SIEMENS

Guidance Documentation Supplement

RUGGEDCOM ROS v4.2.2.F

Reference Guide

08/2018
RC1408-EN-01

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

Open Source

RUGGEDCOM ROS contains Open Source Software. For license conditions, refer to the associated *License Conditions* document.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit https://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit https://support.automation.siemens.com.

Contacting Siemens

Address
Siemens Canada Ltd
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

Web
https://www.siemens.com/ruggedcom

Table of Contents

1 Introduction

The Target of Evaluation (TOE) is the Siemens Canada Ltd (Siemens) RUGGEDCOM ROS (Rugged Operating System) v4.2.2.F. The TOE is a proprietary operating system designed for the RUGGEDCOM appliances developed and built by Siemens. These appliances are designed specifically to withstand harsh environmental conditions including temperature and humidity extremes, shock, vibration, and electromagnetic interference. The M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF switches, equipped with the RUGGEDCOM ROS v4.2.2.F operating system, provide Ethernet switching capabilities for customer networks in virtually any environment.

The following conventions are used throughout this document:

- *Italics* – used for all document titles
- **Bold** – used for web interface menu items (note: CLI and web interface menu names are the same)
- `Courier New font` – used for file names

CONTENTS

Section 1.1

Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria Evaluated Configuration. This document provides clarifications and changes to the Siemens documentation and should be used as the guiding document for the installation and administration of the TOE in the Common Criteria-evaluated configuration. The official Siemens documentation should be referred to and followed only as directed within this document.

Table 1 lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1: Guidance Documentation

Document Name	Platform	Description
RUGGEDCOM M2100F Installation Guide *[https://support.industry.siemens.com/cs/ww/en/view/109757152]*	M2100F	Includes steps for the basic initialization and setup of the TOE.
RUGGEDCOM M2200F Installation Guide *[https://support.industry.siemens.com/cs/ww/en/view/109757153]*	M2200F	
RUGGEDCOM M969F Installation Guide *[https://support.industry.siemens.com/cs/ww/en/view/109757214]*	M969F	

Document Name	Platform	Description
RUGGEDCOM RS400F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757213]	RS400F	
RUGGEDCOM RS416F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757163]	RS416F	
RUGGEDCOM RS416PF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757164]	RS416PF	
RUGGEDCOM RS900F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757159]	RS900F	
RUGGEDCOM RS900GF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757161]	RS900GF	
RUGGEDCOM RS900GPF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757162]	RS900GPF	
RUGGEDCOM RS940GF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757165]	RS940GF	
RUGGEDCOM RSG2100F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757154]	RSG2100F	
RUGGEDCOM RSG2100PF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757155]	RSG2100PF	
RUGGEDCOM RSG2200F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757156]	RSG2200F	
RUGGEDCOM RSG2300F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757157]	RSG2300F	
RUGGEDCOM RSG2300PF Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757158]	RSG2300PF	
RUGGEDCOM RSG2488F Installation Guide [https://support.industry.siemens.com/cs/ww/en/view/109757160]	RSG2488F	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757151]	RS400F	Contains detailed steps for how to properly configure and maintain the TOE.
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757141]	RS416F, RS416PF	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757144]	RS900F	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757142]	RS900GF	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757143]	RS900GPF	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757145]	RS940GF	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757146]	M969F	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757147]	RSG2100F, RSG2100PF, M2100F	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757148]	RSG2200F, M2200F	

Document Name	Platform	Description
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757149]	RSG2300F, RSG2300PF	
RUGGEDCOM ROS v4.2.2.F User Guide [https://support.industry.siemens.com/cs/ww/en/view/109757150]	RSG2488F	
FAQ - "How to Implement Secure, Unattended Logging in ROS" [https://support.industry.siemens.com/cs/ww/en/view/109756843]	N/A	A guide on how to setup and maintain secure audit logging on the TOE.
RUGGEDCOM ROS Devices Security Policy, v0.14, August 16, 2017 [https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3000.pdf]	N/A	FIPS 140-2 validation documentation that describes FIPS mode and any configurations necessary for FIPS mode.

Section 1.2
Target Audience

The audience for this document consists of the end-user, the Siemens development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

Section 1.3
Evaluated TOE Configuration

Figure 1 depicts the evaluation configuration of the TOE. The following are previously undefined acronyms that appear within the diagram:

- SSH – Secure Shell
- HTTPS – Hypertext Transfer Protocol – Secure
- OCSP – Online Certificate Status Protocol

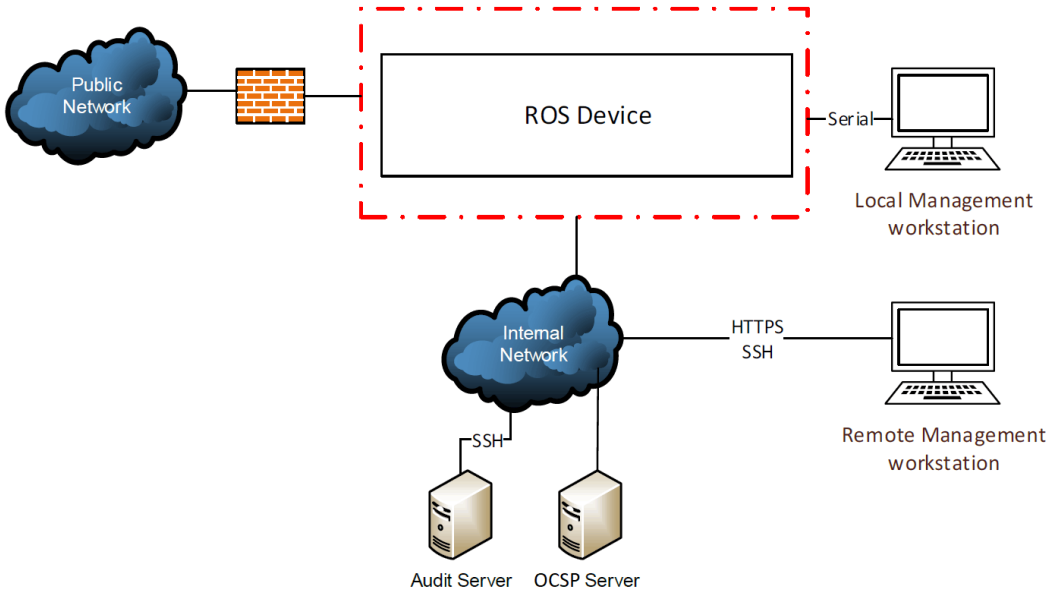

Figure 1: Physical TOE Boundary

Section 1.4

Assumptions

The writers of this document assume the following:

- The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the collaborative Protection Profile (cPP) will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
- The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the Network Device (ND) cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

- The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities
- The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment

2 Installation Procedure

This section describes the installation procedure notes and changes.

CONTENTS

Section 2.1

Introduction

This section provides guidance for how to properly step through the installation instructions documented in the hardware Installation Guides and the RUGGEDCOM ROS v4.2.2.F User Guides, along with additions and changes to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

Before beginning the installation, the administrator should make certain that all the necessary components have been collected. The following items will be needed and must be acquired before continuing with this guidance:

- **Siemens RUGGEDCOM Appliance**
  At least one of the following Siemens RUGGEDCOM appliances with preinstalled firmware v4.2.2.F must be available: M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF
- **Autossh**
  This program is an open-source tool that allows the audit server to connect to the RUGGEDCOM ROS device and collect log data
- **Management Workstation**
  The selected workstation must meet the System Requirements in the “Preface” section of each of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*[1] listed in Section 1.1, “Purpose”. The same workstation can be used for local and remote access.
- **Audit Server**
  An audit server with an SSH client and autossh
- **OCSP Responder**
  Access to an OCSP Responder is required. Each Certificate Authority (CA) should provide an OCSP Responder link. The TOE must be able to access this link.

