Cisco Cyber Vision Syslog Notification Format Configuration Guide, Release 5.3.x

First Published: 2022-11-17

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this documentation

Document purpose

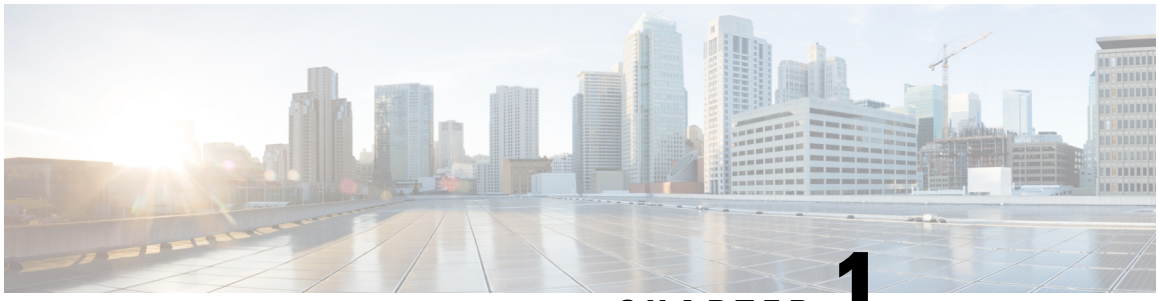
This document specifies the syslog format used by Cisco Cyber Vision when exporting events or alerts to an external server and describes how to configure it.

This manual applies to **system versions 5.3.x**.

Warnings and notices

To ensure your personal safety and to prevent damage to property, observe the following: Warnings and notices and Safety Alert symbols. These notices are graded according to the degree of danger.

Warning	Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage. Take precautions.
Important	Indicates risks that could involve property or Cisco equipment damage and minor personal injury. Take precautions.
Note	Indicates important information on the product described in the documentation.



CHAPTER 1

Overview

Cisco Cyber Vision events and alerts

Events and alerts are system-generated notifications that

- indicate significant activity or irregularities detected within an industrial network,
- categorize information based on type, associated data, and network components, and
- provide warnings or alerts to help with security monitoring and response.

Event: You receive an event notification when Cisco Cyber Vision detects notable network activity, such as a PLC being reprogrammed or a new device appearing. You can configure Syslog integration for events in the Classic UI.

Alert: An alert is a notification that triggers when a user-defined rule's condition is met. You can set up Syslog integration for alerts in the New UI.

Additional reference information

Cisco Cyber Vision sensors analyze industrial protocols and gather network properties. The system sends these properties to the Center. The Center processes the information and creates a model of your operational technology (OT) network.

Events notify you about changes, incidents, or anomalies in your industrial environment. In the Classic UI, events appear in a timeline. You can forward events to external systems through Syslog.

In the New UI, you can configure Cyber Vision to forward alerts through Syslog when alerts are raised or cleared.

Examples

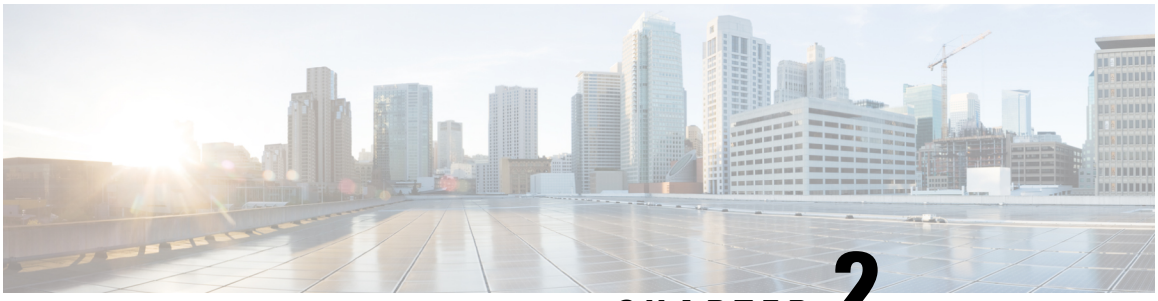
These events trigger logs and syslog integration in the Classic UI:

- Init: The system detects new industrial communications.
- Start or Stop CPU: The system detects when a PLC starts or stops.
- Exception: The system detects an exception in an industrial connection.

