

# SyslogCollector

IEC 61131 Library for ACSELERATOR RTAC® Projects

SEL Automation Controllers

# Table of Contents

<b>Section 1: SyslogCollector</b>	
Introduction .....	3
Supported Firmware Versions .....	3
Structures .....	3
Enumerations .....	4
Function Blocks .....	5
Examples .....	6
Release Notes .....	9

---

---

## RTAC LIBRARY

---

---

# SyslogCollector

## Introduction

---

This library allows the RTAC to receive syslog messages from other devices. Once the RTAC receives a syslog message, the contents of the message are available to the IEC 61131 logic engine. Logic can be performed on the syslog messages to accomplish the following:

- ▶ Store syslog messages into the SOE log of the RTAC.
- ▶ Create a custom syslog file with the FileIO library.
- ▶ Map syslog data into protocol servers.
- ▶ Display syslog messages on RTAC HMI screens.
- ▶ Generate an email or text message.
- ▶ Generate syslog messages based on received syslog messages with modified content.

The syslog message is presented to the logic engine as a string data type. Anything that can be done with a string in the logic engine can be done with the received syslog message.

This library offers the ability to filter received syslog messages based on its origin IP address. It also allows for automatically logging the received syslog messages into the RTAC SOE.

## Supported Firmware Versions

---

You can use this library on any device configured using ACSELERATOR RTAC® SEL-5033 Software with firmware version R143 or higher.

## Structures

---

Structures provide a means to group together several memory locations (variables), making them easier to manage.

## struct\_syslogMessageFormat

Name	IEC 61131 Type	Description
ReceivedIPAddress	String(15)	IP address from which the syslog message was received.
FacilityLevel	enum_facility	The facility level of the syslog message.
SeverityLevel	enum_severity	The severity level of the syslog message.
SyslogMessage	STRING(2000)	The content of syslog message.

## Enumerations

Enumerations make code more readable by allowing a specific number to have a readable textual equivalent.

### enum\_severity

This enumeration lists the different severity levels allowed in syslog.

Enumeration	Value	Description
Emergency	0	System is unusable
Alert	1	Action must be taken immediately
Critical	2	Critical conditions
Error	3	Error conditions
Warning	4	Warning conditions
Notice	5	Normal but significant conditions
Informational	6	Informational messages
Debug	7	Debug-level messages
None	8	No severity selected

### enum\_facility

This enumeration lists the different facility levels allowed in syslog.

Enumeration	Value	Description
kern	0	Kernel messages
user	1	User-level messages
mail	2	Mail system
daemon	3	System daemons
auth	4	Security/authorization messages
syslog	5	Messages generated internally by syslogd
lpr	6	Line printer subsystem

Enumeration	Value	Description
news	7	Network news subsystem
uucp	8	UUCP subsystem
clock	9	Clock daemon
authpriv	10	Security/authorization messages
ftp	11	FTP daemon
NTP	12	NTP subsystem
logAudit	13	Log audit
logAlert	14	Log alert
cron	15	Scheduling daemon
local0	16	Local use 0
local1	17	Local use 1
local2	18	Local use 2
local3	19	Local use 3
local4	20	Local use 4
local5	21	Local use 5
local6	22	Local use 6
local7	23	Local use 7
None	24	No facility selected

## Function Blocks

### fb\_syslogCollector (Function Block)

This function block makes syslog messages that were received on one of the IP addresses of the RTAC available to the IEC 61131 logic engine.

#### Inputs

Name	IEC 61131 Type	Description
LocalIPAddress	STRING(15)	Specify an RTAC IP address on which to listen. Default is 0.0.0.0, which listens on all interfaces.
LocalPortNumber	UINT	Defaults to 514, which is the standard syslog port.
LogReceivedSyslog	BOOL	If TRUE, received syslog data will be entered into the RTAC SOE log.
FilterOnSeverity	enum_Severity	If set to a value other than NONE, the RTAC will only log syslog messages that have a severity of NONE or higher. Default value is NONE.
UseSeverityInSyslogMessage	enum_Severity	If set to a value other than NONE, received syslog messages will use this severity when logged. If set to NONE, logged syslog messages will use the severity received in message. Default value is NONE.

## Inputs

Name	IEC 61131 Type	Description
IPAddressFilterList	STRING(1600)	Enter a comma-separated list of IP addresses for the RTAC to process syslog messages from. If left empty, the RTAC processes all received syslog messages.