[1] This is a generic reference to the Siemens RUGGEDCOM ROS v4.2.2.F User Guides. Please refer to the User Guide that is specific to the model being used.

Section 2.2
Secure Installation

This section provides the secure installation steps in a series of installation phases.

CONTENTS

Section 2.2.1
Phase 1 – Hardware Installation

Prior to hardware installation, the administrator should confirm that the model number of the device to be installed matches one of the TOE model numbers. Siemens provides a set of hardware installation guides that include instructions for installation, connecting communication ports, and mounting the appliance as well technical specification of the hardware components. There is a unique hardware installation guide for each of the hardware models claimed in the TOE: M2100F, M2200F, M969F, RSG2100F, RSG2100PF, RSG2200F, RSG2300F, RSG2300PF, RSG2488F, RS400F, RS416F, RS416PF, RS900F, RS900GF, RS900GPF, and RS940GF. The administrator should follow the appropriate hardware installation guide for the appliance that is being setup.

Section 2.2.2
Phase 2 – TOE Environment Setup

The following sections include the setup instructions for the TOE environment components.

CONTENTS

Section 2.2.2.1
Management Workstation

Administrators use both local and remote management workstations to manage the TOE. This can be the same workstation connected in two different ways or two different workstations. The administrator will connect a workstation that meets the requirements to the Serial or Management port on the appliance. Guidance on how to make these physical connections can be found in "Chapter 2 – Using RUGGEDCOM ROS" of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*. To access the TOE over SSH, the user's workstation must have an SSH client that supports FIPS-validated cryptographic algorithms. Refer to the respective SSH client documentation for information on installing and configuring an SSH client.

Section 2.2.2.2
Audit Server

The evaluated configuration requires that an external audit server is setup in the TOE environment. The TOE is compatible with any external audit server that has autossh installed. The FAQ *How to Implement Secure, Unattended Logging in ROS* includes a script to run from the audit server to access the logs over SSH. The audit server is intended to be deployed in the same secure network as the TOE. Refer to the respective vendor documentation for information on configuring and enabling the server.

Section 2.2.2.3
Online Certificate Status Protocol Server

The TOE will need to connect to an OCSP Responder to verify the validity of certificates within the TOE. Certificates will include the Uniform Resource Identifiers (URIs) to check and the TOE must have access to these URIs. The OCSP Responder should be located in the same secure network as the TOE. As per RFC requirements, the connection to the OCSP Responder is not done via a trusted channel.

Section 2.2.3
Phase 3 – Configuration of the TOE Software

Upon request, the appliance is delivered with the RUGGEDCOM ROS v4.2.2.F firmware preloaded. The v4.2.2.F firmware is configured with FIPS-mode configurations when shipped. FIPS-mode disables any functionality that is not permitted to be used by a FIPS evaluated module. Some initial configurations are necessary to complete FIPS-mode set-up, please see *Siemens RUGGEDCOM ROS Devices Security Policy*, Section 3 to ensure all FIPS configurations are completed. If an upgrade to the v4.2.2.F firmware is required, please refer to Section 3.1.1.

CONTENTS

Section 2.2.3.1
Console Access

The CLI can be accessed via a direct console connection. Details on this connection are found in the “Connecting Directly” Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*.

Section 2.2.3.2
SSH

The SSH server functionality is enabled by default with the algorithms and settings described in the *Siemens RUGGEDCOM ROS Security Target*. These algorithms and settings are not administrator configurable. The TOE supports public key-based or password-based authentication over SSH.

The public keys used for authentication are stored in `sshpub.keys` file. A default SSH key pair is generated and provisioned at the factory. An administrator should generate a new key pair as part of the initial configuration. To update, add, or delete these keys, refer to "SSH Public Keys" in the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*.

Section 2.2.3.3
Web Interface

Secure web service files must be configured on the device using the CLI before the web service will start. The TOE uses Transport Layer Security (TLS) v1.1 or v1.2 for secure management connections to the web interface. The TOE always acts as a server in TLS communications. The TOE only supports the algorithms and the elliptic curves extensions listed in the *Siemens RUGGEDCOM ROS Security Target*. As all TLS selections are allowed in the evaluated configuration, the TOE does not provide a mechanism to modify the TLS configuration setting. X.509 certificates are required to access the web interface. See Section 2.2.3.4, "Setting up X.509 Certificates" for details on this setup. The web service will not start until proper certificates have been added to the trust store (`sslpub.certs`) and the TLS server certificate and corresponding private key have been written to the `ssl.crt` file.

Section 2.2.3.4
Setting up X.509 Certificates

The TOE ensures that the X.509 certificates adhere to RFC[2] 5280 (certificate validation and certificate path validation) and that the certificate path terminates with a trusted CA certificate. A CA certificate should be imported from a trusted CA. An administrator must then add the certificate and certificate chain to the TOE through the CLI Shell. The "SSL Certificates" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* describes this process.

A Certificate Signing Request (CSR) can be generated from the TOE. The ***Administration » Generate Certificate Signing Request*** page provides the form for creating a CSR. The key can be selected as RSA 2048 bit or RSA 3072 bit. Once the additional details are filled in, a CSR and corresponding private key are generated and saved in `csr.txt`. Please see the "Generating a Certificate Signing Request (CSR)" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* for details on the fields.

The certificate chain that is returned can be loaded onto the TOE in a single `ssl.crt` file. The "SSL Certificates" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* describes the format and process for this file. When the TOE accepts a new certificate, the TOE verifies that the DNS[3] name and the Common Name follow the rules laid out in RFC 6125. However, the TOE will reject a Common Name that contains asterisks (*) or wildcard values if the first three (3) characters are numbers (as with an IP[4] address).

A Security Administrator can configure the OCSP Unreachable Action. After navigating to the ***Administration » Configure IP Services*** menu, the **OCSP Unreachable Action** screen has the following options:

- Reject – deletes the `ssl.crt` file

[2] RFC - Request For Comment
[3] DNS - Domain Name System
[4] IP - Internet Protocol

- Accept – the certificate is accepted

Section 2.2.3.5
Audit Data Generation

As administrators manage and configure the TOE through the console port, SSH shell, or web interface, their activities are tracked and recorded as audit records. Actions performed by the user using the password-based 'Admin' account are identified by the username 'Admin' being displayed in the '<USERNAME>' field and the 'fingerprint: <VALUE>' will not be present. Note that only one user of the TOE is allowed to use the password-based 'Admin' account while operating in the evaluated configuration. This will ensure that all actions associated with the username 'Admin' that do not display 'fingerprint: <VALUE>' can be attributed to that individual user. Actions performed by users authenticated using key-based authentication are identified by their username in the '<USERNAME>' field and their SSH public key fingerprint in the 'fingerprint: <VALUE>' field. The username in that case is the client's username associated with particular SSH public key and it is used by the SSH service of the TOE to select the respective public key. These audit records are stored in the file system. The TOE generates audit records for all the required events, which are specified in the *Siemens RUGGEDCOM ROS Security Target* and listed in Appendix A. Logs are stored in syslog.txt and are found in ***Diagnostics » View System Log***. The logs can also be viewed through the CLI using `type syslog.txt`.

