Syslog Security Events

SCALANCE & RUGGEDCOM Network components

https://support.industry.siemens.com/cs/ww/en/view/109805218

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

© Siemens 2021 All rights reserved

Table of contents

© Siemens AG 2021 All rights reserved

© Siemens AG 2021 All rights reserved

1 Introduction

The purpose of this documentation is to provide a categorized list of the syslog security messages generated by the Siemens network components. In this version the messages created by the SCALANCE and RUGGEDCOM modules are listed.

Along with the message text of the events the following information is provided.

Facility

The source of the event. Options for the RUGGEDCOM devices include:

- (1) USER
- (3) DEAMON
- (4) AUTH
- (10) AUTHPRIV

The facility of the SCALANCE modules is set to

- (16) Local0.

Severity

The severity level associated with the event. Options include:

- (0) Emergency
- (2) Critical
- (3) Error
- (4) Warning
- (5) Notice
- (6) Info
- (7) Debug, Verbose

NOTE

The firmware of the SCALANCE modules supports the following three severity levels:

- Critical
- Warning
- Info

Events with the following severities will automatically be assigned to another severity as follows:

- Emergency is assigned to critical
- Error is assigned to warning
- Notice is assigned to info

The module will send the event with the newly assigned severity (critical, warning or info).

© Siemens AG 2021 All rights reserved

Event type

- Event

  Events are authorized activities that can be expected to occur during routine use.
- Alarm

  Alarms are activities that may indicate unauthorized activity.

Validity of this document

This document applies to the following software versions:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG firmware as of version 4.3
- SCALANCE XM-400/XR-500 firmware as of version 6.4
- SCALANCE M-800 firmware as of version 6.4
- SCALANCE S615 firmware as of version 6.4
- SCALANCE SC-600 firmware as of version 2.1
- SCALANCE W760/W720 firmware as of version 6.5
- SCALANCE W770/W730 firmware as of version 6.5
- SCALANCE W780/W740 firmware as of version 6.5
- SCALANCE W1780/W1740 firmware as of version 2.0
- RUGGEDCOM RX1400 firmware as of version 2.14

© Siemens AG 2021 All rights reserved

2 Events categories

2.1 Human user identification and authentication

2.1.1 Local successful logon

Description

Valid logon information that is specified during logon.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500

Table 2-1

Message text	{Local interface}: User {user name} logged in.
Example	Console: User admin logged in.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

© Siemens AG 2021 All rights reserved

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-2

Category	SE_LOCAL_SUCCESSFUL_LOGON
Message text	Ruggedcom confd[{pid}]: audit user: {user}/{user id} assigned to groups:{role}
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

Table 2-3

Category	SE_LOCAL_SUCCESSFUL_LOGON
Message text	Ruggedcom rmfmgr[{pid}]: username:{user name} usid:{user id} started {context} session from ip:127.0.0.1 sourceport:{src port} through {local interface} protocol
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

2.1.2 Default user authentication used

Description

User is logged in with default username and password.

This event might be a hint that the system configuration was not changed from the default setup.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500

Table 2-4

Message text	{Local interface}: Default user {user name} logged in.
Example	Console: Default user admin logged in.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

© Siemens AG 2021 All rights reserved

2.1.3 Local unsuccessful logon

Description

Incorrect username or password specified during logon.

If this happens quite often, it might indicate an automated password guessing attack.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500

Table 2-5

Message text	{Local interface}: User {user name} failed to log in.
Example	Console: User admin failed to log in.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Invalid username

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-6

Category	SE_LOCAL_UNSUCCESSFUL_LOGON
Message text	audit user: {username}1/0 no such local user
Facility	LOG_AUTHPRIV

Category	SE_LOCAL_UNSUCCESSFUL_LOGON
Severity	Info
Event type	Event
Log	Auth.log

Table 2-7

Category	SE_LOCAL_UNSUCCESSFUL_LOGON
Message text	login failed, reason='No such local user', user='{username}', context='{context}', proto='{local interface}',user ipaddr='127.0.0.1'
Facility	LOG_AUTHPRIV
Severity	Error
Event type	Event
Log	Auth.log

