



Cisco Cyber Vision syslog notification format Configuration Guide

First Published: 2022-11-17

Last Modified: 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

PREFACE	About this documentation v
	Document purpose v
	Warnings and notices v

CHAPTER 1	Overview 1
	Overview 1

CHAPTER 2	Syslog compatibility 3
	Syslog compatibility 3

CHAPTER 3	Syslog configuration 5
	Configure syslog in Cisco Cyber Vision 5
	Set the events to be sent to syslog 6

CHAPTER 4	Log format 9
	Common header 9
	Extension 10
	Fixed extension fields 10
	Optional extension fields 11
	Component metadata 11
	Flow metadata 12
	Important fields 12

CHAPTER 5	Annex 13
	Examples 13



About this documentation

- [Document purpose, on page v](#)
- [Warnings and notices, on page v](#)

Document purpose

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

This manual applies to **system versions 4.1.3**.

Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. 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 if proper precautions are not taken.



Important

Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.



Note

Indicates important information on the product described in the documentation to which attention should be paid.



CHAPTER 1

Overview

- [Overview, on page 1](#)

Overview

Cisco Cyber Vision monitors the industrial network using sensors which analyze industrial protocols and forward useful properties to a central appliance, the Center. The Center processes this data to generate a model of the current view of the installation, which can then be compared to previous states and serves as a base for cybersecurity analysis.

During this analysis, events can be generated to warn the administrator of significant happenings: for example, a PLC being reprogrammed is considered to be unusual activity and generates a new event. Events are categorized based on their type and associated data (e.g. a network component or a flow) and are usually presented as a timeline in Cisco Cyber Vision. They can also be exported by the Center using syslog to external servers like log aggregation platforms, SIEMs, and automated event correlation tools.

For example, logs can be emitted when the following events occur:

- Init: new industrial communications being established
- Start CPU: a PLC is being started
- Stop CPU: a PLC is being stopped
- Exception: an exception has been detected in an industrial connection
- Program Download: a PLC program is being downloaded
- Program Upload: a PLC program is being uploaded
- New Communication: a new communication flow is detected
- New Properties: new industrial properties have been detected on the network
- New Component: a new component has been identified on the network
- Protocol Decode Failure: a received packet has generated a decoding error



CHAPTER 2

Syslog compatibility

- [Syslog compatibility, on page 3](#)

Syslog compatibility

Cisco Cyber Vision uses the industry-standard *rsyslog* implementation internally and supports both UDP and TCP. The destination IP and port is to be set in Cisco Cyber Vision's admin page.

Syslog is a loosely defined format, that is there is very little standardization between vendors. The Cisco Cyber Vision Center follows best practices to format the exported data and make it easy to process.

Four syslog formats are available in Cisco Cyber Vision:

- Standard
- Standard/CEF
- RFC3164
- RFC3164/CEF

Standard and RFC3164 formats are available for historical reasons.

CEF (Common Event Format) is an open log management standard that improves interoperability of security-related information from different security and network devices and applications. CEF enables customers to use a common event log format so that data can easily be collected and aggregated for analysis by an enterprise management system.

In RFC3164 and RFC3164/CEF formats, a standard message header containing the date and time (i.e. a timestamp) is applied when a message is generated, as detected from the Windows event log, followed by the hostname and the message content. The value can either be RFC or RFC3164, as both values are equivalent.

RFC3164 provides nanoseconds information, whereas the standard format provides seconds.

For example, a timestamp with/without RFC3164 looks like:

- Timestamp with RFC3164: “2020-11-18T15:45:15.376781+00:00”
- Timestamp without RFC3164: “Nov 18 15:45:15”



CHAPTER 3

Syslog configuration

Syslog configuration can be performed by Product and Admin users.

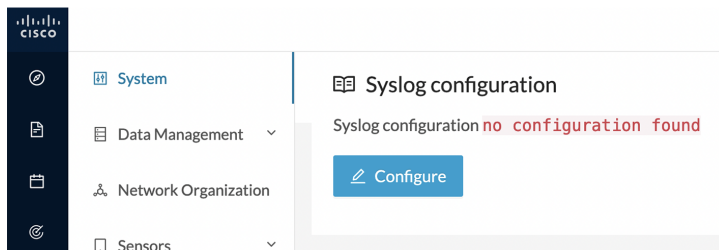
- [Configure syslog in Cisco Cyber Vision, on page 5](#)
- [Set the events to be sent to syslog, on page 6](#)