An example audit record is shown below:

- 15/09/15 18:29:54.481 INFO 32C Console user 'admin' logged out

This example shows the following event information:

- **Date and time:** September 15, 2015 18:29:54.481
- **Level of event:** possible levels include DEBUG, INFO, NOTICE, WARN, ERROR, CRITICAL, ALERT
- **Interface where event occurred:** possible values are Console, SSH, or HTTPS
- **Username of user who performed the action:** 'admin'
- **Description of the action:** logged out

The TOE maintains between 1.5 and 5.5 MB[5] of local audit storage. At runtime, logs are stored in the `syslog.txt` file. The Administrator roles can view these logs. Only the Administrator role can delete the logs. Modifying the logs is not allowed by any role. The TOE can include a ColdFire or PowerPC processor. The action that is taken when the audit storage is full depends on the type of processor. When the log becomes full on a TOE with a ColdFire processor, the TOE will erase the first sector of the file and begin recording audit records in this sector. When the log becomes full on a TOE with a PowerPC processor, the TOE will erase the log file and begin a new one. A Security Administrator must configure logs to be sent to the external server as they occur so that no log events are lost.

The external audits Server establishes a secure communication channel between the TOE and the external audit server over SSH. Administrators must follow the guidance in the FAQ *How to Implement Secure, Unattended Logging in ROS* to enable and configure the use of a remote audit server. When the remote audit server is enabled, audit events sent to local storage and streamed over SSH to the external audit server. This connection, by design, is not subject to the inactivity timeout. While disconnected, the logs are stored in the `syslog.txt` file. Once the connection is reestablished an administrator shall manually export these records and add them to the external audit server.

The logs command should not be used on the device. This command is only intended for use in exporting logs to an audit server. If it is used on the device the SSH session with the audit server may be interrupted.

[5] MB - Megabytes

Section 2.2.3.6

Configure IP Services

The ***Administration » Configure IP Services*** menu provides the ability to configure session timeouts, the number of authentication attempts allowed, and the lockout behavior. Once configured, this behavior is implemented at the web interface and over SSH. The administrator must make the following configurations in this menu (see Figure 2):

- **Inactivity Timeout**
  This defines how long a user can be inactive before their session times out. The default is 5 minutes, but the console can be 1 to 60 minutes and the web interface can be 1 to 30 minutes.
- **Web Server**
  This defines the number of concurrent user sessions the web interface will support. The default is 4 users, but it must be at least 1 so that the web interface is enabled.
- **SSH Sessions**
  This defines the number of concurrent user sessions the CLI will support. The default is 4 users, but it must be at least 2 so that SSH sessions and external audit server session are enabled.
- **Max Failed Attempts**
  This defines the number of unsuccessful password authentication attempts a user can perform before they are locked out. The default is 10 attempts, but it can be between 1 and 20.
- **Failed Attempts Window**
  This defines the time between maximum failed password login attempts. The default is 5 minutes, but it can be 1 to 30 minutes.
- **Lockout Time**
  This defines how long a user authenticated by password is locked out after failed login attempts. The default is 60 minutes, but it can be 1 to 120 minutes.
- **OCSP Unreachable Action**
  This defines the action the TOE will take if a certificate revocation check fails because the TOE cannot access the OCSP responder. The default is Reject, but it can be set to Accept or Reject.

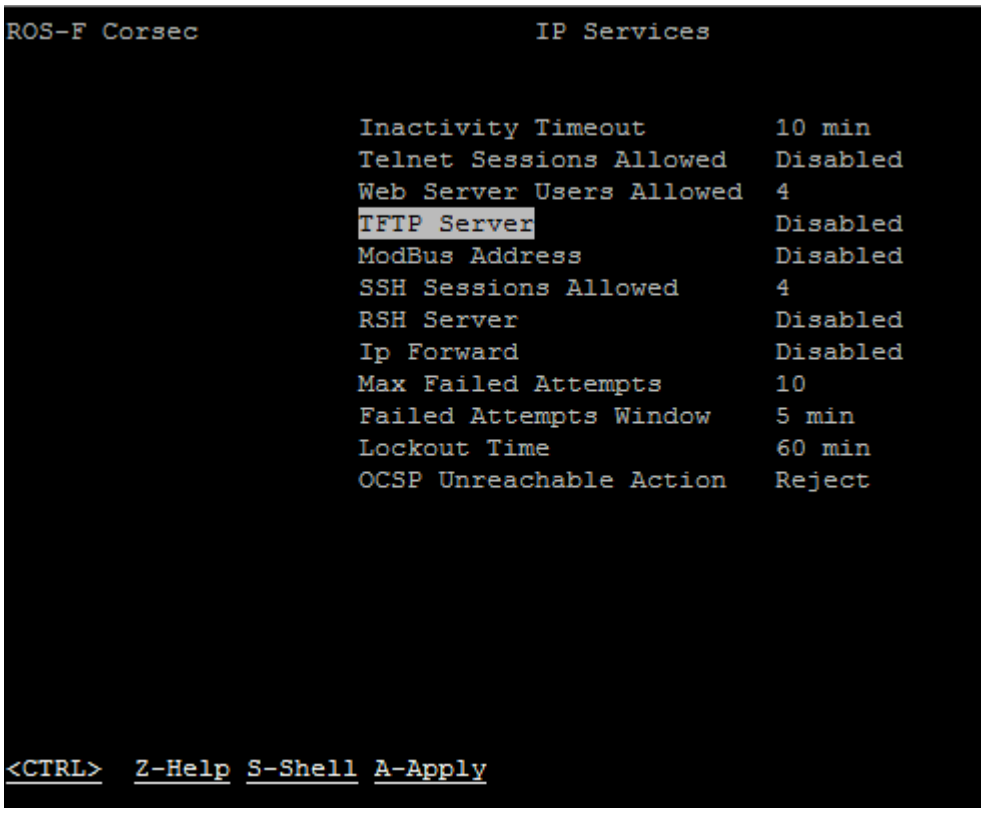

Figure 2: Configure IP Services Menu

More details about setting these parameters are available in the "Configuring IP Services" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*. When configured, an administrator accessing the TOE remotely will be locked out after the **Max Failed Attempts** number of unsuccessful logins has been reached on a particular service (SSH, Console, or Web UI). The administrator's access will be prevented until the **Failed Attempts Window** time has expired or a reboot occurs. SSH key-based authentication is a more secure authentication mechanism and it will not be disabled/blocked by unsuccessful authentication attempts.

Section 2.2.3.7

Password Configurations

The ***Administration » Configure Passwords*** menu (see Figure 4) is used to configure passwords for the TOE. The ADMIN password must be set according to the password policy listed below. The Operator and Guest usernames should be set to null to complete TOE configuration. The TOE interprets a null username as the role not being allowed and will not allow the Operator or Guest roles to login. An alarm is triggered if a password that does not meet the password guidelines is configured as shown in Figure 3.