Invalid password

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-8

Category	SE_LOCAL_UNSUCCESSFUL_LOGON
Message text	audit user: {username}/0 Provided bad password
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

Table 2-9

Category	SE_LOCAL_UNSUCCESSFUL_LOGON
Message text	login failed, reason='Bad password', user='{username}', context='{context}', proto='{protocol}', user ipaddr='127.0.0.1''
Facility	LOG_AUTHPRIV
Severity	Error
Event type	Event
Log	Auth.log

2.1.4 Logout

Description

User session ended - logged out.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500

© Siemens AG 2021 All rights reserved

Table 2-10

Message text	{Local interface}: User {user name} logged out.
Example	Console: User admin logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

The following message appears for the module:

- RUGGEDCOM RX1400

Table 2-11

Category	SE_LOGOFF
Message text	audit user: {username}/0 logged in over {protocol} from {source ip-address} with authmeth: {authenticationmethod}
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

© Siemens AG 2021 All rights reserved

2.1.5 Network successful login

Description

Valid login information that is specified during remote login.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-12

Message text	{Protocol}: User {User name} has logged in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has logged in from 192.168.0.1.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-13

Category	SE_NETWORK_SUCCESSFUL_LOGON
Message text	audit user: {username}/0 logged in over {protocol} from {source ip-address} with authmeth: {authenticationmethod}
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

Table 2-14

Category	SE_NETWORK_SUCCESSFUL_LOGON
Message text	audit user: admin/ {user id} assigned to groups: {role}
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

© Siemens AG 2021 All rights reserved

Table 2-15

Category	SE_NETWORK_SUCCESSFUL_LOGON
Message text	username:{username} usid:{user id} started {session-type} session from ip:{source ipaddress} source-port: {source port} through {protocol} protocol
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

2.1.6 Default network user authentication used

Description

The default user is logged in via the IP address.

This event might be a hint that the system configuration was not changed from the default setup.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730

- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-16

Message text	{protocol}: Default user {user name} logged in from {ip address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user admin logged in from 192.168.0.1.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

2.1.7 Network unsuccessful login

Description

Incorrect username or password specified during remote login.

If this happens quite often, it might indicate an automated password guessing attack.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-17

Message text	{Protocol}: User {User name} failed to log in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
Severity	Error Warning (for SCALANCE W1780/W1740)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Invalid username

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-18

Category	SE_NETWORK_UNSUCCESSFUL_LOGON

© Siemens AG 2021 All rights reserved

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	audit user: {user name}/0 no such local user
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

Table 2-19

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	login failed, reason='No such local user', user='{username}', context='{sessiontype}', proto='{protocol}', user ipaddr='{source ip-address}'
Facility	LOG_AUTHPRIV
Severity	Error
Event type	Event
Log	Auth.log

Table 2-20

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	audit user: {username}/0 Failed to login over {protocol}: No such local user
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

© Siemens AG 2021 All rights reserved

Invalid password

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-21

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	audit user: {username}/0 Provided bad password
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

Table 2-22

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	login failed, reason='Bad password', user='{username}', context='{sessiontype}', proto='{protocol}', user ipaddr='{source ip-address}'
Facility	LOG_AUTHPRIV
Severity	Error

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Event type	Event
Log	Auth.log

Table 2-23

Category	SE_NETWORK_UNSUCCESSFUL_LOGON
Message text	audit user: {username}/0 Failed to login over {protocol}: Bad password
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

2.1.8 Network logout

Description

Session ended with user logout.

© Siemens AG 2021 All rights reserved

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-24

Message text	{protocol}: User {user name} has logged out from {ip address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-25

Category	SE_LOGOFF

Category	SE_LOGOFF
Message text	username:{user name} usid:{user id} stopped {context} session from ip: {source ip-address}
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

Table 2-26

Category	SE_LOGOFF
Message text	audit user: {user name}/0 Logged out {protocol} <local> user
Facility	LOG_AUTHPRIV
Severity	Info
Event type	Event
Log	Auth.log

2.1.9 No access to server

Description

No access to the server or the server is not responding.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740

Table 2-27

Message text	{Protocol}: {IP address} - No response from the RADIUS server.
Example	WBM: 192.168.1.105 - No response from the RADIUS server.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

2.2 Identification and authentication of devices (access via firewall)

2.2.1 Successful device identification

Description

A known device requested a connection.