Configure syslog in Cisco Cyber Vision

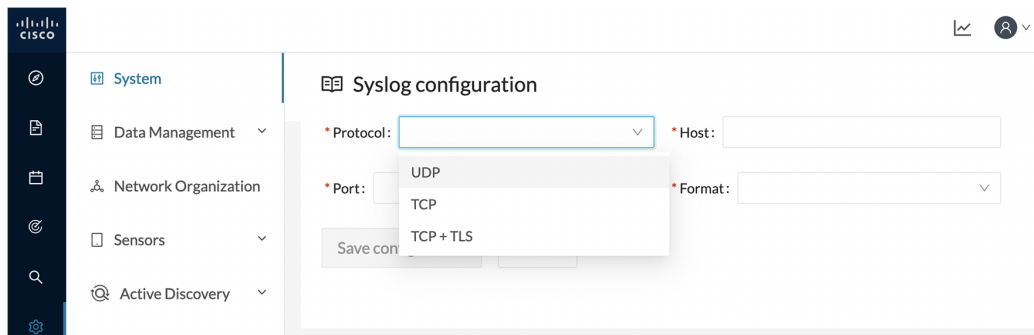
Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. To configure which machine syslogs will be sent to:

Step 1 In Cisco Cyber Vision, navigate to Admin > System > Syslog configuration.

Step 2 Click **Configure**.



Step 3 Select a protocol among UDP, TCP and TCP + TLS.



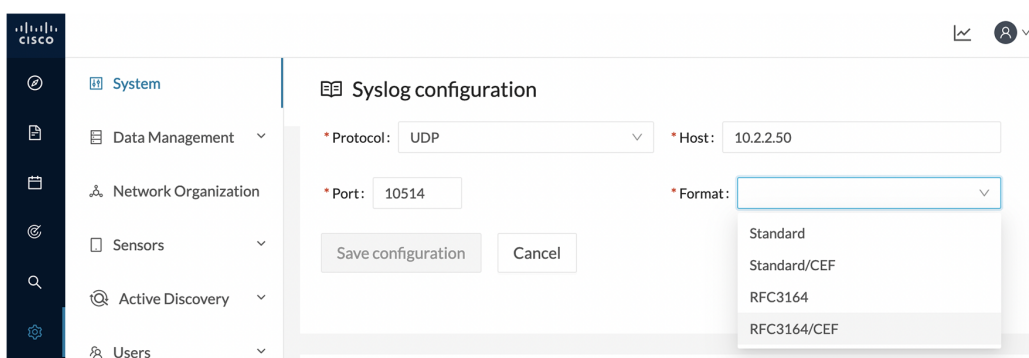
If you select TCP + TLS connection an additional **Set certificate** button is displayed to import a p12 file. This file is to be provided by the administrator of your SIEM solution to secure communications between the Center and the syslog collector.

Step 4 Enter the IP address of the SIEM reachable from the Administration network interface (i.e. eth0) of the Center.

Step 5 Enter the port on the SIEM that will receive syslogs.

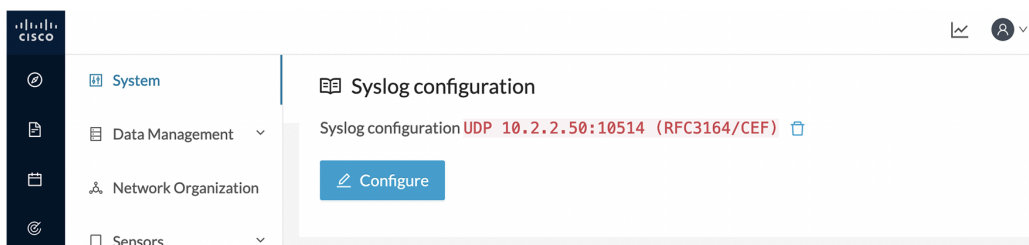
Step 6 Select the variant of syslog format:

- Standard: event messages are sent in a format specific to Cisco Cyber Vision and with legacy timestamps (one-second precision).
- CEF: industry standard ("Common Event Format") which is understood by most SIEM solutions (no extra configuration is needed on the SIEM). This is the recommended option.
- RFC3164: extended syslog header format with microsecond precision for timestamps.



Step 7 Click **Save configuration**.

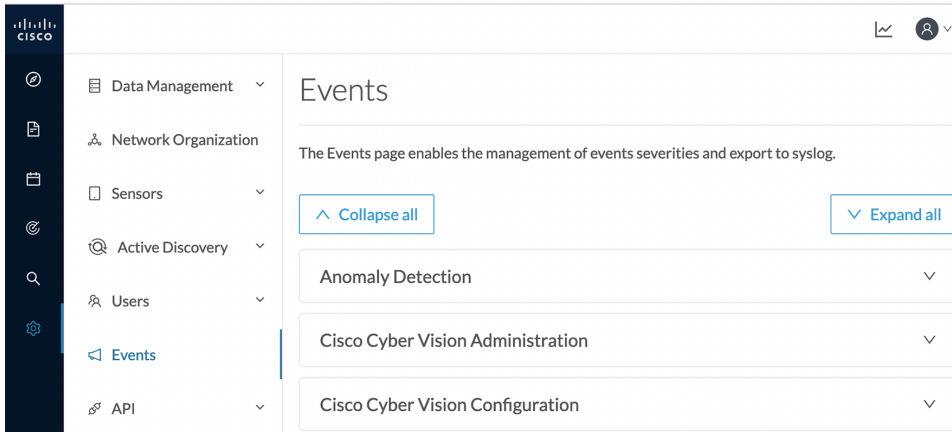
The syslog configuration is displayed on the Admin System page.