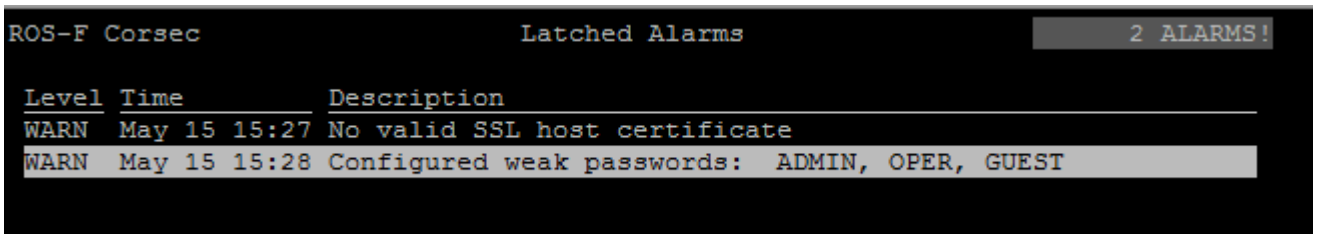

Figure 3: Weak Password Alarm

When setting the passwords, the administrator can refer to the Siemens RUGGEDCOM ROS Security Target for a list of possible characters that can be used. The following configurations should be used:

- **Auth Type Field**
  Should only be set to **Local**, this is the only option allowed in the evaluated configuration
- **Password Minimum Length Field**
  Should be set to at least 15 characters, but can be set from 1 character to up to 17 characters
- **Clear Private Data Option**
  Should be set to **Enabled**. When enabled, this allows an administrator to clear all configuration data, including passwords and private keys, and restore to factory defaults. Restoring factory defaults is available when this parameter is enabled, only from a special sequence entered at the serial console on boot-up. If disabled, a full factory reset may be required to change this data.
- **Guest Username**
  Should be left blank. A blank username disables this account from accessing the TOE.
- **Operator Username**
  Should be left blank. A blank username disables this account from accessing the TOE.

Only the user using password authentication via a specific service (e.g. SSH) will be blocked for that service (e.g. SSH). Password authentications via other services are not affected, meaning that the same user blocked on password authentication on SSH can still be successfully authenticated using the password via the HTTPS service or local Console.

More details about setting these parameters are available in the “Configuring Passwords” Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*.

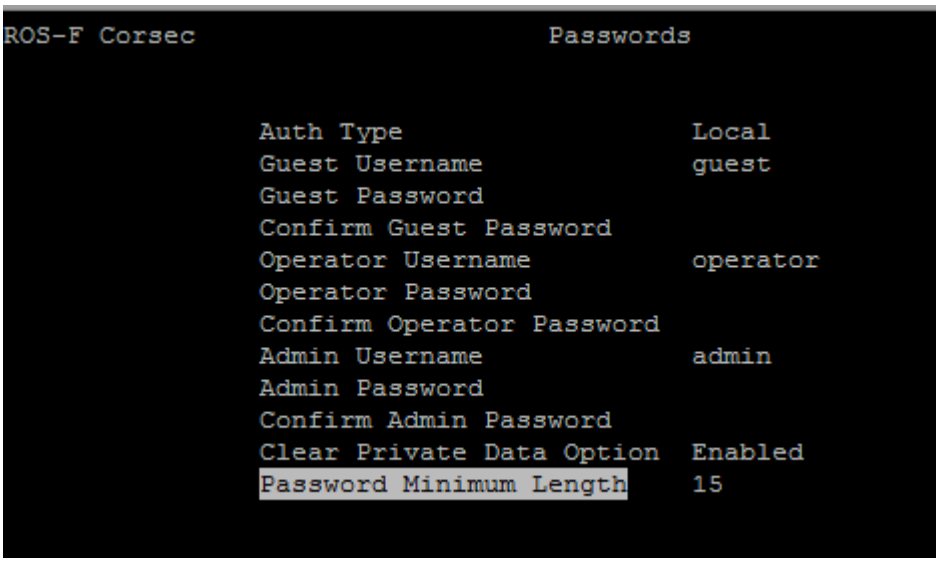

Figure 4: Configure Password Menu

Section 2.2.3.8

Configure the Distributed Network Protocol (DNP)

When configuring the RS416F and RS416PF devices, DNP must be disabled manually. To disable DNP from the Main Menu, navigate to ***Serial Protocols » Configure Protocols » Configure DNP Protocol » Configure DNP***. On the DNP form, change **Transport** to **Disabled** and click the **Apply** button. Details about configuring DNP are found in the "Configuring the DNP Protocol" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* for RS416F and RS416PF devices.

Section 2.2.3.9

Configure the Network Time Protocol (NTP) Time Synchronization

When configuring the ROS device, NTP must be disabled manually. To disable NTP from the Main Menu, navigate to ***Administration » System Time Manager » Configure NTP » Configure NTP Service***. The SNTP Parameters form appears. Select **Disabled** and then click the **Apply** button. Details about configuring NTP are found in the "Managing NTP" section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*.

3 Administrative Guidance

This section provides additional guidance not found in the guides listed in Section 1.1, "Purpose". Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in Chapter 2, *Installation Procedure* before applying the guidance found in Section 3.1, "Clarifications" and Section 3.2, "Exclusions".

CONTENTS

Section 3.1

Clarifications

This section contains clarifications that need to be made to existing guidance documentation.

CONTENTS

Section 3.1.1

Firmware Upgrades

Security Administrators can download firmware upgrades from Siemens Customer Support (https://www.siemens.com/ruggedcom). A Security Administrator can update the TOE by transferring the TOE binary or upgrade packages from an upgrade server using Secure File Transfer Protocol (SFTP). The SFTP transfer uses SSH. See the "Uploading/Downloading Files" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* for details on how to perform this transfer. Once the firmware is uploaded the device must be reset. Follow the instructions in the "Resetting the Device" Section of *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* to reset the device. All firmware is signed by Siemens, and the TOE will reject any firmware updates that are not signed by Siemens.

The TOE stores upgrades in the non-volatile flash memory until a device is reset. Upgrades are applied only after a device reset and digital signature verification. Once the upgrade is complete, the new version can be verified using `>version` on the CLI. See the "Upgrade/Downgrading Firmware" section of the *Siemens RUGGEDCOM ROS*

v4.2.2.F User Guides for more details on the upgrade process. On devices with ColdFire CPUs, the output of this command will show the currently installed versions of the Boot software and the Main software. Each of these is updated separately as shown in Figure 5.

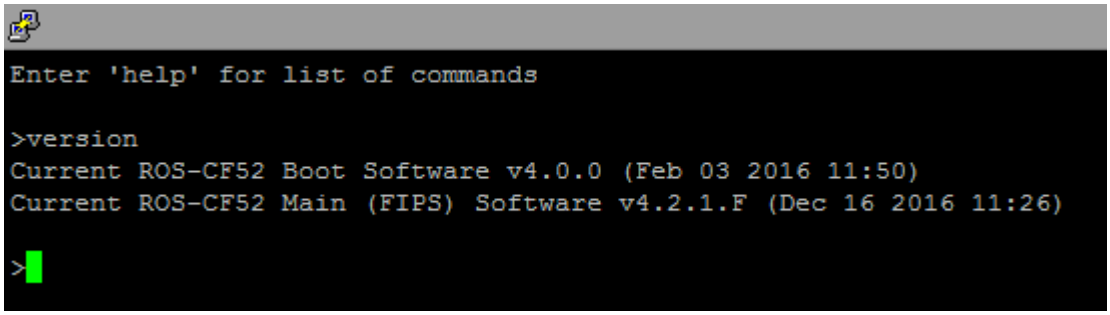

Figure 5: Show Version

On devices with PowerPC processors run uBoot as a bootloader and only the main software version will be shown. If an upgrade has been uploaded and the signature verified, but a rest has not occurred the `>version` command will show a `Next` listing that lists the version that is loaded but not yet active.