## Outputs

Name	IEC 61131 Type	Description
RecSyslogMessage	ARRAY[1..50] OF struct_SyslogMessageFormat	Received syslog messages.
InvalidInputPin	STRING	Lists an incorrectly configured input pin.

## Processing

- This function block will log received syslog messages in the RTAC SOE if the LogReceivedSyslog input is set to TRUE. If the syslog message is longer than 255 characters, the logged message will be truncated and MessageTruncated will be appended to the end of the SOE message.
- This function block filters received syslog messages based upon the originating IP address. These addresses can be entered into the IPAddressFilterList input. If this value is left empty or set to 0.0.0.0 (which is the default setting), the function block will process all received syslog messages.
- This function block will process as many as 50 received syslog messages per processing cycle. If the RTAC receives more than 50 syslog messages in a single processing cycle, the excess messages will be buffered and processed in a subsequent processing interval. The function block displays processed messages for a single processor cycle.
- By default, Port 514 is used to listen for syslog messages. This can be changed by configuring the LocalPortNumber input to a desired port to listen for syslog messages.
- This function block only processes UDP-based syslog messages. No TCP syslog messages are processed with this function block.
- This function block must be used in conjunction with an Ethernet listening UDP incoming access point that matches the LocalPortNumber input. Unless the input pin is configured to a nondefault value, this port must be 514 on the Ethernet listening UDP incoming access point.

## Examples

*These examples demonstrate the capabilities of this library. Do not mistake them as suggestions or recommendations from SEL.*

*Implement the best practices of your organization when using these libraries. As the user of this library, you are responsible for ensuring correct implementation and verifying that the project using these libraries performs as expected.*

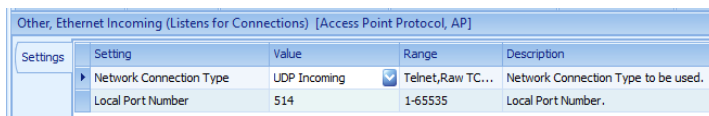
# Receiving Syslog Messages

## Objective

A user would like to collect all syslog messages from other devices in their substation network.

## Assumptions

A UDP incoming access point needs to be included in the project configuration. The Local Port Number setting input of the port must match the LocalPortNumber setting on the syslog function block, as shown in *Figure 1* and *Code Snippet 1*.



Setting	Value	Range	Description
Network Connection Type	UDP Incoming	Telnet,Raw TC...	Network Connection Type to be used.
Local Port Number	514	1-65535	Local Port Number.

**Figure 1 UDP Incoming Access Point**

## Solution

The syslog function block can be used as shown in *Code Snippet 1*. This example shows the function block processing all received syslog messages on a specified interface (by entering the IP address used on that interface). This example also shows the function block storing all received messages with their received severity levels into the SOE log of the RTAC.

### Code Snippet 1 prg\_SyslogCollector

```
PROGRAM prg_SyslogRec
VAR
_syslogCollector : fb_SyslogCollector;
END_VAR

_syslogCollector(LocalIPAddress := '192.168.1.2',
LocalPortNumber := 514,
LogReceivedSyslog := TRUE,
FilterOnSeverity := SyslogCollector.enum_severity.None,
UseSeverityInSyslogMessage := SyslogCollector.enum_severity.None,
IPAddressFilterList := '');
```

*Figure 2* shows the same program but in a CFC program.

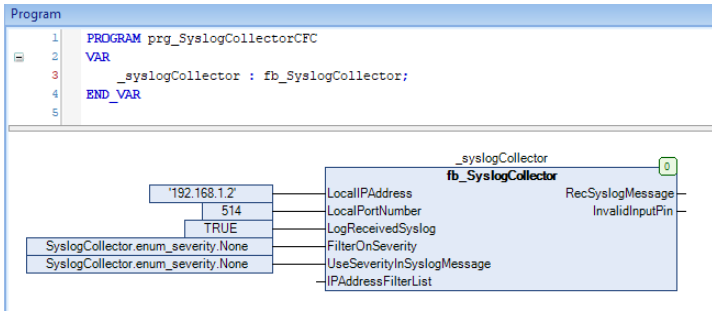


Figure 2 prg\_SyslogCollector in CFC Form



# Release Notes

---

Version	Summary of Revisions	Date Code
3.5.0.0	► Initial release.	20180928