

SIEMENS

FIPS 140-2 Non-Proprietary Security Policy Security Level: 2

RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server

RUGGEDCOM ROS-F v4.2.2.F

Reference Guide

For RS416F, M2100F, M2200F, M969F, RS900F,
RS900GF, RS940GF, RSG2100F, RSG2200F, RSG2488F

Introduction

1

RUGGEDCOM ROS-F Devices

2

Secure Operation

3

Acronyms

4

Appendix A

5

06/2019

RC1409-EN-01

Copyright © 2019 Siemens Canada Ltd

Dissemination or reproduction of this document, or evaluation and communication of its contents, is permitted.

» 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-F 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

Chapter 1

Introduction	1
1.1 Purpose	1
1.2 References	1
1.3 Document Organization	2

Chapter 2

RUGGEDCOM ROS-F Devices	3
2.1 Product Overview	3
2.2 Module Specification	8
2.3 Module Interfaces	12
2.4 Roles, Services, and Authentication	18
2.4.1 Authorized Roles	19
2.4.2 Operator Services	19
2.4.3 Maintenance Mode	25
2.4.4 Additional Services	28
2.4.5 Authentication	29
2.5 Physical Security	30
2.6 Operational Environment	30
2.7 Cryptographic Key Management	31
2.8 EMI / EMC	35
2.9 Self-tests	35
2.9.1 Power-up Self-tests	35
2.9.2 Conditional Self-tests	36
2.9.3 Critical Functions Self-Tests	36
2.9.4 Self-test Error Behavior and Recovery	36
2.10 Mitigation of Other Attacks	37

Chapter 3

Secure Operation	39
3.1 Initial Setup	39
3.2 Crypto Officer Guidance	48
3.2.1 Monitoring Status	48
3.2.2 Physical Inspection	48
3.2.3 On-demand Self-test Execution	49

3.2.4 CSP Zeroization	49
3.2.5 Upgrading/Downgrading Firmware	50
3.2.6 Password Complexity	51
3.3 User Guidance	52
3.4 Additional Guidance and Usage Policies	52
3.5 Non-FIPS-approved Mode	52
 Chapter 4	
Acronyms	53
 Chapter 5	
Appendix A	57
5.1 RSG2100F	57
5.2 M2100F	59
5.3 RSG2200F	59
5.4 M2200F	61
5.5 RSG2488F	61
5.6 M969F	62
5.7 RS900F	63
5.8 RS900GF	64
5.9 RS416F	65
5.10 RS940GF	65

1 Introduction

The following subsections introduce the RUGGEDCOM ROS-F FIPS 140-2 Non-Proprietary Security Policy.

CONTENTS

- [Section 1.1, "Purpose"](#)
- [Section 1.2, "References"](#)
- [Section 1.3, "Document Organization"](#)

Section 1.1

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the RUGGEDCOM Ethernet Switches (Hardware Models: M2100F, M2200F, M969F, RS900F, RS900GF, RS940GF, RSG2100F, RSG2200F, and RSG2488F; Firmware Version: 4.2.2.F) and RUGGEDCOM Serial Device Server (Hardware Model: RS416F; Firmware Version: 4.2.2.F) from Siemens Canada Ltd (Siemens). This Security Policy describes how the RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the [Communications Security Establishment \(CSE\) Cryptographic Module Validation Program \(CMVP\) website](http://csrc.nist.gov/groups/STM/cmvp) [http://csrc.nist.gov/groups/STM/cmvp].

This document also describes how to run the modules in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server are referred to in this document as "RUGGEDCOM ROS-F Devices" or "modules".

Section 1.2

References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the modules from the following sources:

- The [Siemens website](http://siemens.com) [http://siemens.com] contains information on the full line of products from Siemens
- The [CMVP website](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) [http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm] contains contact information for individuals to answer technical or sales-related questions for the module

Section 1.3

Document Organization

The Security Policy document is organized into two (2) primary sections. [Chapter 2, *RUGGEDCOM ROS-F Devices*](#) provides an overview of the validated modules. This includes a general description of the modules' capabilities and their use of cryptography as well as a presentation of the validation level achieved in each applicable functional areas of the FIPS standard. It also provides high-level descriptions of how the modules meet FIPS requirements in each functional area. [Chapter 3, *Secure Operation*](#) documents the guidance needed for the secure use of the modules, including initial setup instructions, management methods, and applicable usage policies.

