



Syslog Technology Reference Manual



IMPORTANT: This manual links to Syslog Status Messages Reference Data, publication [SYSLOG-RD001](#). Download the spreadsheets and PDF files now for offline access.

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT: Identifies information that is critical for successful application and understanding of the product.

These labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

The following icon may appear in the text of this document.



Identifies information that is useful and can help to make a process easier to do or easier to understand.

Rockwell Automation recognizes that some of the terms that are currently used in our industry and in this publication are not in alignment with the movement toward inclusive language in technology. We are proactively collaborating with industry peers to find alternatives to such terms and making changes to our products and content. Please excuse the use of such terms in our content while we implement these changes.

Syslog Technology	5
Configure Syslog Routing in FactoryTalk Policy Manager.....	5
Syslog Routing Settings.....	6
Understanding Event Messages.....	8
Syslog Facility Values and Severity Values.....	9
Syslog Event Facility Values.....	9
Syslog Severity Values.....	10

Preface

This manual provides reference for the Rockwell Automation implementation of the Syslog protocol and its functions.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation. You can view or download publications at rok.auto/literature.

Resource	Description
Syslog Status Messages Reference Data, SYSLOG-RD001 on page	Provides parameters and event codes for products utilizing the Syslog protocol.
System Security Design Guidelines Reference Manual, publication SECURE-RM001	Describes guidelines for how to use Rockwell Automation® products to improve the security of your industrial automation system.
System Security User Manual, SECURE-UM001	This manual describes the system-level configuration requirements to use devices that have achieved IEC 62443 certifications.

Syslog Technology

Syslog is a standardized and widely used event message logging technology. Syslog is used to generate, store, report, and analyze security-related events.

When Syslog operates over a network, it uses a client-server architecture in which a syslog server monitors for, and logs, messages that are coming from clients.

The following products support Syslog:

- FactoryTalk® Linx software, version 6.21 or later
- ControlLogix® 5580 controllers, firmware revision 34.011 or later
- ControlLogix® 5590 controllers, firmware revision 38.011 or later
- GuardLogix® 5580 controllers, firmware revision 34.011 or later
- 1756-EN4TR EtherNet/IP™ communication module, firmware revision 4.001 or later
- 1783-CSP CIP Security™ Proxy, firmware revision 1.001 or later
- PowerFlex® 755T drives, firmware revision 10.001 or later
- PowerFlex® 6000T drives, firmware revision 10.001 or later

IMPORTANT:

CIP Security™-capable devices are Syslog-capable. To enable and configure Syslog in certified security applications, you must implement CIP Security™.

However, Syslog is not exclusive to industrial automation control systems that use CIP Security™.

You can also use Syslog in applications that aren't certified security applications, and with CIP Security™-capable devices when CIP Security™ is not enabled on the devices.

For more information on Syslog, see Syslog Status Messages Reference Data, publication [SYSLOG-RD001](#).

Syslog Collector

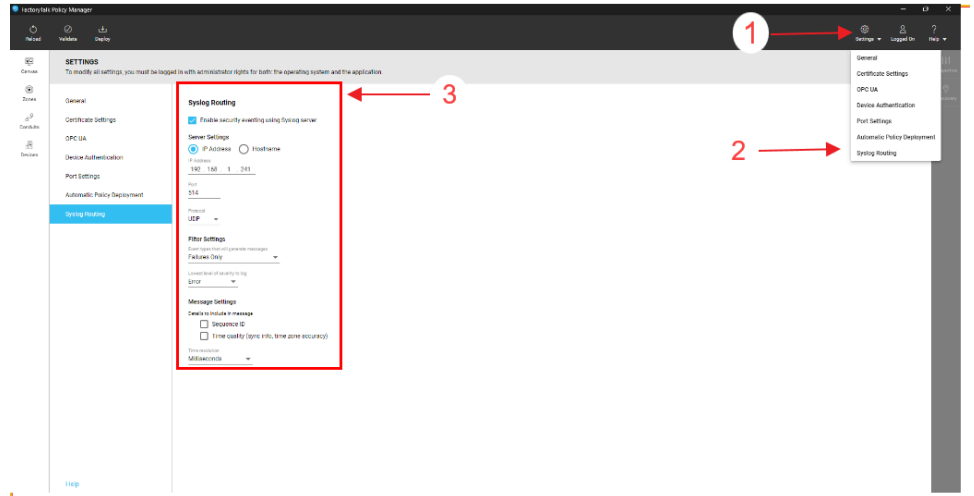
A Syslog collector stores event messages that are sent from the generating device to the collector.

When you choose a Syslog collector tool, it must support the following:

- RFC-5424 Syslog protocol
- Ability to receive messages from CIP Security™-enabled devices

Configure Syslog Routing in FactoryTalk Policy Manager

1. Select Settings.
2. Select Syslog Routing.
3. Configure the routing rules under Syslog Routing.



Syslog Routing Settings

Below are settings for enabling and configuring Syslog in FactoryTalk® Policy Manager.

Syslog Routing

Table 1. Syslog Routing Settings

Property	Description
Enable Syslog routing using Syslog server	Enables devices that support Syslog routing to start sending Syslog messages as configured in the policy. These settings apply to all devices that support Syslog routing.

Table 2. Syslog Server Settings

Use these settings to identify the location of the Syslog server.

