vbr
#event.outcome:unknown
#observer.type:dataprotection
#repo:3pi_parsers
#type:veeam-veeamdataplatform
#Vendor:veeam
@id:pegiep8dFX6NE6Ld5oqfh34V_0_0_1699272426
@ingesttimestamp:1743402396371 (2025-03-31T06:26:36.371+00:00)
@rawstring:<14>1 2023-11-06T13:07:06.763566+01:00 DEMOSERVER01 Veeam_MP - - [origin enterpriseId="31023"]
[categoryId=0 instanceId=42405 Operation="Delete backup VMware Tiny Servers - EY - VMware Tiny Server 01"
InitiatorName="<ModifiedUserInfo fullName="domain\SYSTEM" loginType="0" />" param3="<ModifiedUserInfo
fullName="domain\SYSTEM" loginType="0" />" Version="1" Description="Delete backup VMware Tiny Servers - EY
- VMware Tiny Server 01 event initiated by domain\SYSTEM has expired while waiting for additional approval
and was auto-rejected."]
@timestamp:1699272426763 (2023-11-06T12:07:06.763+00:00)
@timestamp.nanos:566000
@timezone:+01:00
event.action:Delete backup VMware Tiny Servers - EY - VMware Tiny Server 01
event.category[0]:api
event.id:42405
event.severity:70
event.type[0]:info
log.syslog.appname:Veeam_MP
log.syslog.hostname:DEMOSERVER01
log.syslog.priority:14
log.syslog.structured_data:[categoryId=0 instanceId=42405 Operation="Delete backup VMware Tiny Servers - EY
- VMware Tiny Server 01" InitiatorName="<ModifiedUserInfo fullName="domain\SYSTEM" loginType="0" />"
param3="<ModifiedUserInfo fullName="domain\SYSTEM" loginType="0" />" Version="1" Description="Delete backup
VMware Tiny Servers - EY - VMware Tiny Server 01 event initiated by domain\SYSTEM has expired while waiting
for additional approval and was auto-rejected."]
log.syslog.version:1
message:Delete backup VMware Tiny Servers - EY - VMware Tiny Server 01 event initiated by domain\SYSTEM has
expired while waiting for additional approval and was auto-rejected.
Parser.version:1.0.0
user.domain:domain
user.name:SYSTEM
Vendor.categoryId:0
Vendor.FullUserName:domain\SYSTEM
Vendor.InitiatorName:<ModifiedUserInfo fullName="domain\SYSTEM" loginType="0" />
Vendor.ModifiedUserInfo._loginType:0
Vendor.param3:<ModifiedUserInfo fullName="domain\SYSTEM" loginType="0" />
Vendor.Severity:High
```

```
Vendor.Version:1
```

This is how a syslog RAW string from Veeam ONE looks like before parsing:

```
<11>1 2024-10-08T22:05:53.300815+00:00 DEMOSERVER01 DEMOSERVER01.dummydomain.local 4388 veeamdcs-alarm-285
[origin enterpriseId="31023"] alarm_name="Suspicious incremental backup size" predefined_alarm_id="364"
alarm_type="Backup server" object_path="DEMOSERVER01.dummydomain.local"
object_name="DEMOSERVER01.dummydomain.local" status_old="Error" status_new="Error"
alarm_details="Incremental backup size of 'testserver' (77.1%) created by 'Clean Room 1' job is above the
configured threshold (3.0%) Incremental backup creation time 2024-10-08 22:00:14 (UTC+0:00) "
```

This is how the Veeam ONE output looks like after parsing:

```
#Cps.version

1.0.0



#ecs.version

8.17.0



#event.kind

alert



#event.module

veeamone



#event.outcome

unknown



#observer.type

dataprotection



#repo

3pi_parsers



#type

veeam-veeamdataplatform



#Vendor

veeam



@id

0kG3d4DduvA1Npjb5KT6iRvH_0_0_1728425153



@ingesttimestamp

1743402396385 (2025-03-31T06:26:36.385+00:00)



@rawstring

<11>1 2024-10-08T22:05:53.300815+00:00 DEMOSERVER01 DEMOSERVER01.dummydomain.local 4388 veeamdcs-alarm-285
[origin enterpriseId="31023"] alarm_name="Suspicious incremental backup size" predefined_alarm_id="364"
alarm_type="Backup server" object_path="DEMOSERVER01.dummydomain.local"
object_name="DEMOSERVER01.dummydomain.local" status_old="Error" status_new="Error"
alarm_details="Incremental backup size of 'testserver' (77.1%) created by 'Clean Room 1' job is above the
configured threshold (3.0%) Incremental backup creation time 2024-10-08 22:00:14 (UTC+0:00) "
```

@timestamp

1728425153300 (2024-10-08T22:05:53.300+00:00)

@timestamp.nanos

815000

@timezone

Z

event.category[0]

api

event.id

364

event.severity

90

event.type[0]

info

host.name

DEMOSERVER01

log.syslog.appname

DEMOSERVER01.dummydomain.local

log.syslog.hostname

DEMOSERVER01

log.syslog.msgid

veeamdcs-alarm-285

log.syslog.priority

11

log.syslog.procid

4388

log.syslog.structured_data

alarm_name="Suspicious incremental backup size" predefined_alarm_id="364" alarm_type="Backup server"
object_path="DEMOSERVER01.dummydomain.local" object_name="DEMOSERVER01.dummydomain.local"

```
status_old="Error" status_new="Error" alarm_details="Incremental backup size of 'testserver' (77.1%)
created by 'Clean Room 1' job is above the configured threshold (3.0%) Incremental backup creation time
2024-10-08 22:00:14 (UTC+0:00) "



Log.syslog.version

1



message

Incremental backup size of 'testserver' (77.1%) created by 'Clean Room 1' job is above the configured
threshold (3.0%) Incremental backup creation time 2024-10-08 22:00:14 (UTC+0:00)



Parser.version

1.0.0



Vendor.alarm_name

Suspicious incremental backup size



Vendor.alarm_type

Backup server



Vendor.object_name

DEMOSERVER01.dummydomain.local



Vendor.object_path

DEMOSERVER01.dummydomain.local



Vendor.Severity

Critical



Vendor.status_new

Error



Vendor.status_old

Error
```

Next-Gen SIEM events

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

- Api:Info:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#y81vvmdx]
- Configuration:Info:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Malware:Info:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#r5b30nfi]

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