LOGZILLA DOCUMENTATION

Network Communications

Network protocols, ports, and transports used by LogZilla for syslog ingest, raw data listeners, HTTP receivers, and management endpoints

Administration · Generated April 29, 2026 · logzilla.ai/docs/administration/network-communications

LogZilla supports multiple network communication protocols and ports to accommodate diverse logging environments. The platform receives data through standard syslog protocols, raw data formats, and HTTP-based interfaces.

Syslog Communication

LogZilla receives syslog data using industry-standard protocols and formats:

RFC 3164 (BSD Syslog)

- **Default Port**: 514
- **Protocols**: TCP and UDP
- **Format**: Traditional BSD syslog format
- **Use Case**: Legacy devices and standard syslog implementations

RFC 5424 (Structured Syslog)

- **Default Port**: 601
- **Protocol**: TCP only
- **Format**: Modern structured syslog with enhanced metadata
- **Use Case**: Applications requiring structured data fields

Raw Data Communication

LogZilla accepts non-syslog data formats for specialized use cases:

Text Data

- **Default Port**: 516
- **Protocols**: TCP and UDP
- **Format**: Plain text messages
- **Use Case**: Devices sending non-standard or malformed syslog data

JSON Data

- **Default Port**: 515
- **Protocol**: TCP only
- **Format**: JSON-formatted messages
- **Use Case**: Applications sending structured JSON logs

Note: Raw data requires LogZilla apps or parsing rules to interpret and process the incoming messages effectively.

HTTP/HTTPS Communication

Web Interface

- **HTTP Port**: 80
- **HTTPS Port**: 443
- **Purpose**: User interface access and API endpoints

HTTP Log Reception

The same HTTP/HTTPS ports support log data ingestion. For detailed configuration, refer to the HTTP Event Receiver (https://www.logzilla.ai/docs/receiving-data/http-event-receiver) documentation.

Port Configuration

Network ports can be customized using the `logzilla config` command:

```
logzilla config SYSLOG_RAW_PORT 516
```

Available Configuration Options

Configuration Option	Default	Description
SYSLOG_BSD_TCP_PORT	514	TCP port for RFC 3164/BSD syslog messages
SYSLOG_BSD_UDP_PORT	514	UDP port for RFC 3164/BSD syslog messages
SYSLOG_RFC5424_PORT	601	TCP port for RFC 5424 syslog messages
SYSLOG_JSON_PORT	515	TCP port for raw JSON messages
SYSLOG_RAW_PORT	516	TCP port for raw text messages
SYSLOG_RAW_UDP_PORT	516	UDP port for raw text messages

Network Security Considerations

Firewall Configuration

Ensure appropriate firewall rules allow traffic on configured ports:

- Standard syslog ports (514, 601) for log reception
- HTTP/HTTPS ports (80, 443) for web interface access
- Custom ports if non-default configurations are used

Protocol Selection

- **Use TCP** for reliable delivery and flow control
- **Use UDP** for high-volume environments where occasional loss is acceptable
- **Use HTTPS** for encrypted web interface access in production

Access Control

- Restrict syslog port access to authorized log sources
- Implement network segmentation for sensitive logging infrastructure
- Monitor unusual traffic patterns on logging ports

Performance Optimization

High-Volume Environments

- Use TCP for better flow control during traffic bursts
- Monitor queue depths and connection counts
- Configure syslog receivers, batching, and buffering (see Server Settings and Syslog Settings).

Network Bandwidth

- Consider log compression for high-volume remote sources
- Implement log filtering at the source to reduce network traffic
- Use structured formats (RFC 5424, JSON) for more efficient parsing

Troubleshooting Network Issues

Connection Problems

- Verify firewall rules allow traffic on configured ports
- Check network connectivity between sources and LogZilla server
- Confirm port configurations match between senders and receivers

Performance Issues

- Monitor network utilization during peak logging periods
- Check for packet loss on UDP connections
- Verify adequate bandwidth for expected log volume

Configuration Validation

- Test port changes in staging environments first
- Verify configuration changes take effect after service restart
- Monitor logs for connection errors after configuration changes