IQSIGHT

LOG MONITORING AND TIME SYNCHRONIZATION

SECURING AND MAINTAINING IP CAMERAS

2.0.0 2026-06

Visual intelligence for a world uninterrupted.

CONTENTS

Overview 3
Log Management 3
Syslog Configuration on the Camera 3
Sample Ubuntu 26.04 LTS Syslog Configuration 4
Log Message Format 6
Time Synchronization 7
Time Configuration on the Camera 7
Distribute NTP Server via DHCP 7
Enable NTP Server on Windows 8
Install NTP Server on Ubuntu 26.04 8
Best Practices 9
References 9
Summary 9

This guide provides step-by-step instructions for configuring syslog forwarding and time synchronization on IQSIGHT IP cameras. It is intended for security integrators who need to set up centralized log collection and accurate timekeeping across camera deployments.

OVERVIEW

Centralized logging and accurate time synchronization are essential for effective security monitoring. Without them, log correlation across devices becomes unreliable, incident timelines cannot be reconstructed, and forensic analysis loses credibility.

IQSIGHT cameras generate syslog-formatted log messages that can be forwarded to any standard syslog server or SIEM system. Time synchronization ensures that timestamps across all cameras and infrastructure devices align, enabling accurate event correlation.

LOG MANAGEMENT

Regularly reviewing camera logs reveals configuration problems, failed login attempts, and other security-relevant events. Each camera reserves a fixed space of approximately 249 KB for internal log storage — enough for about 1,800 log messages. Once that space fills, older entries are overwritten.

To retain logs long-term and enable centralized analysis, forward them to a syslog server or SIEM system.

SYSLOG CONFIGURATION ON THE CAMERA

Configure the syslog server in **Network** → **Advanced** on the camera web interface.

Set the IP address and port of the syslog server (default port: `514`). Three transport protocols are available:

- **UDP** — Fast but unreliable; packets may be lost without retransmission.
- **TCP** — Slower but reliable; lost packets are retransmitted.
- **TLS** — Same reliability as TCP, with added encryption.

> **NOTICE**
>
> If the network is not fully trusted, use TLS encryption for syslog transport. This prevents attackers from intercepting log data containing security-relevant events such as login attempts.

Configure a Client Certificate for TLS Syslog

When TLS is selected as the syslog protocol, the camera requires a client certificate to authenticate against the TLS syslog server.

1. Upload an existing certificate in PKCS#12 format (e.g., `client-cert.p12`), or generate a CSR and submit it to your PKI infrastructure.
2. After the certificate is installed, set its usage to **SYSLOG client** in the certificate store.

SAMPLE UBUNTU 26.04 LTS SYSLOG CONFIGURATION

The following examples show how to configure a clean Ubuntu 26.04 LTS system to receive syslog messages using rsyslog, which is included by default.

UDP Syslog

Edit the rsyslog configuration:

```
sudo nano /etc/rsyslog.conf
```

Uncomment the following two lines:

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

Restart rsyslog:

```
service rsyslog restart
```

TCP Syslog

Edit the rsyslog configuration:

```
sudo nano /etc/rsyslog.conf
```

Uncomment the following two lines:

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

Restart rsyslog:

```
service rsyslog restart
```

TLS Syslog

TLS-based syslog requires certificates on both the camera (client) and the syslog server. Integrate with your existing PKI infrastructure where possible. If no PKI is available, see the section below to generate certificates manually.

Install the required TLS module:

```
sudo apt install rsyslog-gnutls
```

Edit the rsyslog configuration:

```
sudo nano /etc/rsyslog.conf
```

Uncomment the TCP module lines, then replace the input line:

```
module(load="imtcp")
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, pointing to the certificate files in `/etc/rsyslog/`:

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

Restart rsyslog:

```
service rsyslog restart
```

Generate Certificates for TLS Syslog

If no PKI infrastructure is available, generate the required certificates manually using OpenSSL:

Generate a CA:

```
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
```

Generate the syslog server certificate:

```
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
```

Generate the syslog client certificate for the 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 -descert -legacy \
  -out client-cert.p12 -in client-cert.pem -inkey client-key.pem
```

Upload `client-cert.p12` to the camera and set the certificate usage to **SYSLOG client**. Copy `ca.pem`, `server-cert.pem`, and `server-key.pem` to `/etc/rsyslog/` on the syslog server.