Section 3.1.2

Handling Self-testing Errors

The TOE performs FIPS power-up and conditional self-tests for all cryptographic algorithms. The "FIPS Self-Tests" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* provides details on the tests and how to run the tests on demand. If all tests pass, it is logged in the system log file as "Cryptographic tests passed". If a test fails, an event is written to the system log, an LED alarm indicator will blink five times, and the device will restart. During this time, the TOE is in an error state. In this error state, the TOE stops all cryptographic functions, displays an error message on the serial console, logs the error, and initiates a reboot. The TOE is halted upon reaching this error state; no further traffic is processed, and none of the TOE's data output services are available for use. After 10 attempts to restart, if the self test still fails, the device will automatically reboot into Maintenance Mode. This restart counter is reset after the device has run for one hour. Booting into Maintenance Mode will automatically delete the `ssl.crt`, `ssh.keys` and `config.csv` files. If this occurs, administrators should contact Siemen's technical support.

The test can be invoked selectively using `factory` and then `cryptest` at the CLI. A message will be shown if all tests pass.

Section 3.1.3

Time

System time on the TOE must be set manually. The "Managing Time Services" Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* describes how to manually set the time for the TOE. The NTP service is excluded from the TOE and must be disabled.

Section 3.1.4
Key Destruction

Keys are destroyed using a single overwrite of zeros. For non-volatile keys this is done using the `restore-factory-defaults` command. There are no instances where the execution of this command would be delayed.

Section 3.1.5
Public Key-based Authentication

There is only one password-based user, which has the username 'admin' and is assigned the Administrator role. This user is created by default and has a configurable username and password. To allow multiple new users to access the TOE, the password-based user with the role of Administrator can be used to add SSH public keys for specified user names and associate them with the Administrator role. Any user with the role of Administrator is similarly able to add public keys for new users. For information on managing this, refer to the "Managing SSH Public Keys" section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides*.

Section 3.2
Exclusions

Product features and functionality listed in Section 1.5.3 of the Security Target are excluded from the evaluated configuration of the TOE. Any references to those product features and functionality within the guidance documentation should be ignored.

CONTENTS

Section 3.2.1
Disabled Functionality

Upon request, the RUGGEDCOM ROS v4.2.2.F can be delivered as a FIPS model that disables most functionality that should not be used in FIPS mode. This mode restricts services to secure services. Specifically, these devices disable IP forwarding, NTP[1], RADIUS[2], RCDP[3], RSH[4], Remote Syslog, Telnet, TFTP, TACACS+[5], ModBus Management, and SNMP[6] (v1, v2, and v3). The sections of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* that cover these disabled functions include a note that specifically mentions these features are not permitted in FIPS/CC mode. Administrators of the TOE must not enable functionality listed in section 3.2 of this document to remain in the evaluated configuration.

The TOE includes a command, `clear private data`, to zeroize all keys and configurations.

[1] NTP - Network Time Protocol
[2] RADIUS - Remote Authentication Dial-In User Service
[3] RCDP - RUGGEDCOM Discovery Protocol. RCDP has been disabled and removed from all command and debugging interfaces.
[4] RSH - Remote Shell
[5] TACACS+ - Terminal Access Controller Access Control System Plus
[6] SNMP - Simple Network Management Protocol

Section 3.2.2
Remote Authentication

The evaluated configuration of the TOE only supports local authentication. “Managing an Authentication Server” Section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* should not be referenced for the evaluated configuration.

Section 3.2.3
Excluded Functionality

The following services were not part of the evaluated configuration and were not tested:

- Virtual Local Area Network configuration
- Port configuration
- Broadcast Storm filtering
- Quality of Service based on part, tag, MAC16, or IP type of service
- Multiple Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- Enhanced Rapid Spanning Tree Protocol

The following services are present in the TOE but are excluded in this evaluation:

- RADIUS
- TACACS+
- RSH
- Telnet
- TFTP
- ModBus management
- Remote Syslog
- Management connections over SNMP15 v1, v2, and v3
- Management via HTTP
- Network Time Protocol (NTP) time synchronization and service
- RUGGEDCOM Discovery Protocol (RCDP)[7]
- IP forwarding

[7] RCDP has been disabled and removed from all command and debugging interfaces.

4 Acronyms

This section defines the acronyms used throughout this document.

Table 2: Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
cPP	Collaborative Protection Profile
CSR	Certificate Signing Request
DNS	Domain Name System
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LED	Light emitting diode
MAC	Media Access Control
MB	Megabytes
ND	Network Device
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RFC	Request for Comment
ROS	Rugged Operating System
RSA	Rivest-Shamir-Adleman
RSH	Remote Shell
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell

Acronym	Definition
TACACS+	Terminal Access Controller Access Control System Plus
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
URI	Uniform Resources Identifiers
USB	Universal Serial Bus

5 Appendix A: TOE Audit Logs

Table 3 lists the audit event logs generated by the TOE and their descriptions.

Table 3: TOE Aduit Logs

Related SFR	Description	Example Message
FAU_GEN.1	Reset device	<DATE> <TIME> INFO 52C Console user '<USERNAME>', cmd: reset <DATE> <TIME> INFO 52C Reset from shell <DATE> <TIME> INFO 52C Shutting down <FIRMWARE ID>
FAU_GEN.1	Boot up logs which shows the firmware version and model	<DATE> <TIME> INFO 52C Shutting down <FIRMWARE ID> *** Starting <FIRMWARE ID> HwID=<HARDWARE ID>*** <DATE> <TIME> INFO Time Zone updated from 00:00 to -05:00
FAU_GEN.1	Login access through Console with Admin privilege	<DATE> <TIME> INFO 52C Console user '<USERNAME>' logged in with admin level
FAU_GEN.1	Login access via Web GUI with Admin privilege	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged in with admin level <IP ADDRESS>
FAU_GEN.1	Login access through SSH with Admin privilege	<DATE> <TIME> INFO 52C SSH user '<USERNAME>' logged in with admin level <IP ADDRESS>
FAU_GEN.1	Configuration change log: Change the max attempt and attempts window	<DATE> <TIME> INFO 52C Console user '<USERNAME>', IP Services Max Failed Attempts, old: 10, new: 11 Failed Attempts Window, old: 5 min, new: 9 min - MODIFIED <DATE> <TIME> INFO 52C Configuration changed
FAU_GEN.1	Generate certificate signing request	<DATE> <TIME> INFO 53C CSR Generation started <DATE> <TIME> INFO 53C CSR generated
FAU_GEN.1	Configuration change: Change the Admin password	<DATE> <TIME> INFO 52C Console user '<USERNAME>', Passwords Admin Password - MODIFIED <DATE> <TIME> INFO 52C Configuration changed
FAU_GEN.1	Enabling/disabling remote syslog	<DATE> <TIME> INFO 52C RemoteSyslog insert collector <REMOTE SYSLOG IP ADDRESS> <DATE> <TIME> INFO 52C Console user '<USERNAME>', Remote Syslog Server IP Address: <IP ADDRESS> UDP Port: 514 Facility: LOCAL7