Property	Description
IP address	Identifies the Syslog server by the IP address.
Hostname	Identifies the Syslog server by the DNS host name.
Port	Identifies the communications port on the server to receive the Syslog messages. Default port number is 514.
Protocol	Configures logging. <ul style="list-style-type: none"> • Select UDP for low-priority logging. UDP is not a guaranteed reliability protocol, log data that is transferred using UDP can be lost in transit due to various network problems. • Select TCP for log data that cannot tolerate loss and which must be retained.

Table 3. Filter Settings
Use these settings to filter the event messages that are logged to the Syslog server.

Property	Description
<p>Event types that will generate messages</p>	<p>Used to determine which event types generate messages.</p> <p>Failures only</p> <p>Logs events upon failures related to model deployment, device discovery, component connections, and component authentications or authentications.</p> <p>Failures and successes</p> <p>Logs all success and failure events related to model deployment, device discovery, component connections, and component authentications or authorizations.</p>
<p>Lowest level of severity to log</p>	<p>Logs messages that are greater than or equal to the severity level selected. Defined severity levels from highest to lowest are:</p> <p>Emergency</p> <p>System is unusable.</p> <p>Alert</p> <p>Action must be taken immediately.</p> <p>Critical</p> <p>Critical operational conditions such as device hardware major faults.</p> <p>Error</p> <p>Error conditions in software applications and device hardware minor faults.</p> <p>Warning</p> <p>Warning conditions in software applications and hardware.</p> <p>Notice</p> <p>Significant conditions that may require special handling.</p> <p>Information</p> <p>Informational messages about software or hardware operations.</p> <p>Audit</p> <p>Messages from the auditing service.</p> <p>Debug</p>

Table 3. Filter Settings
Use these settings to filter the event messages that are logged to the Syslog server.

(continued)

Property	Description
	Messages about the programmatic operations of the software.

Table 4. Message Settings

Property	Description
Details to include in message	<p>Specifies details included in the message.</p> <p>Sequence ID</p> <p>Uniquely identify the type and purpose of the message so that the receiver can detect lost messages and order messages correctly.</p> <p>Time quality (sync info, time zone accuracy)</p> <p>Describes the system time mechanism used by the message originator.</p>
Time resolutions	<p>Defines the level of precision used in the time stamp of the log messages:</p> <ul style="list-style-type: none"> • Seconds • Milliseconds • Microseconds • Nanoseconds

Understanding Event Messages

Syslog event messages fall within groups as listed and defined in the table below.

Additional information for specific event messages is located in [SYSLOG-RD001](#).

Event Message Group	Definition
Auth	An account management-related event
Backup	A general backup or restore related event
CIP Sec	A CIP Security™-related event
Config	A general configuration-related event
Ctlr	A programmable automation controller related event
Discovery	A system discovery-related event
Log	A log-related event

Event Message Group	Definition
Safety	A CIP Safety™-related event
Sys	A general system-related event
HTTP	A web server or client-related event
CIP	A CIP™-related event

Syslog Facility Values and Severity Values

When detected, each message is labeled with a facility code and is assigned a severity level.

Syslog Event Facility Values

Table 5. Syslog Event Facility Values

Value	ID	Facility	Description
null	0	local0(16)	For future use, no events belong to this category
comms	1	local0(16)	A general communications-related event
config	2	local0(16)	A general configuration-related event
diag	3	syslog(5)	A general fault or error diagnostic
stat	4	local0(16)	A general event providing statistical data
alert	5	syslog(5)	A general event related to a potential threat
control	6	local0(16)	A general control system-related event
audit	7	local0(16)	A general audit log related event
backup	8	local0(16)	A general backup or restore related event
security	9	auth(4)	A general security-related event
cip	10	local0(16)	ACIP™-related event
http	11	local0(16)	A web server or client-related event
OPC	12	local0(16)	An OPC or OPC UA related event
log	13	local0(16)	A log-related event
cert	14	local0(16)	A certificate-related event
discovery	15	local0(16)	A system discovery-related event
auth	16	auth(4)	An account management-related event

Table 5. Syslog Event Facility Values (continued)

Value	ID	Facility	Description
sys	17	local7(23)	A general system-related event
cipsec	18	auth(4)	A CIP Security™-related event
safety	31	local0(16)	A safety-related event
ctrl	32	local0(16)	A programmable automation controller related event

Syslog Severity Values

Events can have security risks that can take many forms, for example:

- Threat actors that try to gain unauthorized, and undetected, access to an IACS network with the intention to commit malicious acts.
- Well-intentioned personnel with no malicious intention but who make mistakes that can result in unintended consequences.

The severity values are defined in The Syslog Protocol, RFC 5424, standard.

Table 6. Syslog Event Security Risk Severity Values

Value	Severity Level		Description
emrg	0	Emergency	System is unusable
alrt	1	Alert	Should be corrected immediately
crit	2	Critical	Critical condition
err	3	Error	Error condition
warn	4	Warning	Error may occur if action is not taken
note	5	Notice	Events are unusual
info	6	Informational	Normal operations, no action required
audit	7	Audit	Information for the audit system
dbg	8	Debug	Information for developers

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Technical Documentation Center	Quickly access and download technical specifications, installation instructions, and user manuals.	rok.auto/techdocs
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Waste Electrical and Electronic Equipment (WEEE)







At the end of life, this equipment should be collected separately from any unsorted municipal waste.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Allen-Bradley, expanding human possibility, and Rockwell Automation are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

rockwellautomation.com — expanding **human possibility**[®]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908)838-800