2 RUGGEDCOM ROS-F Devices

The following subsections outline the security-related features of RUGGEDCOM ROS-F devices.

CONTENTS

- [Section 2.1, "Product Overview"](#)
- [Section 2.2, "Module Specification"](#)
- [Section 2.3, "Module Interfaces"](#)
- [Section 2.4, "Roles, Services, and Authentication"](#)
- [Section 2.5, "Physical Security"](#)
- [Section 2.6, "Operational Environment"](#)
- [Section 2.7, "Cryptographic Key Management"](#)
- [Section 2.8, "EMI / EMC"](#)
- [Section 2.9, "Self-tests"](#)
- [Section 2.10, "Mitigation of Other Attacks"](#)

Section 2.1

Product Overview

The RUGGEDCOM Ethernet Switches and RUGGEDCOM Serial Device Server are utility-grade, fully-managed Ethernet devices designed to operate reliably in electrically harsh and climatically demanding environments. The devices' rugged hardware design, coupled with the embedded RUGGEDCOM ROS-F[®] (Rugged Operating System) version 4.2.2.F, provides improved system reliability and advanced cybersecurity and networking features. This makes them ideally suited for creating secure Ethernet networks for mission-critical, real-time control applications.

- The **RUGGEDCOM RS416F** ([Figure 1](#)) is a fully-managed serial device server featuring a modular design. The RS416F can be equipped with up to 16 serial ports, and up to 4 switched Ethernet ports



Figure 1: RUGGEDCOM RS416F Serial Device Server

- The **RUGGEDCOM M2100F** (Figure 2) and **RUGGEDCOM M2200F** (Figure 3) are fully-managed, modular, MIL-STD hardened Ethernet switches. The M2100F can be equipped with up to 19 switched Ethernet ports, while the M2200F can be equipped with up to 9 Gigabit Ethernet ports.



Figure 2: RUGGEDCOM M2100F Ethernet Switch



Figure 3: RUGGEDCOM M2200F Ethernet Switch

- The **RUGGEDCOM M969F** (Figure 4) is a 10-port, fully-managed Ethernet switch, providing dual fiber optical Gigabit Ethernet ports and up to 8 Fast Ethernet copper ports in a MIL-STD 901D-rated package. It is IP66/IP67-rated for protection against strong jets of water (IP66) and temporary immersion in water (IP67).



Figure 4: RUGGEDCOM M969F Ethernet Switch

- The **RUGGEDCOM RS900F** and **RUGGEDCOM RS900GF** (both in Figure 5) are fully-managed utility-grade Ethernet switches. The RS900F offers 6 10/100BaseTX ports with an option for 3 additional fiber or copper ports, while the RS900GF provides dual fiber optical Gigabit Ethernet ports and 8 Fast Ethernet copper ports. Both switches provide a high level of immunity to electromagnetic interference and heavy electrical surges typical of environments found on electric utility substations, plant floors, or in curbside traffic control cabinets. An operating temperature range of -40°C to $+85^{\circ}\text{C}$ (-40°F to $+185^{\circ}\text{F}$), together with Hazardous Location certification (Class 1 Division 2), allows the RS900F and RS900GF to be placed in almost any location.



Figure 5: RUGGEDCOM RS900F (Left) and RS900GF (Right) Ethernet Switches

- The **RUGGEDCOM RS940GF** (Figure 6) is a fully-managed Ethernet switch, providing 6 or 8 ports of Gigabit Ethernet. Six 10/100/1000BaseTX triple-speed copper ports are standard. An additional two Gigabit fiber or copper ports can be added. The RS940GF provides a way of connecting a cluster of field devices to a Gigabit Ethernet backbone. The RS940GF provides two fiber optical Gigabit Ethernet ports for creating a fiber optical backbone with high noise immunity and long haul connectivity.



Figure 6: RUGGEDCOM RS940GF Ethernet Switch

- The **RUGGEDCOM RSG2100F** (Figure 7) and **RUGGEDCOM RSG2200F** (Figure 8) are modular Ethernet switches. The RSG2100F features up to 3 Gigabit Ethernet ports and up to 16 Fast Ethernet ports, while the RSG2200F offers up to 9 Gigabit Ethernet ports. Support for front or rear mount connectors, coupled with multiple fiber connector types (including SFP, GBIC, LC, and SC) without loss of port density, makes the RSG2100F and RSG2200F highly versatile and suitable for any application.