The following message appears for the modules:

- SCALANCE M-800

© Siemens AG 2021 All rights reserved

- SCALANCE S615
- SCALANCE SC-600

Table 2-28

Message text	{firewall action accept}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	ACCEPT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443
Severity	Info or Warning or Error (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

2.2.2 Unsuccessful device identification

Description

An unknown device requested a connection. The request was denied.

© Siemens AG 2021 All rights reserved

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-29

Message text	{firewall action reject}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port}
Example	REJECT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 dip:217.194.40.109 tcp:53773->443
Severity	Info or Warning or Error (configurable)
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.2

2.3 Account management

2.3.1 Password enabled

Description

Password protection was enabled for some resource.

The following message appears for the module:

- RUGGEDCOM RX1400

Table 2-30

Category	SE_ACCESS_PWD_ENABLED
Message text	Enabling Brute Force Attack Protection
Facility	LOG_USER
Severity	Error
Event type	Event
Log	Syslog

2.3.2 Password disabled

Description

Password protection was disabled for some resource.

The following message appears for the modules:

- RUGGEDCOM RX1400

Table 2-31

Category	SE_ACCESS_PWD_DISABLED
Message text	Brute Force Attack protection not enabled
Facility	LOG_USER
Severity	Error
Event type	Alarm
Log	Syslog

© Siemens AG 2021 All rights reserved

2.3.3 Password changed

Description

User has changed own password.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-32

Message text	{protocol}: User {user name} changed own password.

Message text	{protocol}: User {user name} changed own password.
Example	WBM: User admin changed own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Password of another user changed

User has changed the password of another user.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-33

Message text	{protocol}: User {user name} changed password of user {action user name}.
Example	Telnet: User admin changed password of user test.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

The following message appears for the module:

- RUGGEDCOM RX1400

Table 2-34

Category	SE_ACCESS_PWD_CHANGED
Message text	audit user: {User Group}/{User ID} WebUI action '/ rmf_admin:admin/ users/userid{"{Target User}"}/set-password'
Facility	LOG_DAEMON
Severity	Info
Event type	Event
Log	AUTH_LOG

© Siemens AG 2021 All rights reserved

2.3.4 Account created

Description

The user has created an account.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-35

Message text	{protocol}: User {user name} created user-account {action user name}.
Example	WBM: User admin created user-account service.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

© Siemens AG 2021 All rights reserved

2.3.5 Account disabled

Description

The administrator deleted an existing account.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-36

Message text	{protocol}: User {user name} deleted user-account {action user name}.

Message text	{protocol}: User {user name} deleted user-account {action user name}.
Example	WBM: User admin deleted user-account service.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

2.4 Access enforcement

2.4.1 Access granted

Description

Restricted access was granted for a user.

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-37

Category	SE_ACCESS_GRANTED
Message text	audit user:{Username}/0 logged in through Web UI from {IP Address}
Facility	LOG_DAEMON
Severity	Info
Event type	Event
Log	Auth.log

Table 2-38

Category	SE_ACCESS_GRANTED
Message text	audit user: {Username}/{User ID} assigned to groups: {User Group}
Facility	LOG_DAEMON
Severity	Info
Event type	Event
Log	Auth.log

Table 2-39

Category	SE_ACCESS_GRANTED
Message text	username: {Username} usid: {User ID} started {Context} session from ip:{IP Address} source-port:{Port} through {Protocol} protocol
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

© Siemens AG 2021 All rights reserved

2.4.2 Access denied

Description

Restricted access was denied for a user.