LOG MESSAGE FORMAT

IQSIGHT cameras use the syslog message format defined in RFC 5424. Below is a breakdown of a sample log message:

```
<14>1 2025-04-08T14:50:33.091+01:00 172.31.31.101 user_mgmt service@http ID_USER_LOGIN
- Login by user service from IP 172.31.31.101 to HTTP using Password
```

Field	Value	Meaning
`<14>1`	Priority 14, version 1	Facility 1 (user-level) × 8 + Severity 6 (Informational)
`2025-04-08T14:50:33.091+01:00`	ISO 8601 timestamp	Date, time with milliseconds, time zone offset
`172.31.31.101`	Source IP	IP address that caused the event
`user_mgmt`	Application name	Internal camera application (User Management)
`service@http`	Tag	User name and network service (user@service)
`ID_USER_LOGIN`	Message ID	Unique event identifier for filtering
`-`	Structured data	No additional structured data
`Login by user service...`	Message	Human-readable event description

Syslog severity levels:

Severity	Level	Description
0	Emergency	System is unusable
1	Alert	Immediate action required
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions

5	Notice	Normal but significant
6	Informational	Informational messages
7	Debug	Debug-level messages

The priority value is calculated as: $\text{Priority} = \text{Facility} \times 8 + \text{Severity}$. The facility is typically set to 1 (user-level).

TIME SYNCHRONIZATION

Accurate, synchronized time across all cameras is critical for two reasons:

1. **Log correlation** — Security events from different devices can only be correlated if their timestamps align.
2. **Video stream synchronization** — Following a person across multiple camera views requires matching time references.

Use a central time server (NTP) in the network to synchronize all devices.

TIME CONFIGURATION ON THE CAMERA

The time server can be configured automatically via DHCP or manually in the camera's time settings. Three protocols are available:

- **Time Protocol (RFC 868)** — Legacy protocol with only 1-second precision. Use only for compatibility with older infrastructure.
- **SNTP** — Implementation of the standard NTP protocol, widely supported by Windows and Linux servers. Provides good precision and is the recommended option.
- **TLS** — Derives time from a TLS handshake with any HTTPS server. Easy to deploy (no dedicated time server needed), but lower precision than SNTP. Also known as TLS-Date.

> **Tip:** Use SNTP for the best balance of precision and compatibility. Reserve TLS-Date for environments where no NTP server is available and a nearby HTTPS server can serve as a time reference.

DISTRIBUTE NTP SERVER VIA DHCP

If the camera receives its IP address via DHCP, the DHCP server can also push the NTP server address automatically.

For SNTP, use **DHCP option 42** (NTP Servers):

Linux DHCP server:

```
option ntp-servers <ip-of-NTP-server>;
```

Windows DHCP server: Add a server option for option 42 (NTP Servers) in the DHCP management console.

> **NOTICE**
>
> DHCP option 4 (Time Servers) sets the time server type to RFC 868 Time Protocol automatically. Use option 42 for SNTP.

ENABLE NTP SERVER ON WINDOWS

Every Windows Server installation includes an NTP server. To enable it:

1. Open `regedit.exe`.
2. Navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer` and set `Enabled` to `1`.
3. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Config` and set `AnnounceFlags` to `5`.
4. Restart the **Windows Time** service.

> **Tip:** The Windows server syncs against `time.windows.com` by default. To use a different upstream server, change the `NtpServer` value in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Config`.

INSTALL NTP SERVER ON UBUNTU 26.04

Install the NTP package:

```
sudo apt-get install ntpsec
```

Allow queries from the camera subnet by editing `/etc/ntpsec/ntp.conf`:

```
sudo nano /etc/ntpsec/ntp.conf
```

Add the following line (adjust the IP range and subnet mask to match your camera network):

```
restrict 172.16.16.0 mask 255.255.255.0 nomodify notrap nopeer
```

Restart the NTP service:

```
service ntpsec restart
```

BEST PRACTICES

1. **Use TLS for syslog** in any network that is not fully physically protected against unauthorized access.
2. **Forward logs to a central syslog server or SIEM** — do not rely on internal camera log storage alone.
3. **Use SNTP** as the preferred time synchronization protocol for its precision and broad compatibility.
4. **Push the NTP server address via DHCP option 42** to automate time server configuration across all cameras.
5. **Monitor log messages with severity 0–3** (Emergency through Error) for security-relevant events.
6. **Verify time synchronization** after initial deployment and after any network changes.

REFERENCES

- RFC 5424 — The Syslog Protocol: https://tools.ietf.org/html/rfc5424
- RFC 5425 — TLS Transport Mapping for Syslog: https://tools.ietf.org/html/rfc5425
- RFC 868 — Time Protocol: https://tools.ietf.org/html/rfc868
- RFC 4330 — Simple Network Time Protocol (SNTP) Version 4: https://tools.ietf.org/html/rfc4330

SUMMARY

Forward camera logs via syslog (preferably TLS-encrypted) to a central server or SIEM for long-term retention and security analysis. Synchronize time across all devices using SNTP via a central NTP server. These two measures enable reliable incident detection, accurate event correlation, and trustworthy forensic analysis.