Set the events to be sent to syslog

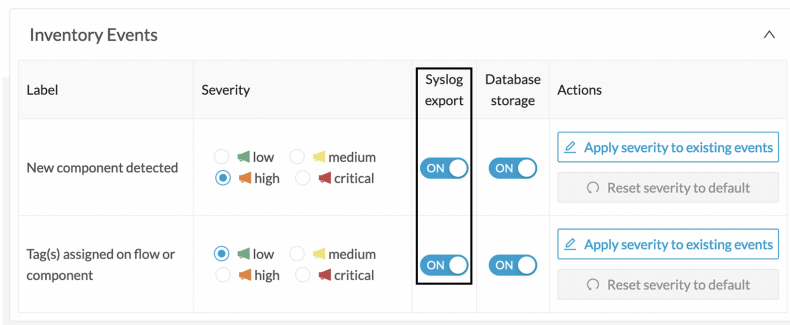
You can enable or disable the export of events to syslog. This option is active by default. However, you need to make sure that syslog has been configured for the export to work.

Step 1 In Cisco Cyber Vision, navigate to Admin > Events.



Step 2 Expand the categories of events you need to set up.

Step 3 Use the toggle button to enable/disable syslog export of the events.





CHAPTER 4

Log format

In this section, we will describe the structure of a syslog message.

Here is an example of a log:

```
Timestamp Center cybervision[xyz]: CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
2022-06-02T10:13:18.051306+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|component_new|New component detected|2|cat=Inventory Events msg=New component
detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff SCVEventtype=new_component
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

- [Common header, on page 9](#)
- [Extension, on page 10](#)
- [Component metadata, on page 11](#)
- [Flow metadata, on page 12](#)
- [Important fields, on page 12](#)

Common header

1. All syslog messages start with a timestamp and the string "Center cybervision[xyz]:".

For example:

```
2021-01-12T09:57:50.986718+00:00 Center cybervision[5485]:
```

Here the timestamp is in RFC3164 Unix format.

2. CEF syslog messages have the same format, which consists of a list of fields separated by a "|", such as:

```
CEF:Version|Device Vendor|Device Product|Device Version| Device Event Class
ID|Name|Severity|
```

For example:

```
CEF:0|Cisco|Cyber Vision|1.0|component_new|New component detected|2|
```

The following fields have a fixed value:

- "CEF:Version": will always be "CEF:0"
- "Device Vendor": "Cisco"
- "Device Product": "Cyber Vision"

- “Device Version”: “1.0”

Then, the fields below vary depending on the message type:

- Device Event Class ID: ID of the event type.
- Name: name of the event type.
- Severity: severity of the event type.

Refer to the [Annex](#) appended at the end of this document to see examples of syslog messages containing these fields.

Finally, there are 4 types of severities:

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

Extension

The extension part is made of two fixed fields and several optional fields.

Fixed extension fields

The extension starts with two fixed fields which are:

- “cat”: Category of the event
- “msg”: Message

For example:

```
cat=Inventory Events msg=New component detected on the network: IP 192.168.69.205, MAC  
d0:ec:35:ca:96:2a, vendor Cisco
```

The value of the category key is a string which can be one of the following values:

- Security Events
- Control Systems Events
- Inventory Events
- Cisco Cyber Vision Administration
- Cisco Cyber Vision Operations
- Cisco Cyber Vision Configuration
- Anomaly detection
- Signature Based Detection

- Extension-based alert
- Protocol Events

Messages' structure will be linked to the event type and will contain variable values like IP and MAC addresses.

For example:

- User 'John Smith' has logged into Cisco Cyber Vision
- Failed attempt to log in with the user 'admin@sentryo.net' (ip: 192.168.72.101)
- Baseline 'label' got 1 difference on 1 item
- New component detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff

Optional extension fields

After the 'msg' fields, several other fields can be found with relevant information for the event type.

For example:

- user_login_fail

```
suser=admin@sentryo.net src=192.168.72.101
```

- user_login

```
suser=admin@sentryo.net spriv=Administrator SCVEventType=user_login
SCVAuthorId=3b56a1a9-e438-4037-a2ef-31509cc0367a
```

- component_new

```
src=192.168.72.19 smac=00:0c:29:6f:e6:de SCVEventType=new_component
SCVComponentId=19543bc9-f0c6-51c3-8bdf-2b2aa5d3d161
SCVSensorId=0ab5830d-fela-46c3-842d-310662508ae6
```

- communication_new