The following messages appear for the module:

- RUGGEDCOM RX1400

Table 2-40

Category	SE_ACCESS_DENIED
Message text	audit user: {Username}/0 Provided Invalid Password
Facility	LOG_DAEMON
Severity	Info
Event type	Alarm
Log	Auth.log

Table 2-41

Category	SE_ACCESS_DENIED
Message text	login failed, user:'{username}', reason='{reason}', user ipaddr='{IP Address}', context='{context}', proto='{protocol}'
Facility	LOG_AUTHPRIV
Severity	Error
Event type	Alarm
Log	Auth.log

© Siemens AG 2021 All rights reserved

2.5 Identifier management

2.5.1 User group created

Description

The administrator has created a group and assigned it to a role.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-42

Message text	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
Example	WBM: User admin created group it-service and assigned to role service.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

2.5.2 User group deleted

Description

The administrator has deleted an existing group and the role assignment.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

© Siemens AG 2021 All rights reserved

Table 2-43

Message text	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
Example	WBM: User maier deleted group it-service and the role service assignment.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.4

2.6 Unsuccessful login attempts

Description

If there are too many failed logins, the corresponding user account was locked for a specific period of time.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-44

Message text	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

The following messages appear for the module:

- RUGGEDCOM RX1400

© Siemens AG 2021 All rights reserved

Table 2-45

Category	SE_ACCOUNT_LOCKED_TEMP
Message text	ALARM: BFA from IP {IP Address} is blocked -> {Event Time}
Facility	LOG_DAEMON
Severity	Emergency
Event type	Alarm
Log	Syslog

Table 2-46

Category	SE_ACCOUNT_LOCKED_TEMP
Message text	{Function}: detect BFA from {IP Address}, raise alarm
Facility	LOG_DAEMON
Severity	Verbose
Event type	Alarm
Log	Syslog

Table 2-47

Category	SE_ACCOUNT_LOCKED_TEMP
Message text	{Function}: alarm asserted id={Event ID}
Facility	LOG_DAEMON
Severity	Verbose
Event type	Alarm
Log	Syslog

Table 2-48

Category	SE_ACCOUNT_LOCKED_TEMP (Freed)
Message text	{Function}: deassert BFA alarm ip={IP address}
Facility	LOG_DAEMON
Severity	Verbose
Event type	Event
Log	Syslog

2.7 Access via untrusted networks (IPsec)

2.7.1 Connection established

Description

VPN connection is established (IPsec).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-49

Message text	[IKE] <{connection name}|{config detail}> IKE_SA {connection name}[{config detail}] established between {ip address}[{config detail}]...{ip address}[{config detail}]
Example	[IKE] <c1|3> IKE_SA c1[1] established between 192.168.55.210[lokal]..192.168.55.211[remote]
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

2.7.2 Connection closed

Description

VPN tunnel is closed (IPsec).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-50

Message text	[IKE] <{connection name}|{config detail}> deleting IKE_SA {connection name}[{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}]

© Siemens AG 2021 All rights reserved

Message text	[IKE] <{connection name}|{config detail}> deleting IKE_SA {connection name}[{config detail}] between {ip address}[{config detail}]...{ip address}[{config detail}]
Example	[IKE] <c1|3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote]
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

2.7.3 Authentication failed

Description

Authentication of VPN connection failed (IPsec).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-51

Message text	[IKE] <{connection name}|{config detail}> received AUTHENTICATION_FAILED notify error
Example	[IKE] <c1|1> received AUTHENTICATION_FAILED notify error
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3)

© Siemens AG 2021 All rights reserved

2.8 Access via untrusted networks (OpenVPN)

2.8.1 Connection established

Description

VPN connection is established (OpenVPN).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-52

Message text	OVPN_{connection name}[{config detail}]: Initialization Sequence Completed
Example	OVPN_Conn_1[2427]: Initialization Sequence Completed
Severity	Info
Facility	local0

Message text	OVPN_{connection name}[{config detail}]: Initialization Sequence Completed
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

2.8.2 Connection closed

Description

VPN connection was closed (OpenVPN).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-53

Message text	OpenVPN connection {connection name} has been deactivated.
Example	OpenVPN connection c1 has been deactivated.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1)