Related SFR	Description	Example Message
		Severity: DEBUGGING - INSERTED <DATE> <TIME> INFO 52C Configuration changed
FAU_GEN.1	Starting/stopping services (example SNTP)	<DATE> <TIME> INFO 52C SNTP Client enabled <DATE> <TIME> INFO 52C Console user '<USERNAME>', NTP Servers IP Address, old: , new: <IP ADDRESS> - MODIFIED <DATE> <TIME> INFO 52C Configuration changed <DATE> <TIME> INFO 52C SNTP Client disabled <DATE> <TIME> INFO 52C Console user '<USERNAME>', NTP Servers IP Address, old: <IP ADDRESS>, new: - MODIFIED <DATE> <TIME> INFO 52C Configuration changed
FAU_GEN.1	TLS service start during bootup	<DATE> <TIME> INFO 52C TLS Certificate serial # <VALUE> succeeded validation <DATE> <TIME> INFO 52C Web Server has a valid certificate – continuing initialization <DATE> <TIME> INFO 52C SSL server starting
FAU_GEN.1	SSH service start during bootup	<DATE> <TIME> INFO 52C SSH host key, fingerprint # <VALUE> succeeded validation <DATE> <TIME> INFO 52C SSH server has valid host keys - continuing initialization <DATE> <TIME> INFO 52C sshpub.keys: Successfully added entry 1, fingerprint: <VALUE> <DATE> <TIME> INFO 52C RemoteSyslog initialized with 0 collector(s) <DATE> <TIME> INFO 52C SSH server starting
FAU_GEN.1	Entropy collection	<DATE> <TIME> INFO 52C Entropy Testing... <DATE> <TIME> INFO 52C Entropy Testing... Passed
FAU_GEN.1	DRBG seeding	<DATE> <TIME> INFO 52C DRBG reseeded
FAU_GEN.1	Changing the access banner	<DATE> <TIME> INFO 45C Console user '<USERNAME>', cmd: xmodem receive banner.txt <DATE> <TIME> INFO 45C Flashing banner.txt started <DATE> <TIME> INFO 45C Flashing banner.txt done
FAU_GEN.1	Starting and stopping services (HTTPS)	<DATE> <TIME> INFO 45C Console user '<USERNAME>', IP Services Web Server Users Allowed, old: 4, new: Disabled - MODIFIED <DATE> <TIME> INFO 45C Configuration changed <DATE> <TIME> INFO 45C Web Server disabled <DATE> <TIME> INFO 45C Console user '<USERNAME>', IP Services Web Server Users Allowed, old: Disabled, new: 4 - MODIFIED <DATE> <TIME> INFO 45C Web Server enabled
FAU_GEN.1	Disabling the DNP service	<DATE> <TIME> INFO 45C Console user '<USERNAME>', DNP

Related SFR	Description	Example Message
		Transport, old: TCP, new: Disabled - MODIFIED
FAU_GEN.1	Configuring the lockout time	<DATE> <TIME> INFO 46C Console user '<USERNAME>', IP Services Lockout Time, old: 1 min, new: 2 min - MODIFIED <DATE> <TIME> INFO 46C Configuration changed
FAU_GEN.1	Changing the configured OCSP Unreachable Action	<DATE> <TIME> INFO 46C Configuration changed <DATE> <TIME> INFO 46C Console user '<USERNAME>', IP Services OCSP Unreachable Action, old: Reject, new: Accept - MODIFIED
FAU_GEN.1	Start-up of the audit functions	*** Starting <FIRMWARE ID> HwID=<HARDWARE ID>*** <DATE> <TIME> INFO Time Zone updated from 00:00 to -05:00
FAU_GEN.1	Shut-down of the audit functions	<DATE> <TIME> INFO 52C Console user '<USERNAME>', cmd: reset <DATE> <TIME> INFO 52C Reset from shell <DATE> <TIME> INFO 52C Shutting down <FIRMWARE ID>
FAU_GEN.1	Enabling the Guest and Operator accounts.	<DATE> <TIME> INFO 45C Console user 'admin', Passwords Guest Username, old: , new: <USERNAME> Guest Password Operator Username, old: , new: <USERNAME> Operator Password - MODIFIED.
FAU_GEN.1	Disabling the Guest and Operator accounts by setting the username to blank/ null.	<DATE> <TIME> INFO 45C Console user 'admin', Passwords Guest Username, old: <USERNAME>, new: Operator Username, old: <USERNAME>, new: - MODIFIED.
FAU_STG_EXT.1	Logout from Web GUI with admin privilege	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged out <IP ADDRESS>
FCS_CKM.1	SSH key generation	<DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS>, cmd: sshkeygen rsa 2048 <DATE> <TIME> INFO 52C Generation pending for ssh.keys: SSH Keys <DATE> <TIME> INFO 52C Started generating ssh.keys: SSH Keys <DATE> <TIME> INFO 52C Successfully updated ssh.keys <DATE> <TIME> INFO 52C Generated ssh.keys was saved <DATE> <TIME> INFO 52C Key generation task finished for ssh.keys <DATE> <TIME> NOTE 53C TFTP put file ssh.keys from <IP ADDRESS> <DATE> <TIME> INFO 53C SSH host key, fingerprint # <VALUE> <DATE> <TIME> INFO 53C Flashing ssh.keys started <DATE> <TIME> INFO 53C Flashing ssh.keys done <DATE> <TIME> INFO 53C Successfully updated ssh.keys

Related SFR	Description	Example Message
FCS_CKM.4	Destroying SSH and SSL keys. Generating SSH keypair overwrites existing set.	See FCS_CKM.1 key generation log.
FCS_CKM.4	Clearing private data via console prior to login	<DATE> <TIME> NOTE 52C Clearing private data upon request <DATE> <TIME> NOTE 52C User private data cleared <DATE> <TIME> NOTE 52C Reboot device after clearing private data
FCS_CKM.4	Accessing maintenance mode	<DATE> <TIME> INFO 52C Reset due to Maintenance request <DATE> <TIME> INFO 52C Shutting down <FIRMWARE ID> <DATE> <TIME> NOTE 52C User private data cleared
FCS_COP.1/ DataEncryption	Cryptest 6 (AES-CBC KAT)	<DATE> <TIME> INFO SSH user '<USERNAME>' <IP ADDRESS>, cmd: cryptest 6 <DATE> <TIME> INFO Running cryptographic algorithm self tests <DATE> <TIME> INFO Cryptographic algorithm self tests passed
FCS_COP.1/SigGen	Cryptest 10 (ECDSA-P256 PCT)	<DATE> <TIME> INFO SSH user '<USERNAME>' <IP ADDRESS>, cmd: cryptest 10 <DATE> <TIME> INFO Running cryptographic algorithm self tests <DATE> <TIME> INFO Cryptographic algorithm self tests passed
FCS_COP.1/Hash	Cryptest 3 (SHA-224, SHA-256 KAT)	<DATE> <TIME> INFO SSH user '<USERNAME>' <IP ADDRESS>, cmd: cryptest 3 <DATE> <TIME> INFO Running cryptographic algorithm self tests <DATE> <TIME> INFO Cryptographic algorithm self tests passed
FCS_COP.1/Keyed Hash	Cryptest 5 (HMAC-SHA-1, HMAC-SHA-2 KAT)	<DATE> <TIME> INFO SSH user '<USERNAME>' <IP ADDRESS>, cmd: cryptest 5 <DATE> <TIME> INFO Running cryptographic algorithm self tests <DATE> <TIME> INFO Cryptographic algorithm self tests passed
FCS_HTTPS_EXT.1	Failed negotiation with client	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_TCP_WRITE_ERROR
FCS_TLSS_EXT.1	SSL protocol version mismatch	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_PROTOCOL_VERSION <DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_PROTOCOL_VERSION <DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_TCP_SOCKET_CLOSED
FCS_SSHS_EXT.1	Failure to establish an SSH session	<DATE> <TIME> NOTE 52C SSH Negotiation failure status: ERR_SSH_DISCONNECT_BY_APPLICATION <DATE> <TIME> INFO 52C SSH user '<USERNAME>' closing connection <IP ADDRESS>
FCS_SSHS_EXT.1	Successful SSH rekey	<DATE> <TIME> INFO 52C SSH: Initiating re-keying operation <DATE> <TIME> INFO 52C SSH: Re-keying operation with peer <IP ADDRESS>: took 2 seconds
FCS_SSHS_EXT.1	SSH large packet	<DATE> <TIME> ERROR SSH Reception error: ERR_PAYLOAD_TOO_LARGE. Closing connection.
FCS_SSHS_EXT.1	Adding SSH public key	<DATE> <TIME> INFO 52C sshpub.keys: Successfully added entry 1, fingerprint: <VALUE> <DATE> <TIME> INFO 52C Flashing sshpub.keys started <DATE> <TIME> INFO 52C Flashing sshpub.keys done
FCS_SSHS_EXT.1	Removing SSH public key	<DATE> <TIME> INFO 42C Console user '<USERNAME>', cmd: sshpubkey remove 1 <DATE> <TIME> NOTE 42C Removed Public Key 1