Figure 7: RUGGEDCOM RSG2100F Ethernet Switch



Figure 8: RUGGEDCOM RSG2200F Ethernet Switch

- The **RUGGEDCOM RSG2488F** (Figure 9) is the first utility-grade, field-upgradable, Layer 2 Ethernet switch with hot-swappable dual redundant power supplies. The RSG2488F's modular flexibility provides up to 28 non-blocking ports that can be configured as 10/100/1000TX copper or 100FX/1000SX fiber. With its 1U form factor and vertical Gigabit loading design, the RSG2488F provides users with the flexibility and field maintenance simplicity needed to efficiently implement, maintain, and evolve a broadband local area network.



Figure 9: RUGGEDCOM RSG2488F Ethernet Switch

Device management can be accomplished using the following three management interfaces:

- Web Interface – An interactive web-based Graphical User Interface (GUI) over HTTPS accessible remotely over HTTPS via Ethernet ports and optical fiber ports
- Console Interface – An interactive menu-based GUI accessible directly via a direct RS-232 serial console port or over SSH via Ethernet ports and optical fiber ports
- Console CLI – A full-featured command-based interface accessible after accessing the Console Interface and pressing **Ctrl + S**

The RUGGEDCOM ROS-F Devices are validated at the FIPS 140-2 section levels shown in [Table 1](#).

Table 1: Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2

Section	Section Title	Level
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Section 2.2

Module Specification

The RUGGEDCOM ROS-F Devices are hardware cryptographic modules with a multiple-chip standalone embodiment. The overall security level of the modules is 2. The cryptographic modules consist of firmware and hardware components enclosed in a secure, industrially-hardened metal case. The hardware components include a main circuit board and power supplies, with some models being equipped with port interface boards. For all devices, the cryptographic boundary is defined as the outer edge of the chassis (illustrated by the red-dotted line shown in Figure 10 below).

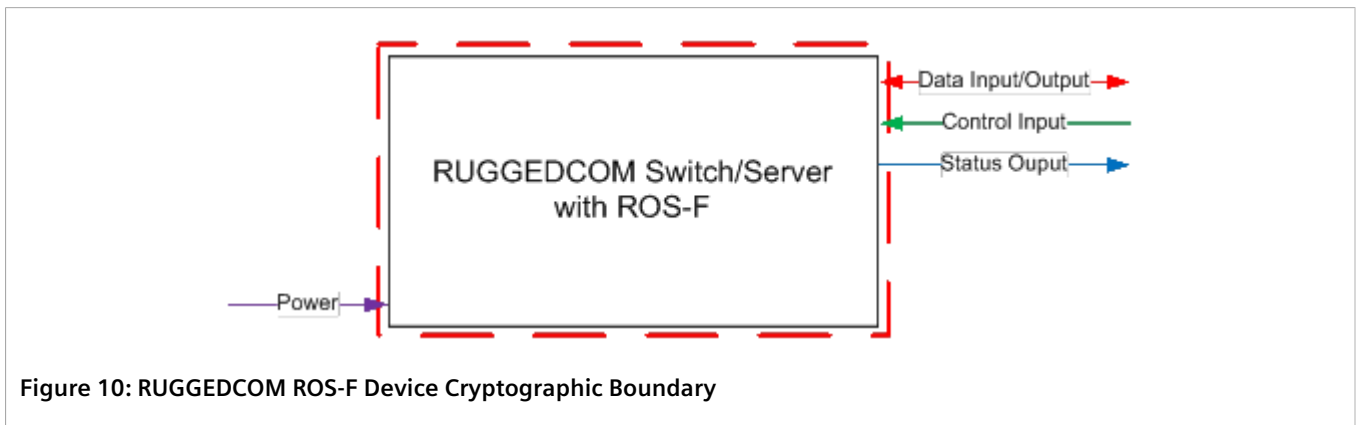


Figure 10: RUGGEDCOM ROS-F Device Cryptographic Boundary

Each module is primarily composed of the following components:

- Processor
- SDRAM
- Flash memory
- Ethernet switch chip
- LEDs
- Failsafe relay