© Siemens AG 2021 All rights reserved

2.9 Access via untrusted networks (SINEMA Remote Connect)

2.9.1 Connection established (SINEMA RC, Digital Input)

Description

Remote access is permitted. (SINEMA RC, Digital Input)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-54

Message text	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Example	SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

2.9.2 Connection established (SINEMA RC, Wakeup SMS)

Description

Remote access is permitted. (SINEMA RC, Wakeup SMS)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615

Table 2-55

Message text	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Example	SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

© Siemens AG 2021 All rights reserved

2.9.3 Connection closed (IPsec)

Description

The remote session was ended after a period of inactivity (IPsec).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-56

Message text	[JOB] <{connection name}|{config detail}> deleting CHILD_SA after {time second} seconds of inactivity
Example	[JOB] <to_Baugruppe1|21> deleting CHILD_SA after 20 seconds of inactivity
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

2.9.4 Connection closed (OpenVPN)

Description

The remote session was ended after a period of inactivity (OpenVPN).

The following message appears for the modules:

- SCALANCE M-800

- SCALANCE S615
- SCALANCE SC-600

Table 2-57

Message text	OVPN_{connection name}[{config detail}]: [{config detail}] Inactivity timeout (--ping-restart), restarting
Example	OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

2.9.5 Remote access denied (SINEMA RC, Digital Input)

Description

Remote access denied (SINEMA RC, Digital Input)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-58

Message text	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Example	SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

2.9.6 Remote access denied (SINEMA RC, Wakeup SMS)

Description

Remote access denied (SINEMA RC, Wakeup SMS)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615

© Siemens AG 2021 All rights reserved

Table 2-59

Message text	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Example	SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.13

2.10 Authorization enforcement (access via custom firewall)

2.10.1 User logged onto the user-specific firewall

Description

The user has logged onto the user-specific firewall. (USF Digital User Login)

The following messages appear for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-60

Message text	User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout: {timeout} minutes.
Example	User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout 5 minutes.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)

Table 2-61

Message text	User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip "{ip address}".
Example	User specific firewall digital input 1 activated rule set "cpu2" with ip "192.168.16.1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)4820486

2.10.2 Access to user-specific firewall denied

Description

The access to the user-specific firewall was denied.

The access time is expired. (USF User Logout)

© Siemens AG 2021 All rights reserved

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-62

Message text	User specific firewall user "{user name}" ruleset "{firewall rule}" time expired.
Example	User specific firewall user "usf" ruleset "rs1" time expired.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

2.10.3 Access to user-specific firewall denied

Description

The access to the user-specific firewall was denied.

The device administrator deactivates the user using the "Force Deactivate" button. (USF user force log out by admin)

© Siemens AG 2021 All rights reserved

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-63

Message text	User specific firewall user "{user name}" logged out by administrator configuration.
Example	User specific firewall user "usf" logged out by administrator configuration.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

2.10.4 Access to user-specific firewall denied

Description

The access to the user-specific firewall was denied. The device administrator has deactivated the user. (USF user deactivated by admin)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-64

Message text	User specific firewall user "{user name}" deactivated by administrator configuration.
Example	User specific firewall user "usf" deactivated by administrator configuration.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

2.10.5 Access to user-specific firewall denied

Description

The access to the user-specific firewall was denied. The corresponding set of rules has been deactivated. (USF Digital Input Logout)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-65

Message text	User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}".
Example	User specific firewall digital input 1 deactivated rule set "rs1".
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

© Siemens AG 2021 All rights reserved

2.11 Session lock

Description

The current session was locked due to inactivity.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-66

Message text	The session of user {user name} was closed after {time} seconds of inactivity.
Example	The session of user admin was closed after 60 seconds of inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

2.12 Wireless access restrictions

2.12.1 WLAN client connected to AP

Description

WLAN client connected to AP.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-67

Message text	{vap}: Client {SRC mac} associated successfully.
Example	VAP1.1: Client 00:0C:29:2F:09:B3 associated successfully.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.12.2 WLAN client could not connect to AP

Description

WLAN client connection to AP denied.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-68

Message text	{vap}: Client {SRC mac} failed to associate, status {status}.