Related SFR	Description	Example Message
FCS_SSHS_EXT.1	Logging in with SSH public key	<DATE> <TIME> INFO 52C SSH user <USERNAME> (pub id 1 fingerprint: <VALUE>) logged in with <USERNAME> access <IP ADDRESS>
FCS_SSHS_EXT.1	Public key algorithm rejection	<DATE> <TIME> NOTE SSH Negotiation failure status: ERR_TCP_SOCKET_CLOSED <DATE> <TIME> INFO SSH user '<USERNAME>' closing connection <IP ADDRESS>
FCS_SSHS_EXT.1	Public key validation failure	<DATE> <TIME> WARN 52C SSH user pub key add failed <DATE> <TIME> ERRO 52C sshpub.keys: Failed to add entry due to invalid Key Entry ID <DATE> <TIME> ERRO 52C sshpub.keys: Failed to add entry 3. Key failed validation.
FCS_SSHS_EXT.1	SSH connection failure – MAC algorithm	<DATE> <TIME> NOTE SSH Negotiation failure status: ERR_SSH_DISCONNECT_KEY_EXCHANGE_FAILED
FCS_SSHS_EXT.1	SSH connection failure – key exchange	<DATE> <TIME> NOTE SSH Negotiation failure status: ERR_SSH_DISCONNECT_KEY_EXCHANGE_FAILED
FCS_SSHS_EXT.1	SSH connection – rekey	<DATE> <TIME> INFO SSH: Initiating re-keying operation <DATE> <TIME> INFO Re-keying operation with peer <IP ADDRESS>: took <SECONDS> seconds
FCS_TLSS_EXT.1	TLS connection – cipher mismatch	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_NO_CIPHER_MATCH
FCS_TLSS_EXT.1	TLS connection – handshake failure	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_PROTOCOL_PROCESS_FINISHED
FCS_TLSS_EXT.1	TLS connection – handshake failure	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_PROTOCOL_BAD_LENGTH
FCS_TLSS_EXT.1	TLS connection – handshake failure	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_NOT_OPEN
FCS_TLSS_EXT.1	TLS connection – handshake failure	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_SSL_INVALID_MSG_SIZE
FCS_RBG_EXT.1	Entropy collection logs	<DATE> <TIME> INFO 52C Entropy Testing... <DATE> <TIME> INFO 52C Entropy Testing... Passed <DATE> <TIME> INFO 52C DRBG reseeded
FIA_AFL.1	Brute force protection	<DATE> <TIME> WARN 52C Excessive failed SSH access/login attempt <DATE> <TIME> INFO 52C SSH service unlocked <DATE> <TIME> WARN 52C Excessive failed HTTPS access/login attempts, service locked <DATE> <TIME> INFO 52C HTTPS service unlocked
FIA_PMG_EXT.1	Minimum password length	<DATE> <TIME> INFO 52C Console user '<USERNAME>', Passwords Guest Password Operator Password Admin Password Password Minimum Length, old: 1, new: 2 - MODIFIED <DATE> <TIME> INFO 52C Configuration changed
FIA_PMG_EXT.1	Resetting password	<DATE> <TIME> INFO 52C 'guest' level password changed <DATE> <TIME> INFO 52C Console user '<USERNAME>', Passwords Guest Password - MODIFIED

Related SFR	Description	Example Message
		<DATE> <TIME> INFO 52C Configuration changed
FIA_UIA_EXT	User login	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged in with admin level <IP ADDRESS> <DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged out <IP ADDRESS> <DATE> <TIME> INFO 52C Failed HTTPS user '<USERNAME>' login attempt <IP ADDRESS> <DATE> <TIME> INFO 52C SSH user '<USERNAME>' logged in with admin level <IP ADDRESS> <DATE> <TIME> INFO 52C Failed SSH user '<USERNAME>' login attempt <IP ADDRESS> <DATE> <TIME> INFO SSH user '<USERNAME>' (pub id 1 fingerprint: <VALUE> logged in with admin access <IP ADDRESS> <DATE> <TIME> INFO 52C Console user '<USERNAME>' logged in with admin level <DATE> <TIME> INFO 52C Failed Console user '<USERNAME>' login attempt
FIA_X509_EXT.1/REV	Certificate validation failure	<DATE> <TIME> INFO Console user '<USERNAME>', cmd: xmodem receive ssl.crt <DATE> <TIME> WARN TLS Certificate serial # <VALUE> failed validation. Error: ERR_CERT_CHAIN_NO_TRUST_ANCHOR
FIA_X509_EXT.1/REV	Certificate validation successful	<DATE> <TIME> INFO Console user '<USERNAME>', cmd: xmodem receive ssl.crt <DATE> <TIME> INFO TLS Certificate serial # <VALUE> succeeded validation
FIA_X509_EXT.1/REV	Certificate expired failure	<DATE> <TIME> INFO 49C Console user '<USERNAME>', cmd: xmodem receive ssl.crt <DATE> <TIME> WARN 49C TLS Certificate serial # <VALUE> failed validation. Error: ERR_CERT_EXPIRED <DATE> <TIME> WARN 49C Failed to load SSL Certificate from ssl.crt. Error: ERR_CERT_EXPIRED <DATE> <TIME> WARN 49C Failed to update ssl.crt <DATE> <TIME> INFO 49C Console user '<USERNAME>', cmd: Command execution failed
FIA_X509_EXT.1/REV	Revoked certificate	<DATE> <TIME> WARN TLS Certificate serial # <VALUE> failed validation. Error: ERR_CERT_REVOKED
FIA_X509_EXT.1/REV	OCSP revocation check failure	<DATE> <TIME> WARN TLS Certificate serial # <VALUE> failed validation. Error: ERROR_CERT_OCSP_FAILED
FIA_X509_EXT.1/REV	Certificate validation failure	<DATE> <TIME> WARN Certificate failed validation. Error: ERR_CERT_INVALID_STRUCT <DATE> <TIME> WARN Failed to update ssl.crt
FIA_X509_EXT.2	OCSP revocation check failure	<DATE> <TIME> WARN Timeout contacting OCSP responder at <IP ADDRESS> <DATE> <TIME> WARN TLS Certificate Serial # <VALUE> failed validation. Error: ERROR_CERT_OCSP_FAILED <DATE> <TIME> WARN ERASING SSL Certificate in ssl.crt <DATE> <TIME> WARN Timeout contacting OCSP responder at <IP ADDRESS>, but OCSP Unreachable Action is set to Accept
FIA_X509_EXT.3	Certificate signing request	<DATE> <TIME> INFO 53C CSR Generation started <DATE> <TIME> INFO 53C CSR generated
FMT_MOF.1/ ManualUpdate	Software update	<DATE> <TIME> INFO 49C SFTP put file main.bin from <IP ADDRESS> by user '<USERNAME>' <DATE> <TIME> INFO Console user '<USERNAME>', cmd: xmodem receive main.bin <DATE> <TIME> INFO 49C Flashing main.bin started <DATE> <TIME> INFO 49C Flashing main.bin done: <FIRMWARE ID>
FMT_MTD.1/CoreData	Importation of SSL certificate	<DATE> <TIME> INFO 52C Console user '<USERNAME>', cmd: xmodem receive ssl.crt <DATE> <TIME> WARN 52C Timeout contacting OCSP responder at <OCSP IP ADDRESS>:<PORT>, but OCSP Unreachable Action is set to Accept

