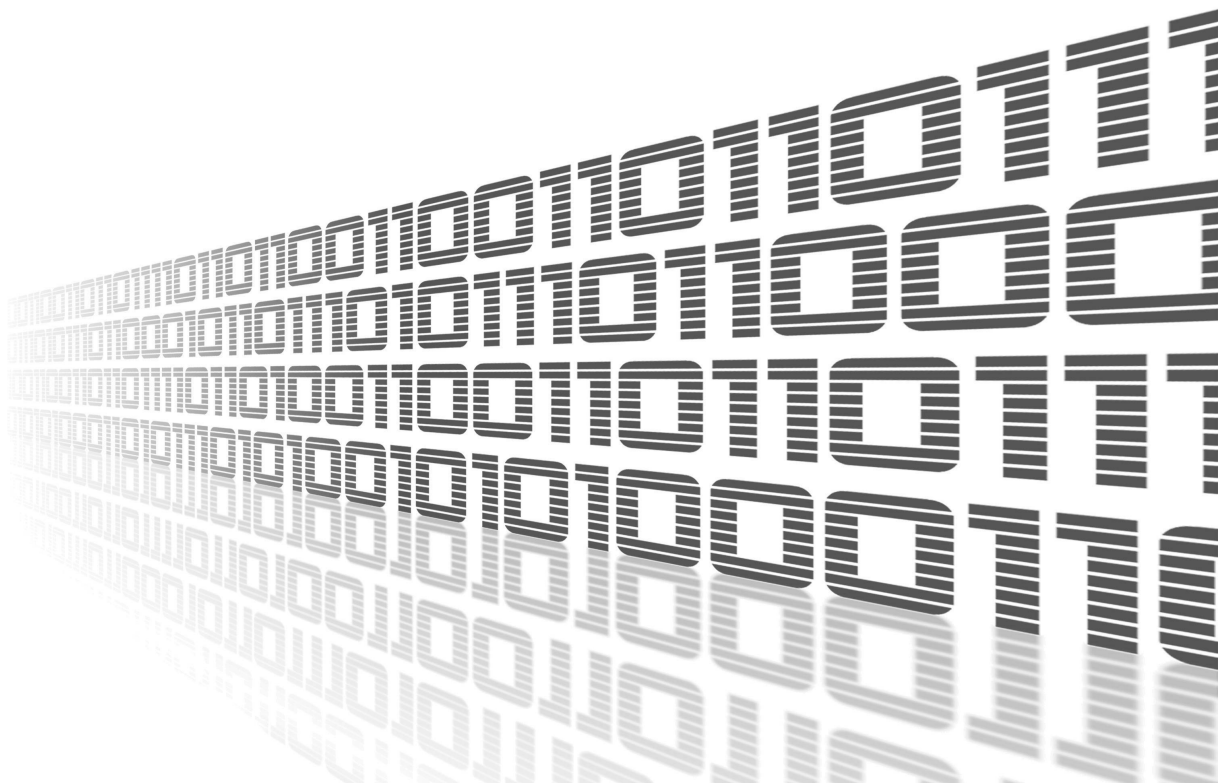




# Secure Syslog

APPLICATION NOTE



## Used symbols



*Danger* – Information regarding user safety or potential damage to the router.



*Attention* – Problems that may arise in specific situations.



*Information or notice* – Useful tips or information of special interest.



*Example* – example of function, command or script.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Web Interface</b>	<b>2</b>
2.1	Configuration . . . . .	3
2.1.1	Global . . . . .	3
2.2	Integration with local syslog service . . . . .	5
2.3	Integration with Graylog server . . . . .	6
<b>3</b>	<b>Troubleshooting</b>	<b>7</b>
<b>4</b>	<b>Licenses</b>	<b>8</b>
<b>5</b>	<b>Related Documents</b>	<b>9</b>

# List of Figures

1	Menu . . . . .	2
2	Configuration . . . . .	3
3	Syslog configuration . . . . .	5
4	Graylog message . . . . .	6
5	Licenses . . . . .	8

# 1. Introduction



Router app *Secure Syslog* is not contained in the standard router firmware. Uploading of this router app is described in the Configuration manual (see Chapter [Related Documents](#)).

As described in the Remote Monitoring Guide [1], the System Logging (syslog) protocol is used to send router event information to a specific server, such as Graglog <sup>1</sup> or PRTG Network Monitor <sup>2</sup>. The default syslog service provided by router firmware supports the UDP transport protocol only, which may be used in secure private networks only.