© Siemens AG 2021 All rights reserved

Message text	{vap}: Client {SRC mac} failed to associate, status {status}.
Example	VAP1.1: Client 00:0C:29:2F:09:B3 failed to associate, status (Invalid group cipher).
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.12.3 WLAN radio in use

Description

Radio frequency is already in use.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-69

Message text	Overlap-AP found on {Wlan interface}: AP {ssid} {Src mac} found on channel {Channel} rssi {Signal strength}.
Example	Overlap-AP found on WLAN1: AP MyWLAN 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

Table 2-70

Message text	Overlap-AP found on {Wlan interface}: AP {ssid_Hex} {Src mac} found on channel {Channel} rssi {Signal strength}.
Example	Overlap-AP found on WLAN1: AP 050E081234 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.12.4 WLAN client cisocnnected

Description

WLAN client disconnected from AP.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730

© Siemens AG 2021 All rights reserved

- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-71

Message text	{vap}: Client {SRC mac} disassociated with reason {reason}.
Example	VAP1.1: Client 00:0C:29:2F:09:B3 disassociated with reason (Unknown peer).
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.12.5 WLAN client authentication failed

Description

WLAN client connection to AP denied.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-72

Message text	{vap}: Client {SRC mac} failed to authenticate, status {status}.
Example	VAP1.1: Client 00:0C:29:2F:09:B3 failed to authenticate, status (Invalid group cipher).
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.12.6 RADIUS server not available

Description

RADIUS server not found.

The following message appears for the modules:

- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-73

Message text	{Protocol}: {IP address} - No response from the RADIUS server.

© Siemens AG 2021 All rights reserved

Message text	{Protocol}: {IP address} - No response from the RADIUS server.
Example	WBM: 192.168.1.105 - No response from the RADIUS server.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.2

2.13 Remote session termination

Description

The remote session was ended after a period of inactivity.

The following message appears for the modules:

- SCALANCE SC-600

Table 2-74

Message text	{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote session OpenVPN was closed after 44 seconds of inactivity.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

© Siemens AG 2021 All rights reserved

2.14 Limiting the number of simultaneous sessions

Description

The maximum number of parallel sessions has been exceeded.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-75

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The maximum number of 10 concurrent login sessions exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

2.15 Protection of audit information

2.15.1 Audit log cleared

Description

The administrator cleared the Audit Trail buffer.

The following message appears for the modules:

- RUGGEDCOM RX1400

Table 2-76

Category	SE_AUDIT_LOG_CLEARED
Message text	Deleted logs by restore-factory defaults issued by user {Username}
Facility	LOG_DAEMON
Severity	Emergency
Event type	Alarm
Log	Syslog

© Siemens AG 2021 All rights reserved

2.16 Nonrepudiation

Description

The device configuration has been changed permanently.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-77

Message text	Device configuration changed.
Example	Device configuration changed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

2.17 Communication integrity

2.17.1 Communication data integrity error

Description

Integrity check failed

The following message appears for the modules:

- RUGGEDCOM RX1400

Table 2-78

Category	SE_COMMUNICATION_DATA_INTEGRITY_ERROR
Message text	FAILURE. The firmware integrity check has failed. This may indicate that some operating system files have been modified or tampered with. For assistance, contact Siemens Customer Support.
Facility	LOG_DAEMON
Severity	Critical
Event type	Alarm
Log	Syslog

© Siemens AG 2021 All rights reserved

2.17.2 Communication data integrity error (IPsec)

Description

Integrity check failed (IPsec)

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-79

Message text	[IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored.

Message text	[IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored.
Example	[IKE] "c1" "1" received invalid DPD sequence number 10 (expected 12), ignored.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

2.17.3 Communication data integrity error (OpenVPN)

Description

Integrity check failed (OpenVPN).

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600

Table 2-80

Message text	OVPN_{connection name}{config detail}: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Example	OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

© Siemens AG 2021 All rights reserved

2.18 Session authenticity

2.18.1 Session closed

Description

The session is closed. Authenticated communication connection (not user sessions).

