Log Management

Securing & Maintaining IP cameras

Table of contents

1 **Log Management** **3**

2 **Syslog Configuration on the Camera** **4**

3 **Sample Ubuntu 22.04 LTS Syslog Configuration** **5**

3.1 UDP Syslog Configuration 5

3.2 TCP Syslog Configuration 5

3.3 TCP / TLS Syslog Configuration 6

3.4 Generate certificates on the Ubuntu Server 7

3.4.1 Generate a CA with OpenSSL 7

3.4.2 Generate Syslog Server Certificates 7

3.4.3 Generate Syslog Client Certificate for Camera 7

4 **References** **8**

1 Log Management

Keeping watch of the logs is an important part of security analysis or maintenance activity. Regular review of the logs can reveal configuration problems or security violations like false logins.

Each camera will reserve a fixed space for logging, capable of roughly 500+ log entries, but will overwrite older logs if that space is filled.

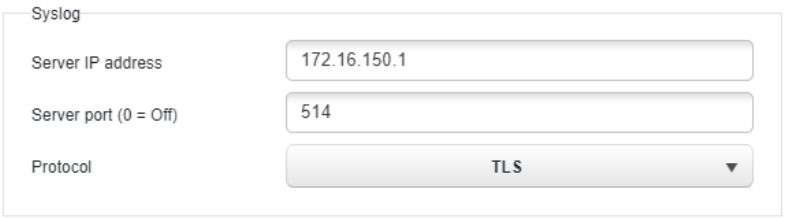
For analyzing logs and storing them for long term it is advised to send the logs of the camera to a syslog server or a SIEM (Security Information and Event Management) system.

Most SIEM system support either direct receival of logs via syslog protocol or the collection of logs from a syslog server.

This documentation describes the configuration of the camera and a quick setup of a Ubuntu Server in case no existing system is available.

2 Syslog Configuration on the Camera

The syslog server can be configured in Network – Advanced



The IP address and port of the server (default 514 for syslog) can be configured here. There are three syslog protocols available with each different advantages and disadvantages.

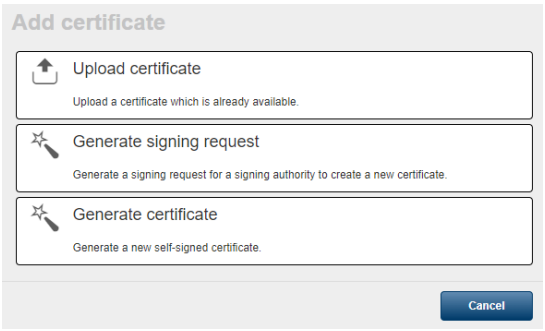
- ▶ UDP = fast, but unreliable in case of packet loss
- ▶ TCP = slower, but more reliable as it offers retransmit of lost packages
- ▶ TLS = Like TCP, additionally encrypted

Note: If the network is not fully trusted it is recommended to use TLS encryption for syslog.

Configure Client Certificate on the camera

In case TLS is selected as syslog protocol, the camera needs a proper client certificate to authenticate against the TLS syslog server.

An existing certificate in form of a PKCS#12 file can be uploaded (e.g. client-cert.p12, see below) or a signing request can be generated and sent to an existing PKI infrastructure to receive a certificate.



After the certificate has been installed, the usage “SYSLOG client” needs to be set.

3 Sample Ubuntu 22.04 LTS Syslog Configuration

Here is an example configuration how to set up a clean Ubuntu 22.04 LTS to receive syslog messages.

Ubuntu 22.04 already includes the software *rsyslog* which can receive either UDP, TCP or TLS syslog messages.

3.1 UDP Syslog Configuration

Edit rsyslog configuration

sudo nano /etc/rsyslog.conf

To enable UDP based syslog, uncomment the following two lines

module(load="imudp")
input(type="imudp" port="514")

Restart rsyslog

service rsyslog restart

3.2 TCP Syslog Configuration

Edit rsyslog configuration

sudo nano /etc/rsyslog.conf

To enable TCP based syslog, uncomment the following two lines

module(load="imtcp")
input(type="imtcp" port="514")

Restart rsyslog

service rsyslog restart

3.3 TCP / TLS Syslog Configuration

For enabling TLS-based syslog, certificates are needed on the client (IP camera) as well as on the server (Ubuntu / rsyslog in this case).

It is recommended to integrate into any existing PKI Infrastructure and generate the required certificates there.
In case no existing PKI infrastructure is available, see next chapter “Generate certificates on the Ubuntu server” for the necessary commands to generate certificates on the Ubuntu system.

For TLS-based syslog an additional module is required to handle the encryption:

sudo apt-get install rsyslog-gnutls

Edit rsyslog configuration

sudo nano /etc/rsyslog.conf

To enable TCP based syslog, uncomment the following two lines:

module(load="imtcp")
input(type="imtcp" port="514")

Replace the last line with:

input(type="imtcp" port="514" StreamDriver.Name="gtls" StreamDriver.Mode="1"
StreamDriver.Authmode="x509/certvalid")

Add the following lines at the end of the file. The necessary certificates files need to be put in the folder /etc/syslog/ or generated there (see next chapter).

$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/rsyslog/ca.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog/server-cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog/server-key.pem

3.4 Generate certificates on the Ubuntu Server

The following commands will manually create a CA certificate and two certificates which can be used in this scenario.

3.4.1 Generate a CA with OpenSSL

openssl genrsa -aes256 -out ca-key.pem 2048
openssl req -x509 -new -nodes -extensions v3_ca -key ca-key.pem -days 3650 -out ca.pem -sha256

3.4.2 Generate Syslog Server Certificates

openssl genrsa -out server-key.pem 2048
openssl req -new -key server-key.pem -out server-cert.csr -sha256
openssl x509 -req -in server-cert.csr -CA ca.pem -CAkey ca-key.pem -CAcreateserial -out server-cert.pem -days 800 -sha256

3.4.3 Generate Syslog Client Certificate for Camera

openssl genrsa -out client-key.pem 2048
openssl req -new -key client-key.pem -out client-cert.csr -sha256
openssl x509 -req -in client-cert.csr -CA ca.pem -CAkey ca-key.pem -CAcreateserial -out client-cert.pem -days 800 -sha256
openssl pkcs12 -export -3des -out client-cert.p12 -in client-cert.pem -inkey client-key.pem

4 References

1. RFC 5424, The Syslog Protocol
https://tools.ietf.org/html/rfc5424

2. RFC 5425, Transport Layer Security (TLS) Transport Mapping for Syslog
https://tools.ietf.org/html/rfc5425

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com