Related SFR	Description	Example Message
		<DATE> <TIME> INFO 52C TLS Certificate serial # <VALUE> succeeded validation <DATE> <TIME> INFO 52C Flashing ssl.crt started <DATE> <TIME> INFO 52C Flashing ssl.crt done <DATE> <TIME> INFO 52C Successfully updated ssl.crt <DATE> <TIME> INFO 52C Web Server has a valid certificate – continuing initialization <DATE> <TIME> INFO 52C SSL server starting
FPT_STM_EXT.1	Time change	<DATE> <TIME> INFO 52C Configuration changed kernel time from: 2018/05/01 13:01:56 to: 2018/05/01 14:01:40 <DATE> <TIME> INFO 52C Console user '<USERNAME>', Time and Date Time, old: 13:01:56, new: 14:01:40 Date, old: May 01, 2018, new: May 01, 2018 - MODIFIED <DATE> <TIME> INFO 52C WriteUTCTime: UTC_Y_M=1805, y=18, m=5 <DATE> <TIME> INFO 52C WriteUTCTime: UTC_D_H=119, d=1, h=19 <DATE> <TIME> INFO 52C WriteUTCTime: UTC_M_S=140, m=1, s=40 <DATE> <TIME> INFO 52C WriteUTCTime: UTC_MSEC=10
FPT_TUD_EXT.1	Software update	<DATE> <TIME> NOTE 42C SFTP put file main.bin from <IP ADDRESS> by user '<USERNAME>' <DATE> <TIME> INFO Console user '<USERNAME>', cmd: xmodem receive main.bin <DATE> <TIME> INFO 42C Flashing main.bin started <DATE> <TIME> INFO 42C Flashing main.bin done: <FIRMWARE ID>
FPT_TUD_EXT.1	Software update failure	<DATE> <TIME> NOTE 42C SFTP put file main.bin from <IP ADDRESS> by user <DATE> <TIME> INFO Console user '<USERNAME>', cmd: xmodem receive main.bin <DATE> <TIME> ERRO Downloaded file main.bin is invalid: Bad signature <DATE> <TIME> NOTE Downloaded file with invalid signature (-7711) <DATE> <TIME> Downloaded file main.bin is invalid: Body CRC invalid
FTA_SSL_EXT.1	Inactivity timer configuration change	<DATE> <TIME> INFO 52C Console user '<USERNAME>' logged in with admin level <DATE> <TIME> INFO 52C Console user '<USERNAME>', IP Services Inactivity Timeout, old: 5 min, new: Disable - MODIFIED <DATE> <TIME> INFO 52C Configuration changed
FTA_SSL_EXT.1	Inactivity timer expiration	<DATE> <TIME> INFO 50C Console user '<USERNAME>', cmd: loggd out.
FTA_SSL_EXT.1	Brute force configuration change	<DATE> <TIME> INFO 52C Console user '<USERNAME>', IP Services Max Failed Attempts, old: 10, new: 2 - MODIFIED <DATE> <TIME> INFO 52C Configuration changed <DATE> <TIME> INFO 49C SSH user '<USERNAME>' closing connection <IP ADDRESS>
FTA_SSL.3	Inactivity timer configuration change	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' <IP ADDRESS>, IP Services Inactivity Timeout, old: 2 min, new: 1 min - MODIFIED

Related SFR	Description	Example Message
		<DATE> <TIME> INFO 52C Configuration changed <DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged out <IP ADDRESS>, <DATE> <TIME> INFO HTTPS user '<USERNAME>' logged out <IP ADDRESS> <DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS>, IP Services Inactivity Timeout, old: Disabled, new: 2 min - MODIFIED <DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS>, cmd: loggd out
FTA_SSL.4	Local session logout	<DATE> <TIME> INFO 52C Console user '<USERNAME>', cmd: logout <DATE> <TIME> INFO 52C <USERNAME> logged out <DATE> <TIME> INFO 52C Console user '<USERNAME>', cmd: loggd out
FTA_SSL.4	Remote session logout	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged out <IP ADDRESS> <DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS> cmd: logout <DATE> <TIME> INFO 52C <USERNAME> logged out <DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS> cmd: loggd out <DATE> <TIME> INFO 52C SSH user '<USERNAME>' closing connection <IP ADDRESS>
FTP_TRP.1/Admin	Secure login	<DATE> <TIME> INFO 52C SSH user '<USERNAME>' logged in with admin level <IP ADDRESS> <DATE> <TIME> INFO 52C HTTPS user '<USERNAME> logged in with admin level <IP ADDRESS>
FPT_TST_EXT.1	Suite of self-tests specified in the SFR executed and passed during bootup	<DATE> <TIME> INFO 44C Cryptographic tests passed
FPT_ITC.1	Initiation of the trusted channel	<DATE> <TIME> INFO 32C SSH user <USERNAME> (pub id <#> fingerprint: <FINGERPRINT>) logged in with admin access (IP: <IP ADDRESS>) <DATE> <TIME> INFO 33C Logs command – logs transfer started
FPT_ITC.1	Termination of the trusted channel	<DATE> <TIME> INFO 32C SSH user <USERNAME> (pub id <#> fingerprint: <FINGERPRINT>) closing connection (IP: <IP ADDRESS>) successful <DATE> <TIME> INFO 33C Logs command – logs transfer stopped
FPT_ITC.1	Failure of the trusted channel functions	<DATE> <TIME> ERRO 32C SSH reception error: ERR_SSH_DISCONNECT_BY_APPLICATION. Closing connection. <DATE> <TIME> INFO 33C Logs command – logs transfer stopped
FPT_TRP/Admin	Termination of trusted path	<DATE> <TIME> INFO 52C HTTPS user '<USERNAME>' logged out <IP ADDRESS> <DATE> <TIME> INFO 52C SSH user '<USERNAME>' <IP ADDRESS> cmd: loggd out <DATE> <TIME> INFO 52C SSH user '<USERNAME>' closing connection <IP ADDRESS>
FPT_TRP/Admin	Failure of trusted path functions	<DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_TCP_WRITE_ERROR <DATE> <TIME> WARN WebServer: Failed to negotiate an SSL connection: ERR_TCP_SOCKET_CLOSED <DATE> <TIME> ERRO 32C SSH reception error: ERR_SSH_DISCONNECT_BY_APPLICATION. Closing connection.