Syslog configuration

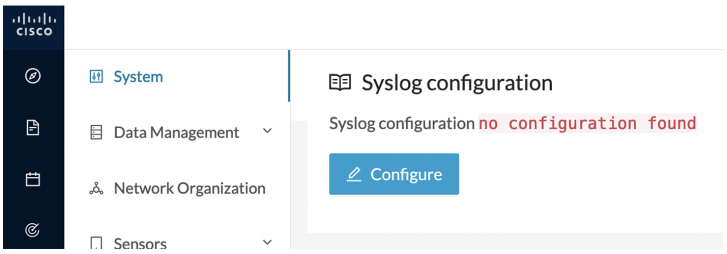
Syslog configuration can be performed by Product and Admin users.

Configure syslog in Cisco Cyber Vision

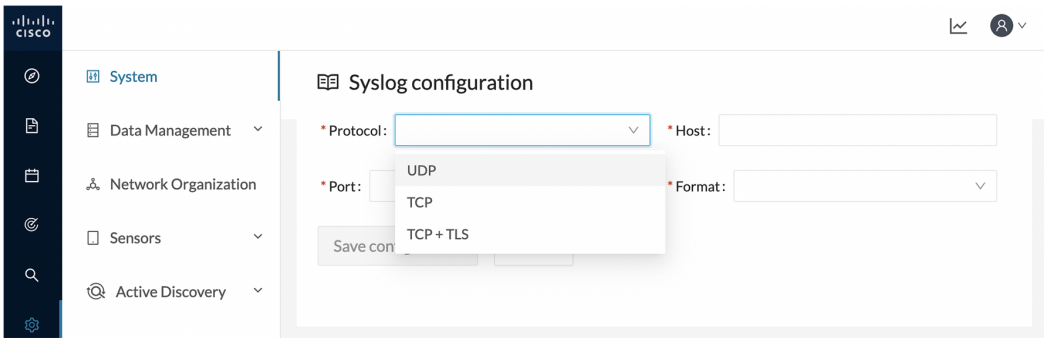
Cisco Cyber Vision provides syslog configuration so that events can be exported and used by a SIEM. To configure which machine syslogs will be sent to:

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.



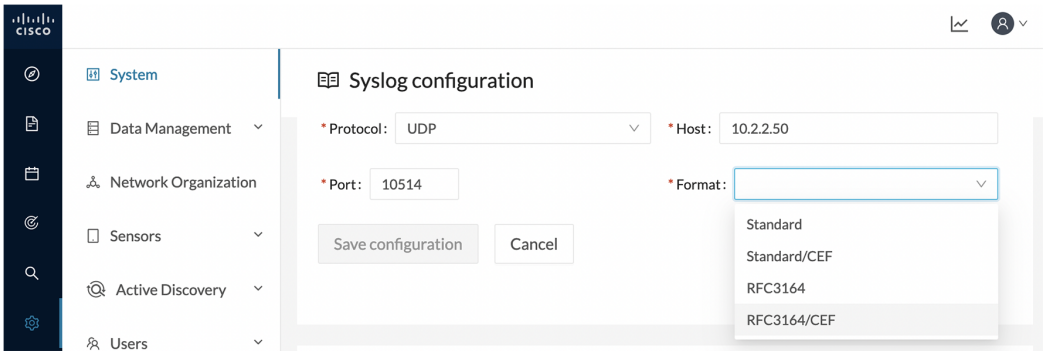
If you select TCP + TLS connection an additional **Set certificate** button is displayed to import a p12 file. This file is to be provided by the administrator of your SIEM solution to secure communications between the Center and the syslog collector.

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.

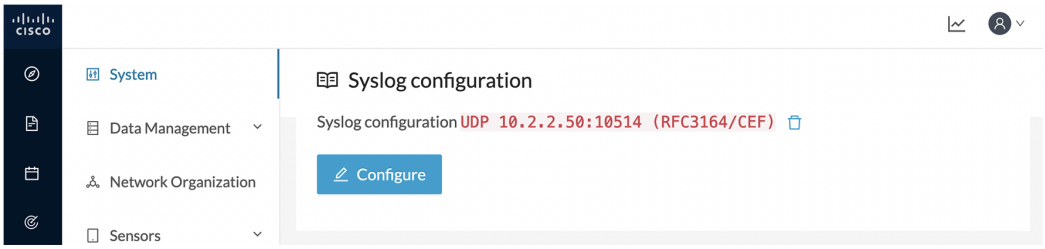
Step 6 Select the variant of syslog format:

- 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**.

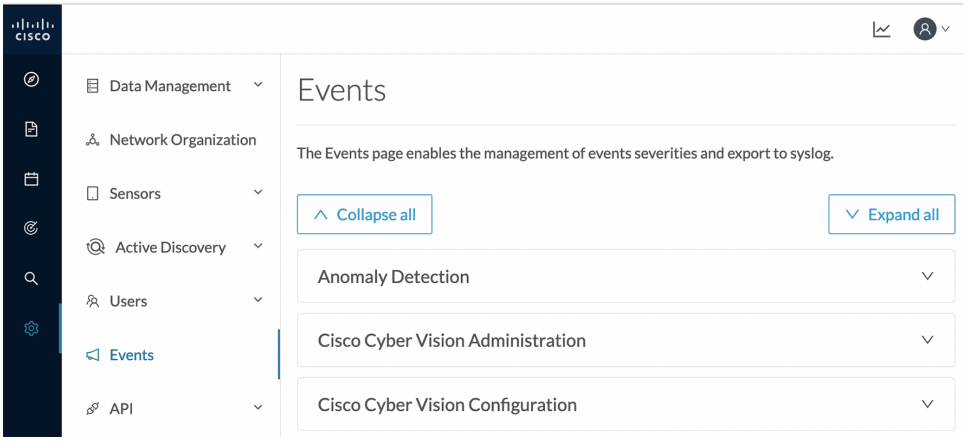
The syslog configuration is displayed on the Admin System page.



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.