```
cmp-a-mac=00:0c:29:6f:e6:e8 cmp-b-mac=d0:ec:35:ca:96:2a cmp-a=192.168.69.1
cmp-b=192.168.69.205 cmp-a-port=50630 cmp-b-port=22 SCVEventType=flow_new
SCVFlowCmpAComponentId=e19e4522-5e28-5f2d-a96e-60a7997b322f
SCVFlowCmpBComponentId=700f809f-fb3a-544d-a364-526f7b70f01b
SCVFlowCommunicationType=REMOTE_ADMIN SCVFlowId=a0a23d42-e30b-57b5-903c-04669a1755ad
SCVSensorId=0ab5830d-fela-46c3-842d-310662508ae6
```

All event types are listed at the end of this document. For some event types, some details are given below.

Component metadata

If the event is associated with a component, an additional component-id key is present. The value is the SCVComponentId (as a string) of the component in the Cisco Cyber Vision database. Component data can be queried via the Cisco Cyber Vision API using this SCVComponentId.

Flow metadata

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

- **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:**

a string containing a comma-separated list of additional properties for the flow. The properties are protocol-dependent and cannot be exhaustively enumerated in this document.

Important fields

SCVSensorId:

The value of sensor ID corresponds to the one from where the event was captured. It is the sensor ID that can be shown in 'sbs-sensor' command output.

We can see that property only on data captured from sensors, it's hidden for login events for example.



CHAPTER 5

Annex

- [Examples, on page 13](#)

Examples

Herebelow, you will find some examples of syslog messages.

```
<158>2022-06-02T10:13:14.195894+00:00 Center cybervision[1]: type="Software" severity="Medium"
category="Cisco Cyber Vision Administration" family="Cisco Cyber Vision" description="Admin
Admin has changed Syslog configuration to local3.* tcp192.168.3.21:1238"
<158>2022-06-02T10:13:14.427693+00:00 Center cybervision[1]: CEF:0|Cisco|Cyber
Vision|1.0|syslog_update|Syslog configuration updated|1|cat=Cisco Cyber Vision Administration
msg=Admin Admin has changed Syslog configuration to local3.* tcp192.168.3.21:1238
suser=admin@sentryo.net spriv=User
<158>2022-06-02T10:13:18.017445+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_new_wizard|Cisco Cyber Vision user created through the Wizard|0|cat=Cisco
Cyber Vision Administration msg=User 'Welcome Wizard' has created the user 'Jane Doe'.
SCVEventtype=user_manage_wizard SCVUserAction=created
SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.020814+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_new|Cisco Cyber Vision user created|0|cat=Cisco Cyber Vision Administration
msg=User 'John Smith' has created the user 'Jane Doe'. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=created SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.021489+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|restore_db_backup|Cisco Cyber Vision database restored|2|cat=Cisco Cyber Vision
Administration msg=The database has been restored from a previously exported dump.
suser=john@smith.com spriv=User SCVEventtype=dump_import
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVImportDataDumpFilename=/foo/bar
SCVImportDataMigrationRequired=true SCVImportDataUpdateSuccess=true
<158>2022-06-02T10:13:18.021995+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_delete|Cisco Cyber Vision user deleted|0|cat=Cisco Cyber Vision Administration
msg=User 'John Smith' deleted the user 'Jane Doe'. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=deleted SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
<158>2022-06-02T10:13:18.022578+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_update_email|Cisco Cyber Vision user email edited|0|cat=Cisco Cyber Vision
Administration msg=Changed the email from 'jane@doe.com' to 'dane@joe.com'. Changes done
by John Smith. The updated user now has administrator rights. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed_email SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.024364+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_update_password|Cisco Cyber Vision user password edited|0|cat=Cisco Cyber
Vision Administration msg=Changed the password of 'Dane Joe'. Changes done by John Smith.
```