The following message appear for the modules:

- RUGGEDCOM RX1400

Table 2-81

Category	SE_SESSION_CLOSED
Message text	username: {Username} usid: {User ID} stopped {Context} session from ip:{IP Address}
Facility	LOG_AUTH

Category	SE_SESSION_CLOSED
Severity	Notice
Event type	Event
Log	Auth.log

Table 2-82

Category	SE_SESSION_CLOSED (console)
Message text	username: {Username} usid: {User ID} started {Context} session from ip: 127.0.0.1 source-port:0 through console protocol
Facility	LOG_AUTH
Severity	Notice
Event type	Event
Log	Auth.log

2.18.2 Invalid session ID

Description

The session is invalid.

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615

Table 2-83

Message text	{Protocol}: Session ID verification from {ipaddress} failed.
Example	WBM Session ID verification from 192.168.1.1 failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

2.19 Data backup in automation system

2.19.1 Backup successfully done

Description

The ConfigPack file was saved.

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740

© Siemens AG 2021 All rights reserved

- SCALANCE W1780/W1740

Table 2-84

Message text	{protocol}: Saved file type ConfigPack.
Example	TFTP: Saved file type ConfigPack
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

Description

User has saved the ConfigPack file.

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE W760/W720
- SCALANCE W780/W740
- SCALANCE W1780/W1740

© Siemens AG 2021 All rights reserved

Table 2-85

Message text	{protocol}: User {user name} saved file type ConfigPack
Example	WBM: User admin saved file type ConfigPack.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

2.19.2 Backup failed

Description

User failed to save the ConfigPack file.

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-86

Message text	{protocol}: User {user name} failed to save file type ConfigPack.
Example	WBM: User admin failed to save file type ConfigPack.
Severity	Info
Facility	local0

Message text	{protocol}: User {user name} failed to save file type ConfigPack.
Standard	IEC 62443-3-3 Reference: SR7.3

Description

The ConfigPack file could not be saved.

The following message appears for the modules:

- SCALANCE M-800
- SCALANCE S615
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-87

Message text	{protocol}: Failed to save file type ConfigPack.
Example	TFTP: Failed to save file type ConfigPack.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR7.3

© Siemens AG 2021 All rights reserved

2.20 Recovery and reconstitution

2.20.1 Restore successfully done

Description

The firmware was successfully loaded.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-88

Message text	{protocol}: Loaded file type Firmware {version} (restart required).
Example	TFTP: Loaded file type Firmware V02.00.00 (restart required).
Severity	Notice

Message text	{protocol}: Loaded file type Firmware {version} (restart required).
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Description

The user has successfully loaded the firmware.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

© Siemens AG 2021 All rights reserved

Table 2-89

Message text	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
Example	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

2.20.2 Restore failed

Description

Firmware upload has failed.

The following message appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

Table 2-90

Message text	{protocol}: Failed to load file type Firmware.
Example	WBM: Failed to load file type Firmware.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

2.20.3 Configuration loaded

Description

The configuration is applied.

The following messages appears for the modules:

- SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG
- SCALANCE XM-400/XR-500
- SCALANCE M-800
- SCALANCE S615
- SCALANCE SC-600
- SCALANCE W760/W720
- SCALANCE W770/W730
- SCALANCE W780/W740
- SCALANCE W1780/W1740

© Siemens AG 2021 All rights reserved

Table 2-91

Message text	{protocol}: Loaded file type Config (restart required).
Example	TFTP: Loaded file type Config (restart required).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Table 2-92

Message text	{protocol}: Loaded file type ConfigPack (restart required).
Example	TFTP: Loaded file type ConfigPack (restart required).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Table 2-93

Message text	{protocol}: User {user name} loaded file type Config (restart required).
Example	WBM: User admin loaded file type Config (restart required).
Severity	Notice
Facility	local0

Message text	{protocol}: User {user name} loaded file type Config (restart required).
Standard	IEC 62443-3-3 Reference: SR 7.4

Table 2-94

Message text	{protocol}: User {user name} loaded file type ConfigPack (restart required).
Example	WBM: User admin loaded file type ConfigPack (restart required).
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

2.20.4 Patch deployment succeeded

Description

Patch successfully deployed.