Table 2: RUGGEDCOM ROS-F Devices Hardware Components

Model	Processor	SDRAM	Flash	Ethernet Switch Chip
RS416F	1x Freescale ColdFire MCF5272 (66MHz processor core)	32MB	8MB	1x Marvell 88E6095F

Model	Processor	SDRAM	Flash	Ethernet Switch Chip
M2100F	1x Freescale ColdFire MCF5272 (66MHz processor core)	32MB	8MB	2x Marvell 88E6097F
M2200F	1x Freescale ColdFire MCF5272 (66MHz processor core)	16MB	4MB	1x Marvell 88E6185
M969F	1x Freescale ColdFire MCF5272 (66MHz processor core)	16MB	4MB	1x Marvell 88E6095F
RS900F	1x Freescale ColdFire MCF5272 (66MHz processor core)	32MB	8MB	1x Marvell 88E6095F
RS900GF	1x Freescale ColdFire MCF5272 (66MHz processor core)	32MB	8MB	1x Marvell 88E6095F
RS940GF	1x Freescale ColdFire MCF5272 (66MHz processor core)	16MB	4MB	1x Marvell 88E6185
RSG2100F	1x Freescale ColdFire MCF5272 (66MHz processor core)	32MB	8MB	2x Marvell 88E6097F
RSG2200F	1x Freescale ColdFire MCF5272 (66MHz processor core)	16MB	4MB	1x Marvell 88E6185
RSG2488F	1x Freescale PowerPC MPC8308 (400MHz processor core)	256MB	32MB	1x Broadcom BCM56143

In addition to the primary components listed above, the devices feature a modular design that makes them highly configurable. Each one is specially built according to customer specifications. Because of the modular design, the devices have numerous combinations of interfaces and networking capabilities. However, these customer-orderable components do not provide any additional cryptography-related services or logic. Instead, these components provide options for power and flexible network connectivity. Each available slot must be filled with a line card (or blank) in order to maintain the modules' physical security posture. The selection and configuration of components has no impact on the FIPS-related behavior of the modules. Validation testing was performed on the specific configuration(s) of each device as listed in [Table 3](#) below.

Table 3: RUGGEDCOM ROS-F Devices Tested Configurations

Model	Component Configuration	Component Description
RS416F	A03, B03, C03, D03	4 x Fiber Serial Interface (ST Connector)
	A04, B04, C04, D04	4 x RS232/RS422/RS485 & IRIG-B via DB9 1
	A05, B05, C05, D05	4 x RS232/RS422/RS485 & IRIG-B via RJ45 1
	E01, F01	2 x 10/100Tx RJ45
	E14	1 x IRIG-B in, BNC, 1 x IRIG-B out, BNC (Slot 5 only)
M2100F	A02, B02, C02, D02, G02, H02, J02, K02	2 x 10FL - Multimode, 850nm, ST
	A03, B03, C03, D03, G03, H03, J03, K03	2 x 100FX - Multimode, 1310nm, ST
	A05, B05, C05, D05, G05, H05, J05, K05	2 x 100FX - Singlemode, 1310nm, ST, 20km
	E01	2 x 10/100/1000Tx, Micro-D
M2200F	A01, B01, C01, D01	2 x 10/100/1000Tx, Micro-D
	A02, B02, C02, D02	2 x 1000SX - Multimode, 850nm, LC, 500m
	A04, B04, C04, D04	2 x 1000LX - Singlemode, 1310nm, LC connectors, 25km
	A05, B05, C05, D05	2 x 10/100/1000Tx, Micro-D, with special short jackscrews