```

The updated user now has administrator rights. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed password SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.026156+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_update_name|Cisco Cyber Vision user name edited|0|cat=Cisco Cyber Vision
Administration msg=Renamed from 'Jane Doe' to 'Dane Joe'. Changes done by John Smith. The
updated user now has administrator rights. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=renamed SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49 SCVUserNewAdminValue=true
SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe SCVUserOldAdminValue=false
SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.028013+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_update_rights|Cisco Cyber Vision user rights edited|0|cat=Cisco Cyber Vision
Administration msg=Rights have been changed for 'Dane Joe'. Changes done by John Smith.
The updated user now has administrator rights. suser=john@smith.com spriv=User
SCVEventtype=user_manage SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVUserAction=changed rights SCVUserId=fc003bb5-fe28-4959-8a9c-29e5d8f52a49
SCVUserNewAdminValue=true SCVUserNewEmailValue=dane@joe.com SCVUserNewValue=Dane Joe
SCVUserOldAdminValue=false SCVUserOldEmailValue=jane@doe.com SCVUserOldValue=Jane Doe
<158>2022-06-02T10:13:18.029973+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|offline_data_upload|Offline data file uploaded to Cisco Cyber Vision|0|cat=Cisco
Cyber Vision Operations msg=An offline data file named 'foo' was uploaded to Cyber Vision
(status: OK).
<158>2022-06-02T10:13:18.030028+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_reboot|System reboot|3|cat=Cisco Cyber Vision Operations msg=Center has
been rebooted from Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventtype=center_reboot SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030076+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_reboot|System reboot|3|cat=Cisco Cyber Vision Operations msg=Sensor
e8631c25-e78c-41f9-b0ab-736be48bc2c0 has been rebooted from Cyber Vision by John Smith.
suser=john@smith.com spriv=User SCVEventtype=sensor_reboot
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030116+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_shutdown|System shutdown|3|cat=Cisco Cyber Vision Operations msg=Center
has been shut down from Cyber Vision by John Smith. suser=john@smith.com spriv=User
SCVEventtype=center_shutdown SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030151+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|system_shutdown|System shutdown|3|cat=Cisco Cyber Vision Operations msg=Sensor
e8631c25-e78c-41f9-b0ab-736be48bc2c0 has been shut down from Cyber Vision by John Smith.
suser=john@smith.com spriv=User SCVEventtype=sensor_shutdown
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030235+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|user_login|Login success to Cisco Cyber Vision|0|cat=Cisco Cyber Vision Operations
msg=User 'John Smith' has logged into Cyber Vision. suser=john@smith.com spriv=User
SCVEventtype=user_login SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
<158>2022-06-02T10:13:18.030269+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|decode_failure|Decode failure|1|cat=Security Events msg=<Dissector message for
decode failure> SCVEventtype=decode_failure SCVFlowId=00000000-0000-0000-0000-000000000000
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.030308+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|decode_failure|Decode failure|1|cat=Security Events msg=<Dissector message for
decode failure> SCVEventtype=decode_failure SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.030346+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|analyzer_tags_assign|Tag(s) assigned on flow or component|0|cat=Inventory Events
msg=New tag(s) NETBIOS automatically assigned for the component. cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
<158>2022-06-02T10:13:18.030384+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sdb_imported|KnowledgeDB imported to Cisco Cyber Vision|1|cat=Cisco Cyber Vision
Administration msg=The user John Smith has imported a Sentryo DB file: 'SDB.dat'. It is

```

```

the version 42 of the Sentryo DB. suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.030434+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sdb_import|Processing KnowledgeDB import to Cisco Cyber Vision|1|cat=Cisco Cyber
Vision Administration msg=The user John Smith starts importing a knowledge DB file: SDB.dat
suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.030469+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_authorize|Sensor authorized|0|cat=Cisco Cyber Vision Administration
msg=Sensor EXP1-001 has been authorized. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=enrolled
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.030513+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_capture_mode_change|Sensor capture mode changed|1|cat=Cisco Cyber Vision
Administration msg=User 'John Smith' has changed the capture mode for sensor EXP1-001 from
all to industrial. suser=john@smith.com spriv=User SCVEventtype=sensor_capture_mode
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewCaptureMode=industrial
SCVSensorOldCaptureMode=all SCVSensorOldCustomInput=oldcustominput
<158>2022-06-02T10:13:18.031488+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_capture_mode_change|Sensor capture mode changed|1|cat=Cisco Cyber Vision
Administration msg=User 'John Smith' has changed the capture mode for sensor EXP1-001 from
custom "oldcustominput" to industrial. suser=john@smith.com spriv=User
SCVEventtype=sensor_capture_mode SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewCaptureMode=industrial
SCVSensorOldCaptureMode=custom SCVSensorOldCustomInput=oldcustominput
<158>2022-06-02T10:13:18.033368+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_new_usb|Sensor created by USB provisioning|0|cat=Cisco Cyber Vision
Administration msg=Sensor EXP1-001 has been manually created. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=created
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033429+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_delete|Sensor deleted|1|cat=Cisco Cyber Vision Administration msg=Sensor
EXP1-001 has been removed. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=erased
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033468+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_rename|Sensor renamed|0|cat=Cisco Cyber Vision Administration msg=Sensor
EXP1-001 has been renamed from 'oldname' to 'newname'. SCVEventtype=sensor
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSensorAction=renamed
SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0 SCVSensorNewName=newname
SCVSensorOldName=oldname
<158>2022-06-02T10:13:18.033514+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_reset|Sensor reset|1|cat=Cisco Cyber Vision Administration msg=Sensor
EXP1-001 has been erased. SCVEventtype=sensor SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVSensorAction=revoked SCVSensorId=e8631c25-e78c-41f9-b0ab-736be48bc2c0
<158>2022-06-02T10:13:18.033551+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sensor_high_ressources|Sensor high ressources usage|1|cat=Cisco Cyber Vision
Administration msg=Sensor [Name: blah, IP: 127.0.0.1] high usage of ressources: CPU [81%
>|= 80%], Memory [81% >|= 80%], Disk [81% >|= 80%] SCVEventtype=sensor SCVSensorAction=high
ressources usage SCVSensorCpu=81 SCVSensorDisk=81
SCVSensorId=00000000-0000-0000-0000-000000000000 SCVSensorIp=127.0.0.1 SCVSensorMemory=81
SCVSensorName=blah SCVSensorTime=2022-06-02T10:13:18Z SCVSensorVersion=3.1.0
<158>2022-06-02T10:13:18.034437+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|syslog_delete|Syslog configuration deleted|1|cat=Cisco Cyber Vision Administration
msg=John Smith has deleted Syslog configuration. suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.034497+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|syslog_update|Syslog configuration updated|1|cat=Cisco Cyber Vision Administration
msg=John Smith has changed Syslog configuration to local3.* UDP123.23.23.32:1234 (with
tls) suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.034538+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|sbs_update_failure|Cisco Cyber Vision failed to update|3|cat=Cisco Cyber Vision
Administration msg=System has not been updated from a previously imported file by John
Smith. suser=john@smith.com spriv=User SCVEventtype=sbs_update
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSbsUpdateUpdated=false
<158>2022-06-02T10:13:18.034577+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber

```

