

## LOGZILLA DOCUMENTATION

# Using TLS Tunnels

Secure syslog transport over TLS on LogZilla, covering server certificate generation, client setup, and encrypted delivery across untrusted networks

Administration · Generated June 11, 2026 · [logzilla.ai/docs/administration/using-tls-tunnels](https://logzilla.ai/docs/administration/using-tls-tunnels)

TLS (Transport Layer Security) provides encrypted communication channels for syslog data transmission. LogZilla supports TLS encryption for secure log transport across untrusted networks, ensuring data confidentiality and integrity during transmission.

## TLS Overview

TLS encryption protects syslog data by:

- **Encrypting data in transit** between clients and LogZilla server
- **Authenticating endpoints** using digital certificates
- **Ensuring data integrity** through cryptographic verification
- **Preventing eavesdropping** on sensitive log information

## Server Configuration

### Certificate Generation

Generate TLS certificates for the LogZilla server. The Common Name must match the server's hostname or IP address that clients will use to connect.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out tls.crt
```

Provide accurate certificate information when prompted:

```
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: California
Locality Name (eg, city) []: San Francisco
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Company Name
Organizational Unit Name (eg, section) []: IT Department
Common Name (e.g. server FQDN or name) []: logzilla.company.com
Email Address []: admin@company.com
```

**Important:** The Common Name field must exactly match the hostname or IP address that clients use to connect to the LogZilla server.

### Certificate Installation

Copy the generated certificates to the LogZilla syslog-ng directory:

```
cp tls.key tls.crt /etc/logzilla/syslog-ng
```

Set appropriate file permissions for security:

```
chmod 600 /etc/logzilla/syslog-ng/tls.key
chmod 644 /etc/logzilla/syslog-ng/tls.crt
```

## Certificate File Locations

Purpose	Path	Permissions
Private Key	/etc/logzilla/syslog-ng/tls.key	600
Certificate	/etc/logzilla/syslog-ng/tls.crt	644

### Configuring *syslog-ng*

By default, LogZilla syslog TLS is disabled (which is when `SYSLOG_TLS_PORT` is set to 0). The port can be changed (for example, the customary port is 6514) with the following command:

```
logzilla config SYSLOG_TLS_PORT 6514
```

Then the LogZilla syslog module must be restarted:

```
logzilla restart -c syslog
```

To check if TLS support is working, use the `openssl` command as shown below. Replace `11.22.33.44:6514` with the LogZilla server address and TLS port.

```
openssl s_client -connect 11.22.33.44:6514 < /dev/null
```

If the output shows identification information (C, ST, L, O, etc.), certificate details from the `tls.crt` file, and TLS cipher and key specifications in use, then TLS support is operational.

If an error occurs, verify the steps from the start of this document and restart if necessary:

## Adding Key Files to Client Systems

On the syslog-sending system, create a new directory:

```
mkdir -p /etc/syslog-ng/ssl
```

Transfer the key and certificate files created earlier on the **LogZilla Server** to the **Client** system, placing them in the `/etc/syslog-ng/ssl` directory. You can use `scp` or a similar method.

## Configuring *syslog-ng* on the Client

There are two scenarios:

A local LogZilla instance forwards events to another LogZilla instance.

A standalone `syslog-ng` on the client server forwards events to a LogZilla instance.

### Forwarding Events from One LogZilla Instance to Another

Replace `LZ_SERVER` below with the DNS Name or IP Address of the LogZilla Server. Change the port number accordingly if a different port number was configured at the receiving site. In the `log{}` section, update the `source` according to the sources configured in the `/etc/syslog-ng/syslog-ng.conf` file.

Create a new file named `/etc/syslog-ng/conf.d/tls_to_LogZilla.conf` and put the following content into it:

```
destination d_tls {
  syslog-ng(
    server("LZ_SERVER")
    port(6514)
    transport(tls)
    tls(ca-file("/etc/syslog-ng/ssl/tls.crt"))
  );
};

log {
  source(s_src);
  destination(d_tls);
};
```

Restart `syslog-ng` on the Client system:

```
service syslog-ng restart
```

### Checking configuration

Check the LogZilla server to verify that events are now being received from this Client.

If issues occur, refer to the [Syslog Troubleshooting](https://www.logzilla.ai/docs/administration/syslog-troubleshooting) (<https://www.logzilla.ai/docs/administration/syslog-troubleshooting>) section.

## Advanced server configuration

For more than a single source port with TLS transport, TLS can be added to any syslog source by directly editing the `/etc/logzilla/syslog-ng/config.yaml` file. Find the `sources` array element and for any source, add

`transport: tls` and then `tls_key_file` and `tls_cert_file` options. For example, to enable TLS transport for JSON input, add this:

```
- name: json-tls
  enabled: True
  type: network
  transport: tls
  port: 6515
  tls_cert_file: "/etc/logzilla/syslog-ng/tls.crt"
  tls_key_file: "/etc/logzilla/syslog-ng/key.crt"
  flags:
    - no-parse
  program_override: _JSON
```

After any change to this configuration file, the LogZilla syslog module must be restarted:

```
logzilla restart -c syslog
```