- Program Download: The system detects the download of a PLC program.
- Program Upload: The system detects the upload of a PLC program.
- New Communication: The system detects a new communication flow.
- New Properties: The system detects additional industrial properties on the network.
- New Component: The system identifies a new component on the network.
- Protocol Decode Failure: The system detects a decode error in a received packet.

These alerts trigger syslog integration in the New UI:

- The system generates an alert.
- The system clears an alert.



CHAPTER 2

Syslog compatibility

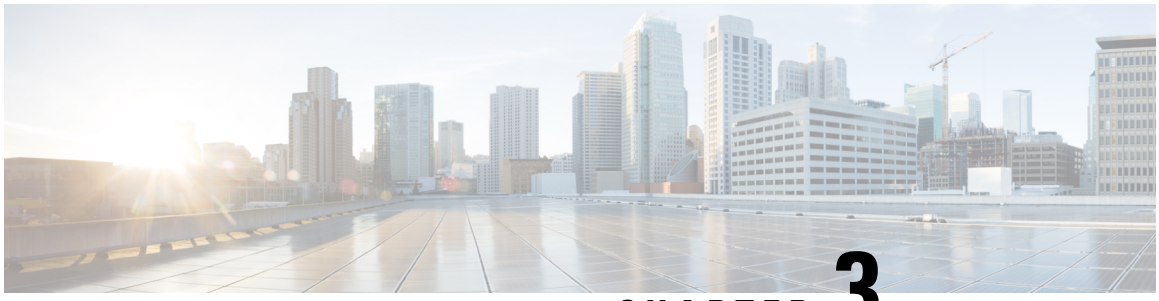
Syslog export formats

A syslog export format is a data formatting method that

- enables export of event or alert data, or both, from Cisco Cyber Vision,
- supports industry standards for integration with third-party security tools, and
- allows selection of different time precision and compatibility levels.

Additional information

Cisco Cyber Vision uses the industry-standard rsyslog implementation internally and supports both UDP and TCP transmission. The destination IP and port can be set in the admin page for Cisco Cyber Vision. Note that syslog formats are often loosely defined and may not be uniformly implemented by all vendors; Cisco Cyber Vision Center adheres to best practices to ensure exported data is broadly compatible and easy to interpret.



CHAPTER 3

Syslog configuration

Syslog configuration can be performed by Product and Admin users.

Configure syslog

Enable forwarding of Cyber Vision events and alerts to an external syslog server to integrate with a Security Information and Event Management (SIEM) system.

To configure syslog, follow these steps:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that the external syslog server is accessible. Obtain the host IP address, port, and the required protocol.
- If secure communication is required, ensure you have the P12 certificate from your SIEM administrator.
- Recent syslog format changes:
  - **Standard** and **RFC3164** formats are deprecated.
  - **Standard/CEF** is now named **CEF**.
  - **RFC3164/CEF** is now named **CEF Extended Time Precision**.

Note If the deployment had **Standard** or **RFC3164** formats configured, version 5.3.x setup migrates the configuration to CEF.

Procedure

Step 1 From the main menu, choose **Admin** > **System**.

Step 2 Click **Configure** in the **Syslog configuration** menu.

Step 3 Select **Protocol**.

Note
If secure communication is required, select **TCP + TLS** and import the P12 certificate.

Step 4 Enter the syslog server **Host** IP address and **Port** that are accessible from Cyber Vision Center.

Step 5 Select the required **Format**.

- **CEF**: This format, based on the Common Event Format (CEF) standard, sends events with second-precision timestamps.
- **CEF Extended Time Precision**: This format, based on the Common Event Format (CEF) and an extended syslog header, sends events with millisecond-precision timestamps.

Step 6 Save the configuration.

Cyber Vision Center sends events from the Classic UI to syslog with 'Version Number = 1.0.' It sends alerts from the New UI to syslog with 'Version Number = 2.0.

What to do next

To export events using syslog, see Configure event export to syslog (Classic UI). To configure notifications for specific alert types, see Enable or disable syslog notifications for alert types (New UI).

Configure event export to syslog (Classic UI)

Manage which event categories Cisco Cyber Vision exports to syslog.

By default, events can be exported to syslog. Ensure that syslog is configured before enabling event export. If syslog is not configured, event export will not function.

To configure event export to syslog, use these steps.

Before you begin

Confirm that syslog destinations and configuration are set up in Cisco Cyber Vision.