```

Vision|1.0|sbs_update|Cisco Cyber Vision updated|3|cat=Cisco Cyber Vision Administration
msg=System has been updated from a previously imported file by John Smith.
suser=john@smith.com spriv=User SCVEventtype=sbs_update
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVSbsUpdateUpdated=true
<158>2022-06-02T10:13:18.034622+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|token_new|Cisco Cyber Vision API token added|1|cat=Cisco Cyber Vision
Administration msg=Token <Name> has been added by John Smith suser=john@smith.com spriv=User
SCVEventtype=token SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVTokenAction=add
SCVTokenEnable=true SCVTokenId=3c18bc6b-0dac-4401-89f0-ce659b7ad3bd SCVTokenName=<Name>
<158>2022-06-02T10:13:18.034663+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|token_update|Cisco Cyber Vision API token updated|1|cat=Cisco Cyber Vision
Administration msg=Token <Name> has been updated by John Smith from
[name]=<Name>,expiration=none, enable=true] to [name]=<Name>,expiration=none,
enable=false] suser=john@smith.com spriv=User SCVEventtype=token
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVTokenAction=updated SCVTokenEnable=false
SCVTokenId=d419579a-8f5f-49bd-a726-f29b2d9fbd74 SCVTokenName=<Name> SCVTokenTokenEnable=true
SCVTokenTokenName=<Name>
<158>2022-06-02T10:13:18.036567+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|token_auth_fail|Cisco Cyber Vision API token authentication failed|1|cat=Cisco
Cyber Vision Administration msg=Token auth failed: FAIL REASON
<158>2022-06-02T10:13:18.036628+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|token_revoke|Cisco Cyber Vision API token revoked|1|cat=Cisco Cyber Vision
Administration msg=Token <Name> (<Hash>) has been revoked by John Smith suser=john@smith.com
spriv=User SCVEventtype=token SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVTokenAction=revoked SCVTokenEnable=true SCVTokenId=3c18bc6b-0dac-4401-89f0-ce659b7ad3bd
SCVTokenName=<Name>
<158>2022-06-02T10:13:18.036669+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|event_metadata_update|Cisco Cyber Vision events settings updated|2|cat=Cisco
Cyber Vision Administration msg=User 'John Smith' updated settings of the event ''
retroactively. suser=john@smith.com spriv=User SCVEventtype=event_metadata_update
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2 SCVEventMetadataIsRetroactive=true
SCVEventMetadataNewSeverity=Low SCVEventMetadataNewSyslogExport=false
SCVEventMetadataOldSeverity=Low SCVEventMetadataOldSyslogExport=false
<158>2022-06-02T10:13:18.037663+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|vuln_ack|Component vulnerability acknowledged in Cisco Cyber Vision|1|cat=Security
Events msg=Vulnerability Big Vuln on component Component A has been ignored by John Smith
(<Comment>)
<158>2022-06-02T10:13:18.037726+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|vuln_detect|Component vulnerability detected|2|cat=Security Events msg=The
component '1.2.3.4' has been detected vulnerable to : Big Vuln SCVEventtype=vulns_assigned
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
SCVVulns0VulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8 SCVVulnsNumber=1
<158>2022-06-02T10:13:18.037774+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|component_no_more_vuln|Component no more vulnerable|1|cat=Security Events msg=The
component '1.2.3.4' seems no more vulnerable to : Big Vuln SCVEventtype=vulns_unassigned
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
SCVVulns0VulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8 SCVVulnsNumber=1
<158>2022-06-02T10:13:18.037821+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|vuln_unack|Component vulnerability unacknowledged in Cisco Cyber
Vision|2|cat=Security Events msg=Vulnerability Big Vuln on component Component A is no
longer ignored (John Smith) SCVEventtype=user_vulnerabilities
SCVAuthorId=823b7cf8-2618-4b76-9d97-8b0cc86b25f2
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3 SCVVulnAction=unack
SCVVulnId=08cec8a3-5b9d-4b98-87c7-9d909488b1c8
<158>2022-06-02T10:13:18.037861+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|port_scan||1|cat= msg=Port scan detected by 1.2.3.4 on 4.3.2.1
cmp-a=mac=aa:bb:cc:dd:ee:ff cmp-b=mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
SCVEventtype=port_scan SCVPortScanDetailsProtocol=TCP
SCVPortScanTargetComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVPortScannerComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
<158>2022-06-02T10:13:18.037902+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_new|Cisco Cyber Vision Baseline created|0|cat=Cisco Cyber Vision

```