Model	Component Configuration	Component Description
M969F	A09	2 x 1000SX Multimode, LC connectors 850nm
RS900F	A09 (Port 7/Port 8)	2 x 100FX - Multimode, 1300nm, ST connector, and 1 x 100FX - Singlemode, Standard 20km
	B03 (Port 9)	1 x 100FX - Multimode, 1300nm, SC connector
RS900GF	A04 (Port 9/Port 10)	Dual 1000LX Singlemode, LC 1310nm, 25km
RS940GF	A03	Dual 1000SX Multimode, LC 850nm 500m
RSG2100F	A01, B01, C01, D01, G01, H01, J01, K01	2 x 10/100Tx RJ45
	A02, B02, C02, D02, G02, H02, J02, K02	2 x 10FL- Multimode, 850nm, ST
	A03, B03, C03, D03, G03, H03, J03, K03	2 x 100FX- Multimode, 1300nm, ST
	A13, B13, C13, D13, G13, H13, J13, K13	2 x 100FX - Singlemode, 1310nm, LC, 90km
	A14, B14, C14, D14, G14, H14, J14, K14	2 x 10/100Tx micro-D
	E01	2 x 10/100/1000Tx RJ45
	F02	1 x 1000SX - Multimode, 850nm, LC, 500m
RSG2200F	A01, B01, C01, D01	2 x 10/100/1000Tx RJ45
	A02, B02, C02, D02	2 x 1000SX - Multimode, 850nm, LC, 500m
	A06, B06, C06, D06	2 x 1000LX - Singlemode, 1310nm, LC connectors, 25 km
	A08, B08, C08, D08	2 x 1000SX SFP - Multimode, 850nm, LC, 500m
	E20	1 x 100FX - Multimode, 1300nm, MTRJ
RSG2488F	A01, B01, C01, D01, E01, F01	4 x 10/100/1000Tx RJ45
	A04, B04, C04, D04, E04, F04	4 x 10/100/1000Tx M12 X-Coded
	A05, B05, C05, D05, E05, F05	4 x 1000SX - Multimode, 850nm, LC, 500m
	A09, B09, C09, D09, E09, F09	4 x 1000SX SFP - Multimode, 850nm, LC, 500m
	A24, B24, C24, D24, E24, F24	4 x 1000LX Singlemode, 1310nm, LC, 25km
	A59	1 x Precision Time Protocol (PTP) - Module: GPS in, IRIG-B AM/TTL, IN/OUT
	G61, H61	2 x 10/100/1000Tx RJ45
	G64, H64	2 x 10/100/1000Tx M12 X-Coded

Appendix A specifies the non-security relevant line card components of the remaining configurations for each device that are excluded from FIPS 140-2 requirements. Each component of the line card, except the faceplate, is excluded from FIPS 140-2 requirements because they do not provide any security relevant functionality. Since tamper evident seals are applied and necessary for physical security protection, the faceplates are security relevant and are required to meet the FIPS 140-2 requirements.

The modules implement the FIPS-Approved algorithms listed in [Table 4](#) below.

Table 4: FIPS-Approved Algorithm Implementations

CAVP Certificate		Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
PowerPC	ColdFire					
4030 [http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#4030]	4037 [http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#4037]	AES	FIPS 197 NIST SP 800-38D	ECB ^a , CBC, GCM	128, 256	Encryption/ Decryption
			FIPS 197	CTR	256	
2078 [http://csrc.nist.gov/groups/STM/cavp/documents/dss/rsanewval.html#2078]	2072 [http://csrc.nist.gov/groups/STM/cavp/documents/dss/rsanewval.html#2072]	RSA	FIPS 186-4	-	2048, 3072	Key Generation
				SHA-1 ^b , SHA-224, SHA-256, SHA-384, and SHA-512 (PKCS #1 v1.5)	2048, 3072	Signature Generation and Verification
				SHA-256 (PSS)	2048, 3072	Signature Verification
899 [http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsanewval.html#899]	903 [http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsanewval.html#903]	ECDSA	FIPS 186-4	-	P-256, P-384, P-521	Key pair generation/ public key validation
3336 [http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.html#3336]	3329 [http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.html#3329]	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	Message Digest
2631 [http://csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html#2631]	2635 [http://csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html#2635]	HMAC ^c	FIPS 198-1	SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	-	Message Authentication
1204 [http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html#1204]	1207 [http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgnewval.html#1207]	DRBG	NIST SP 800-90A	CTR_based	256	Deterministic Random Bit Generation
Vendor Affirmed	Vendor Affirmed	CKG ^d	NIST SP 800-133	-	-	Key Generation
858 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#858]	863 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#863]	CVL for ECC CDH and KAS for ECC	NIST SP 800-56A	-	ECC CDH: P-521 KAS ECC: ^e EC: P-256/ SHA-256 ED: P-384/ SHA-384 EE: P-521/ SHA-512	Key Agreement
859 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#859]	861 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#861]	CVL for Transport Layer Security	NIST SP 800-135 Rev. 1	-	-	Key Derivation

CAVP Certificate		Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
PowerPC	ColdFire					
		(TLS) 1.0/1.1, 1.2 ^f				
		CVL for Secure Shell (SSH) ^g				
876 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#876]	862 [http://csrc.nist.gov/groups/STM/cavp/documents/components/componentnewval.html#862]	CVL for RSA Decryption Primitive	FIPS 186-4	-	2048	Data Decryption

^a CAVP testing was performed on AES ECB mode but is not implemented in the module.