Procedure

Step 1 In the Cyber Vision Classic UI, choose **Admin** > **Events**.

Step 2 Select the event categories to enable or disable for syslog export.

Step 3 Enable or disable **Syslog export** for the selected categories.

The selected event categories are now exported to syslog based on your configuration.

Enable or disable syslog notifications for alert types (New UI)

You can manage whether the Cyber Vision Center sends syslog notifications for alerts of specific alert types to your configured syslog server.

Follow these steps to enable or disable syslog notifications for an alert type:

Before you begin

- Ensure you have administrator access to Cyber Vision Center.
- Confirm that a syslog server is configured. See Configure syslog.

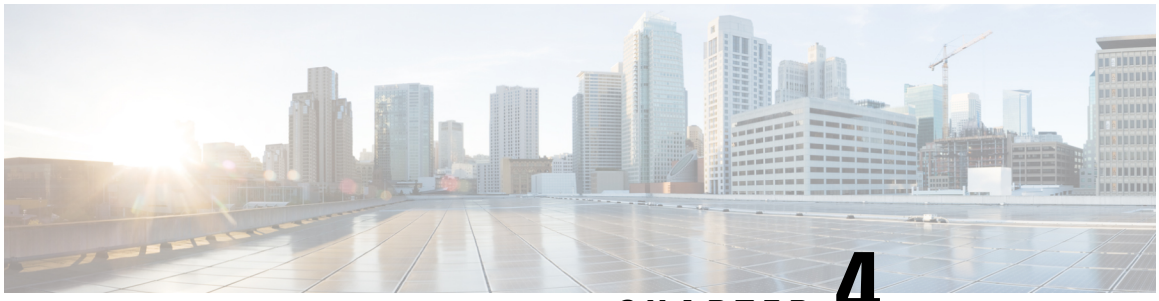
Procedure

Step 1 From the Cyber Vision New UI, choose **Configuration** > **Alerts**.

Step 2 Select an alert type.

Step 3 Enable or disable **Syslog Notification**.

When you enable syslog notifications in the Cyber Vision Center, you receive syslog messages on the configured syslog server whenever the system raises (or unmutes), clears, or mutes an alert.



CHAPTER 4

Log format

Log formats

A log format defines the structure and content of log messages generated by the system. The system supports two primary log formats: CEF (Common Event Format) and CEF Extended Time Precision.

CEF log format

Here are examples:

- Classic UI:

```
Aug 1 05:52:40 10.106.15.39 Aug 1 09:51:26 Center cybervision[1]: CEF:0|Cisco|Cyber
Vision|1.0|user_login|Login success to Cisco Cyber Vision|0|cat=Cisco Cyber Vision
Operations msg=User 'admin user (IP: 10.189.168.24)' has logged into Cyber Vision.
suser=admin@sentryo.net spriv=User SCVEventtype=user_login
SCVAuthorId=e91cc472-0a35-4b63-904b-585617db3873
center-id="564d3c3f-12f5-faff-b335-02d5a1246fc8"
```

- New UI:

```
Aug 1 07:42:29 10.106.15.39 Aug 1 11:41:15 Center cybervision[1]: CEF:0|Cisco|Cyber
Vision|2.0|alert_cleared|Prohibited vendors|2|cat=Property msg=This asset no longer
belongs to this prohibited vendor SCVAuthorId=e91cc472-0a35-4b63-904b-585617db3873
alertId=21e02d4e-4c97-4913-8755-6d22b6a345ac
alertRuleId=0a66abb3-075d-4f91-b3a3-5dd1c875929c assetFunctionalGroupId=
assetId=37dd7107-6eb8-51e3-a74b-de2a6e87bb2a assetName=Hirschmann e:ef:38
sensorNames=explore.pcap;25102016_wincc_nmap_sS.pcapng vendorName=Hirschmann
center-id="564d3c3f-12f5-faff-b335-02d5a1246fc8"
```

CEF Extended Time Precision log format

Examples:

- Classic UI:

```
Aug 1 07:48:21 10.106.15.42 2025-08-01T11:43:02.306722+00:00 Center cybervision[1]:
CEF:0|Cisco|Cyber Vision|1.0|syslog_update|Syslog configuration updated|1|cat=Cisco
Cyber Vision Administration msg=Syslog configuration has been changed by Admin User
(IP: 10.189.161.111) to local3.* udp172.26.154.121:514 suser=admin@sentryo.net spriv=User
 center-id="564de41b-d8c3-d753-0e6f-08b4bca5d596"
```