```

Configuration msg=Baseline 'label' has been created by 'John Smith' suser=john@smith.com
spriv=User
<158>2022-06-02T10:13:18.037946+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_update_meta|Cisco Cyber Vision Baseline updated|0|cat=Cisco Cyber Vision
Configuration msg=Baseline 'label' has been edited by 'John Smith', new label is 'label',
new description is 'description' suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.037985+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_delete|Cisco Cyber Vision Baseline deleted|0|cat=Cisco Cyber Vision
Configuration msg=Baseline 'label' has been deleted by 'John Smith' suser=john@smith.com
spriv=User
<158>2022-06-02T10:13:18.038030+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_update|Configuration of Cisco Cyber Vision Baseline updated|1|cat=Cisco
Cyber Vision Configuration msg=Baseline 'label' has been edited by 'John Smith', new scan
period is '15' seconds suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.038100+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_differences|Differences detected on a Baseline|2|cat=Anomaly Detection
msg=Baseline 'label' got 1 difference on 1 item
<158>2022-06-02T10:13:18.040030+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_difference_ack|Differences acknowledged and included to a
Baseline|1|cat=Cisco Cyber Vision Configuration msg=Difference included in baseline 'label'
by 'John Smith' with message 'comment'. The problematic component was 'Component A'.
suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.041577+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_difference_nack|Anomalies reported on a Baseline|3|cat=Cisco Cyber
Vision Configuration msg=Incident declared in baseline 'label' by 'John Smith' with message
'comment'. The problematic component was 'Component A'. suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.042941+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_difference_ignore|Differences acknowledged but not included in the
Baseline|1|cat=Cisco Cyber Vision Configuration msg=Difference ignored in baseline 'label'
by 'John Smith' with message 'comment'. The problematic component was 'Component A'.
suser=john@smith.com spriv=User
<158>2022-06-02T10:13:18.043347+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|baseline_delete_element|Component, Activity or Variable removed from a
Baseline|0|cat=Cisco Cyber Vision Configuration msg=Component 'Component A' was removed
from the baseline 'label' by 'John Smith' with message 'comment'. suser=john@smith.com
spriv=User
<158>2022-06-02T10:13:18.043523+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|data_expired|Data expiration|2|cat=Cisco Cyber Vision Operations msg=10 old flows
have been purged SCVEventtype=data_expired SCVObjectsName=flow SCVObjectsNb=10
<158>2022-06-02T10:13:18.043703+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|ids|Anomaly detected by signature|3|cat=Signature based Detection msg=Snort
alert id XXX with signature "blablabla" 127.0.0.1:443 -> 192.168.1.1:8080 proto blob
SCVEventtype=snort_event SCVSnortEventDstAddr=192.168.1.1 SCVSnortEventDstPort=8080
SCVSnortEventMsg=blablabla SCVSnortEventService=blob SCVSnortEventSid=XXX
SCVSnortEventSrcAddr=127.0.0.1 SCVSnortEventSrcPort=443
<158>2022-06-02T10:13:18.043846+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|extension_alert|Extension-related alert|3|cat=Extension-based alert msg=test
alert message from extension
<158>2022-06-02T10:13:18.044003+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|extension_info|Extension-related info|0|cat=Extension-based alert msg=test info
message from extension
<158>2022-06-02T10:13:18.047080+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|admin_connection|New connection as a component admin|2|cat=Control Systems Events
msg=New admin connection has been detected from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=admin_connection SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.049266+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|communication_new|New communication|2|cat=Security Events msg=New FTP communication
has been detected between 1.2.3.4:1234 and 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321

```