The following message appears for the modules:

- RUGGEDCOM RX1400

Table 2-95

Category	SE_PATCH_DEPLOYMENT_SUCCEEDED
Message text	The other partition was imaged successfully. A reboot is required to boot the other partition.
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

2.20.5 Patch deployment failed

Description

Failed to deploy patch.

The following message appears for the modules:

- RUGGEDCOM RX1400

Table 2-96

Category	SE_PATCH_DEPLOYMENT_FAILED (Failure during ROXFLASH)
Message text	A failure was encountered in the upgrade process.
Facility	LOG_DAEMON
Severity	Notice
Event type	Event

© Siemens AG 2021 All rights reserved

Category	SE_PATCH_DEPLOYMENT_FAILED (Failure during ROXFLASH)
Log	Upgrade

Table 2-97

Category	SE_PATCH_DEPLOYMENT_FAILED (During uninstall - ROXFLASH)
Message text	A failure was encountered in the uninstallation process.
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

Table 2-98

Category	SE_PATCH_DEPLOYMENT_FAILED (Can not connect to upgrade server - ROXFLASH)
Message text	Failed to get upgrade details from server, please verify connection.
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

Table 2-99

Category	SE_PATCH_DEPLOYMENT_FAILED (No differences - ROXFLASH)
Message text	No differences detected in target version. Nothing to upgrade
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

Table 2-100

Category	SE_PATCH_DEPLOYMENT_FAILED (Failed to configure boot partition - ROXFLASH)
Message text	Failed to configure system to boot partition %s on next boot
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

Table 2-101

Category	SE_PATCH_DEPLOYMENT_FAILED (Failed to upgrade target partition - upgrade)
Message text	Failed upgrading target partition
Facility	LOG_DAEMON

© Siemens AG 2021 All rights reserved

Category	SE_PATCH_DEPLOYMENT_FAILED (Failed to upgrade target partition - upgrade)
Severity	Notice
Event type	Event
Log	Upgrade

Table 2-102

Category	SE_PATCH_DEPLOYMENT_FAILED (General) - upgrade
Message text	Failed running {Command} on target partition
Facility	LOG_DAEMON
Severity	Notice
Event type	Event
Log	Upgrade

© Siemens AG 2021 All rights reserved

3 Appendix

3.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

© Siemens AG 2021 All rights reserved

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that’s tailored to the customer’s specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

3.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

3.3 Links and literature

Table 3-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109805218
\3\	SIMATIC NET: Industrial Ethernet switches SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109799818
\4\	SIMATIC NET: Industrial Ethernet switches SCALANCE XM-400/XR-500 Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109798663
\5\	SIMATIC NET: Industrial Remote Communication Remote Networks SCALANCE M-800 Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109751635
\6\	SIMATIC NET: Industrial Ethernet Security SCALANCE S615 Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109751632
\7\	SIMATIC NET: Industrial Ethernet Security SCALANCE SC-600 Web Based Management (WBM) https://support.industry.siemens.com/cs/ww/en/view/109754815
\8\	SIMATIC NET: Industrial Wireless LAN SCALANCE W760/W720 to IEEE 802.11n Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109759653
\9\	SIMATIC NET: Industrial Wireless LAN SCALANCE W770/W730 to IEEE 802.11n Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109759613
\10\	SIMATIC NET: Industrial Wireless LAN SCALANCE W780/W740 to IEEE 802.11n Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109759652
\11\	SIMATIC NET: Industrial Wireless LAN SCALANCE W1780/W1740 according to IEEE 802.11ac Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109762413
\12\	RUGGEDCOM ROX II v2.14 Web Interface Configuration Manual for RX1400 https://support.industry.siemens.com/cs/ww/en/view/109481698

© Siemens AG 2021 All rights reserved

3.4 Change documentation

Table 3-2

Version	Date	Modifications
V1.0	12/2021	First version

© Siemens AG 2021 All rights reserved