- New UI:

```
Aug 1 07:51:21 10.106.15.42 2025-08-01T11:46:03.329144+00:00 Center cybervision[1]:
CEF:0|Cisco|Cyber Vision|2.0|alert_raised|Severe vulnerabilities in monitored
entities|1|cat=Vulnerability msg=A severe vulnerability has been detected on a monitored
 asset alertId=10db6ad6-4968-4b56-98d8-e2d003ea1959
alertRuleId=35b5ba13-09cf-43b9-a750-5f547693a0bd assetFunctionalGroupId=
assetId=4d37a8a2-38be-5f60-98d0-783b4c7cb726 assetName=192.168.12.83 sensorNames=vlan.pcap
 vulnCSRS=51 vulnCVSSscore=7.5 vulnCveId=CVE-2023-51440 vulnName=TCP Sequence Number
Validation Vulnerability in Siemens CP343-1 Devices
center-id="564de41b-d8c3-d753-0e6f-08b4bca5d596"
```

Comparison of log format attributes

Format	Timestamp style	UI Variants	Use case
CEF	Second-precision timestamps	Classic UI/New UI	Regular event logging
CEF Extended Time Precision	Millisecond-precision timestamps	Classic UI/New UI	High-precision logging

Fields in CEF syslog messages

Timestamp format examples

- CEF examples:
  - `Aug 1 05:52:40 10.106.15.39 Aug 1 09:51:26 Center cybervision[1]:`
- CEF Extended Time Precision examples:
  - `Aug 1 07:48:21 10.106.15.42 2025-08-01T11:43:02.306722+00:00 Center cybervision[1]:`

Syslog message structure example

Fields in CEF syslog messages are separated by a vertical bar ("|").

- `CEF:0|Cisco|Cyber Vision|1.0|user_login|Login success to Cisco Cyber Vision|0|`

Fields with fixed values

The table lists syslog fields with fixed values for Classic UI and New UI.

For Classic UI	For New UI
“CEF:Version”: “CEF:0”	“CEF:Version”: “CEF:0”
“Device Vendor”: “Cisco”	“Device Vendor”: “Cisco”
“Device Product”: “Cyber Vision”	“Device Product”: “Cyber Vision”
“Device Version”: “1.0”	“Device Version”: “2.0”

For Classic UI	For New UI
center-id	center-id

Fields with values that vary by message type

The list below details the fields with values that vary depending on the message type.

- The extension contains two fixed fields at the beginning:
  - cat
  - msg
- The optional extension fields include:
  - For Classic UI:
    - spriv
    - SCVEventtype
    - SCVAuthorId
  - For New UI:
    - assetFunctionalGroupId
    - assetId
    - assetName
    - sensorNames
    - vulnCSRS
    - vulnCVSSscore
    - vulnCveId
    - vulnName
    - vendorName

Severity mapping for syslog messages

Syslog message severities:

- “0”: Low
- “1”: Medium
- “2”: High
- “3”: Critical

Fields in component and flow metadata

Note You can use component and flow metadata for events in the Classic UI.

Component metadata

If the event is associated with a component:

- An additional `component-id` key is present.
- Use the SCVComponentId of the component (as a string) from the Cisco Cyber Vision database.
- Use the SCVComponentId to query component data with the Cisco Cyber Vision API.

Flow metadata

If the event is associated with a flow, these additional keys are present:

Table 1: Descriptions of Flow Metadata Keys

Key	Description
SCVFlowId	ID of the flow
SCmp-a	IPv4 or IPv6 IP address of component A
SCmp-a-mac	MAC address of component A
SCmp-a-port	Port number of component A
SCmp-b	IPv4 or IPv6 IP address of component B
SCmp-b-mac	MAC address of component B
SCmp-b-port	Port number of component B
Sflow-properties	This is a string containing a comma-separated list of additional properties for the flow. These properties are protocol-dependent and this document does not list all possible values.

Important fields

SCVSensorId: This field corresponds to the sensor where the event was captured. The sensor ID appears in the `sbs-sensor` command output and is shown only for data captured from sensors (it is not present for login events).