```

SCVEventtype=flow_new SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3 SCVFlowCommunicationType=FTP
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.051306+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|component_new|New component detected|2|cat=Inventory Events msg=New component
detected on the network: IP 1.2.3.4, MAC aa:bb:cc:dd:ee:ff SCVEventtype=new_component
SCVComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.051380+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|flow_control_action|Action on control parameters|3|cat=Control Systems Events
msg=New <Process Name> control action (<Variable Name>: <New Value>) has been detected from
1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa
cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_control_action
SCVEventDetailsOrientation= SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowControlActionProcessName=<Process
Name> SCVFlowControlActionValue=<New Value> SCVFlowControlActionVarName=<Variable Name>
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.053586+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|exception|Protocol exception detected|2|cat=Security Events msg=Exception
'illegal-function' has been detected between 1.2.3.4 and 4.3.2.1 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_exception SCVExceptionLabel=illegal-function
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=00000000-0000-0000-0000-000000000000
<158>2022-06-02T10:13:18.055526+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|flow_login_failure|Authentication failure on component|2|cat=Security Events
msg=3 unsuccessful authentication attempts detected from 1.2.3.4:1234 on 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_login_failure SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowLoginFailureAttempt0=wrongpassword1
SCVFlowLoginFailureAttempt1=wrongpassword2 SCVFlowLoginFailureAttempt2=wrongpassword3
SCVFlowLoginFailureNumberOfAttempts=3 SCVFlowLoginFailureProtocol=
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.057547+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|flow_forced_variable|Forced variable|3|cat=Control Systems Events msg=New variable
forced (<VarName>: <NewVal>) has been detected from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_forced_variable SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowForcedVariableValue=<NewVal>
SCVFlowForcedVariableVarName=<VarName> SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.059649+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|init|New init command|3|cat=Control Systems Events msg=Init has been detected
from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa
cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_init
SCVEventDetailsOrientation= SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.061499+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|program_download|New program downloaded|2|cat=Control Systems Events msg=New
program has been downloaded, flow from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_program_downloaded
SCVEventDetailsOrientation= SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3

```



```

SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.063244+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|program_download|New program downloaded|2|cat=Control Systems Events msg=New
program download requested from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_program_download_started SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.064925+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|program_upload|New program uploaded|2|cat=Control Systems Events msg=New program
has been uploaded, flow from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_program_uploaded SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.067033+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|network_event|Network event redundancy|1|cat=Protocol Events msg=New network
redundancy event 'failover' has been detected between aa:bb:cc:dd:ee:ff and ff:ee:dd:cc:bb:aa
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_network_redundancy
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=failover
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.068617+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|router_event|Router event highavailability|1|cat=Protocol Events msg=New router
ha event 'Active' has been detected between aa:bb:cc:dd:ee:ff and ff:ee:dd:cc:bb:aa
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_router_ha
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Active
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.070185+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|firmware_activation|Controler Firmware activation|3|cat=Control Systems Events
msg=Firmware Activation has been detected from 1.2.3.4:1234 to 4.3.2.1:4321
cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1
cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=firmware_activation SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.071706+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|smb|SMB protocol event|2|cat=Protocol Events msg=SMB event from 1.2.3.4:1234 to
4.3.2.1:4321 SMB event cmp-a-mac=aa:bb:cc:dd:ee:ff cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4
cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321 SCVEventtype=flow_smb
SCVEventDetailsOrientation= SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=SMB event
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.073187+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|weak_encryption|Weak encryption event|1|cat=Protocol Events msg=Weak encryption
from 1.2.3.4:1234 to 4.3.2.1:4321 weak encryption description cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_weak_encryption SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=weak encryption
description SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.074756+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber

```

```

Vision|1.0|online|Online event|3|cat=Control Systems Events msg=Online command has been
detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_online SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.076239+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|offline|Offline event|3|cat=Control Systems Events msg=Offline command has been
detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_offline SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.077706+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|force_mode|Force mode change event|3|cat=Control Systems Events msg=Force mode
Enabled has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_force_mode SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Enabled
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.079242+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|force_mode|Force mode change event|3|cat=Control Systems Events msg=Force mode
Disabled has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_force_mode SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3 SCVFlowProtocolEventDetected=Disabled
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.080730+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|reset_process|Reset process command|2|cat=Control Systems Events msg=Reset Process
command has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_reset_process SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.082348+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|restart_cpu|New restart cpu command|3|cat=Control Systems Events msg=Restart CPU
command has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_restart_cpu SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.083902+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|start_cpu|New start cpu command|3|cat=Control Systems Events msg=Start CPU command
has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_start_cpu SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
<158>2022-06-02T10:13:18.085398+00:00 Center cybervision[5485]: CEF:0|Cisco|Cyber
Vision|1.0|stop_cpu|New stop cpu command|3|cat=Control Systems Events msg=Stop CPU command

```

```
has been detected from 1.2.3.4:1234 to 4.3.2.1:4321 cmp-a-mac=aa:bb:cc:dd:ee:ff
cmp-b-mac=ff:ee:dd:cc:bb:aa cmp-a=1.2.3.4 cmp-b=4.3.2.1 cmp-a-port=1234 cmp-b-port=4321
SCVEventtype=flow_stop_cpu SCVEventDetailsOrientation=
SCVFlowCmpaComponentId=d9c5e600-4df4-4542-806d-59dcefb3c1df
SCVFlowCmpbComponentId=eea2e756-583e-4bc9-85ef-46fd9036bdb3
SCVFlowId=501332f3-4499-40a4-ba2d-bb7d76c8e1a3
SCVSensorId=0b97afea-929b-4e6a-9791-545466d0f405
```