This module implements an enhanced syslog client (sender) that can forward syslog messages to a server (receiver) over a secure TLS protocol as defined in RFC 5425. Such well authenticated and encrypted communication may be transmitted over a public internet. The insecure, plain UDP and TCP transport protocols are supported too, but not recommended.

---

<sup>1</sup><https://www.graylog.org>

<sup>2</sup><https://www.paessler.com/prtg>

## 2. Web Interface

Once the installation of the module is complete, the module's GUI can be invoked by clicking the module name on the Router apps page of router's web interface.

Left part of this GUI contains menu with Configuration menu section and Information menu section. Customization menu section contains only the Return item, which switches back from the module's web page to the router's web configuration pages. The main menu of module's GUI is shown on Figure 2.

<b>Configuration</b>
Global
<b>Information</b>
Status
Licenses
<b>Customization</b>
Return

Figure 1: Menu

## 2.1 Configuration

### 2.1.1 Global

All Secure Syslog router app settings can be configured by clicking on the *Global* item in the main menu of module web interface. An overview of configurable items is given below.

**Secure Syslog Configuration**

Enable

Read Kernel Log

---

Listen for UDP

Local Port

---

Remote IP Address

Remote Port

Protocol

---

Authentication

Acceptable Peers

CA Certificates 

```
-----BEGIN CERTIFICATE-----
MIIFSTCCAzGgAwIBAgIUURSTXXU4hyWq0pWp8S+YKXxHGcD4wDQYJKoZIhvcNAQEL
BQAwUzELMAkGA1UEBhMCREUxETAPBgNVBAoMCE9wZW5YUETJMQwwCgYDVQQQLDANQ
```

Local Certificate \* 

```
-----BEGIN CERTIFICATE-----
MIIGdzCCBF+gAwIBAgIKD/+CIQqmi67M8DANBgkqhkiG9w0BAQsFADBTMQswCQYD
VQQGEwJERTERMA8GA1UECgwIT3BlblhQS0kxDDAKBgNVBAsMA1BLSTEjMCEGA1UE
```

Local Private Key \* 

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBkwggSlAgEAAoIBAQDiuKxzIORIXySF
K36HOMUtynIZPJW84dFULxe0dFYl78AQkL0cK63cJ7Y5yNRQFEHFIRcNY68dC4zo
```

\* can be blank

Figure 2: Configuration

Item	Description
Enable	Enables Secure Syslog functionality.
Read Kernel Log	Retrieve new log messages from the /dev/kmsg. Check this if you want to forward also kernel messages, such as information about device mounting or messages from the fire-wall LOG target. After service (re)start all existing kernel log entries be sent to the remote server, so the server may receive duplicate messages. Then, the system will await new messages.

Continued on the next page

Continued from previous page

Item	Description
Listen for UDP	Listen for syslog messages incoming via the UDP protocol. The messages can be sent by the local syslog service (see Section 2) and/or by any remote system. After service (re)start the system immediately starts listening for new messages. Prior syslog communication will not be distributed.
Local Port	UDP port where to listen for the incoming syslog messages. The common port number is 514.
Remote IP Address	Forward any message to this IP address.
Remote Port	Forward to this port, e.g. 514.
Protocol	Forward using this protocol. Allowed values are: <ul style="list-style-type: none"> <li>• <b>UDP</b></li> <li>• <b>TCP</b></li> <li>• <b>SSL/TLS</b></li> </ul>
Authentication	How to authenticate the syslog server, when using the SSL/TLS protocol. Allowed values are: <ul style="list-style-type: none"> <li>• <b>None (encryption only)</b> to skip transport receiver authentication. The communication will still be encrypted.</li> <li>• <b>Certificate fingerprint</b> to check fingerprint of the received certificate against the Acceptable Peers.</li> <li>• <b>Certificate validity</b> to accept any server with a valid certificate, signed by the specified CA.</li> <li>• <b>Certified peer name</b> to check certificate validity and then match the certified DNS names in the subjectAltName extension, or the entire certified Common Name against the Acceptable Peers.</li> </ul> <p>Note the server may (depending on its configuration) implement own transport sender authentication, which is independent of this setting.</p>

Continued on the next page

Continued from previous page

Item	Description
Acceptable Peers	Accepted certificate fingerprint (SHA1) or DNS/Common Name of the remote peer. The DNS name may use wild-cards, e.g. „*.example.net“. Required when Authentication is set to Certificate fingerprint or Certified peer name.
CA Certificates	The entire certificate chain (sequence of CA certificates in PEM format) that can validate the remote certificates. Not required when Authentication is set to None.
Local Certificate	Certificate in PEM format. Extended key usage shall permit use for TLS client authentication!
Local Private Key	The local key and certificate don't need to be configured when the server does not enforce transport sender authentication.

Table 1: Configuration items description

## 2.2 Integration with local syslog service

To receive syslog messages from the local syslog service, set *Remote IP Address* in the Syslog service configuration to 127.0.0.1, which will forward the syslog traffic to the Secure Syslog module. The *Remote UDP Port* shall match the *Local Port* discussed above.

Syslog Configuration	
Log Size	<input type="text" value="1000"/> lines
Remote IP Address	<input type="text" value="127.0.0.1"/>
Remote UDP Port	<input type="text" value="514"/>
<input type="button" value="Apply"/>	

Figure 3: Syslog configuration



## 2.3 Integration with Graylog server

First, install the Graylog server, either download the Open Source Edition<sup>1</sup> or purchase the Enterprise Edition. You may, for example, download the OVA image and then import the appliance to your virtual environment.

Run the imported appliance. Once first started, the console will display a Web login and Shell login information (username:password). Write down these information as they will not be displayed again.

```
Open http://192.168.88.79 in your browser to access Graylog.
Write down the following passwords, they appear only once after the first boot.
Web login: admin:pmttJK3z
Shell login: ubuntu:ubuntu
graylog login:
```

Figure 4: Graylog message

Use these information to login to the Graylog admin. In the menu select System – Inputs, then Select input „Syslog TCP“ and click Launch new input. A configuration dialog will appear:

- Give the input some name.
- Set a Port number, e.g. 1514 (in the default configuration the number must be > 1024).
- Enable TLS.
- Optionally, set a full path to a *TLS cert file* and *private key file*. Place the .crt and .key file on the Graylog server in `/etc/graylog/server/ssh`.
- Optionally, set *TLS client authentication* to “optional” or “required”. When set, you have to define also a full path to a directory with *TLS Client Auth Trusted Certs*. Place your CA certificates(s) to the defined directory, e.g. `/etc/graylog/server/ssh/cacerts`.

Once the input is created, it shall display as RUNNING and the received data shall start appearing under Streams – All Messages.



Verify in the *Time configuration* under *System – Overview* that the current time (clock) of your routers match the clock of the Graylog server. Messages may get lost if the clock don't match.

<sup>1</sup><https://www.graylog.org/products/open-source>

## 3. Troubleshooting

Generic tlsv1 alert internal errors (see below) reported in router System Log can be caused by server-initiated session termination. Set the server log level to Debug and inspect the server-side log for more details. Often the Local Certificate is missing or is not permitted to perform the TLS client authentication.

```
rsyslogd: SSL\_ERROR\_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib  
(0):func(0):reason(1)(1)' with ret=0 [v8.2010.0]  
rsyslogd: OpenSSL Error Stack: error:14094438:SSL routines:ssl3\_read\_bytes:tlsv1  
alert internal error [v8.2010.0]
```

## 4. Licenses

Summarizes Open-Source Software (OSS) licenses used by this module.

Secure Syslog Licenses		
Project	License	More Information
rsyslog	GPL 3.0+	<a href="#">License</a>
libestr	LGPL 2.1+	<a href="#">License</a>
libfastjson	MIT	<a href="#">License</a>
openssl	OpenSSL	<a href="#">License</a>
zlib	zlib	<a href="#">License</a>

Figure 5: Licenses

## 5. Related Documents

[1] Advantech Czech: **Remote Monitoring Guide** (APP-0091-EN)

You can obtain product-related documents on *Engineering Portal* at [icr.advantech.cz](http://icr.advantech.cz) address.

To get your router's *Quick Start Guide*, *User Manual*, *Configuration Manual*, or *Firmware* go to the [Router Models](#) page, find the required model, and switch to the *Manuals* or *Firmware* tab, respectively.

The *Router Apps* installation packages and manuals are available on the [Router Apps](#) page.

For the *Development Documents*, go to the [DevZone](#) page.