^b SHA-1 shall not be used for digital signature generation with the exception as specified in SP 800-52 REV1 and SP 800-57 Part 3 REV1.

^c CAVP testing was performed on HMAC with SHA-224 and SHA-512 but is not implemented in the module.

^d In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

^e Section 5.6.2.5, "ECC - Full Public Key Validation" and section 5.6.2.6, "ECC - Partial Public Key Validation."

^f The CVL for TLS 1.0/1.1 does not allow testing of only one version of TLS. Because of this, TLS 1.0 is listed on the CAVP certificate but is not supported by the RUGGEDCOM ROS-F Devices.

^g The TLS and SSH protocols have not been reviewed or tested by the Cryptographic Algorithm Validation Program (CAVP) or CMVP.

The modules also employ the non-FIPS-Approved algorithms listed in [Table 5](#) below (all of which are allowed for use in a FIPS-Approved mode of operation).

Table 5: FIPS Allowed Algorithm Implementations

Algorithm	Caveat	Use
Diffie-Hellman (DH)	Key agreement; Key establishment methodology provides 112 bits of encryption strength	Used for key agreement during SSH and TLS (2048-bit keys)
ECDH	Key agreement; Key establishment methodology provides between 128 and 256 bits of encryption strength	Used for key agreement during SSH and TLS (supported curves of P-256, P-384, P-521)
RSA	Key encapsulation; Key establishment methodology provides 112 or 128 bits of encryption strength	Used for key establishment during TLS (2048-bit and 3072-bit keys)
Non-Deterministic Random Number Generator (NDRNG)	-	Used for gathering entropy (the module generates 384 bits of entropy for key generation). All operations requiring entropy are blocked and made to wait until at least 4,096 bits have been collected in the entropy pool. If 4,096 bits are present in the entropy pool, the bits will be extracted, hashed using SHA-384, and then the CTR_DRBG is seeded with 384 bits of entropy.

Section 2.3

Module Interfaces

The modules' physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface

- Data Output Interface
- Control Input Interface
- Status Output Interface

Table 6 lists the physical ports/interfaces available in the switches and also provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2.

Table 6: FIPS 140-2 Logical Interface Mappings

Device	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
RS416F	Serial port	up to 16	Data Input, Data Output
	Ethernet port	up to 4	Data Input, Data Output, Control Input, Status Output
	IRIG-B port (BNC connectors)* ^h	2 or 4	Data Input, Data Output
	Mode button	1	Control Input
	Failsafe relay	1	Status Output
	Port status indicator LED	20	Status Output
	Display mode LED (status, duplex, and speed)	3	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
	Power supply port	2	Power
M2100F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper or fiber)	up to 3	Data Input, Data Output, Control Input, Status Output
	Fast Ethernet port (copper or fiber)	up to 16	Data Input, Data Output, Control Input, Status Output
	Mode button	1	Control Input
	Failsafe relay	1	Status Output
	Port status indicator LED	32	Status Output
	Display mode LED (status, duplex, and speed)	3	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
	Power supply port	2	Power
M2200F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper or fiber)	up to 9	Data Input, Data Output, Control Input, Status Output
	Mode button	1	Control Input
	Failsafe relay	1	Status Output
	Port status indicator LED	32	Status Output
	Display mode LED (status, duplex, and speed)	3	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
Power supply port	2	Power	

Device	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
M969F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Fast Ethernet port (copper)	8	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (fiber)	2	Data Input, Data Output, Control Input, Status Output
	Failsafe relay	1	Status Output
	Link LED	10	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
	M23 power supply connector	1	Power
RS900F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Fast Ethernet port (copper)	6	Data Input, Data Output, Control Input, Status Output
	Reset button	1	Control Input
	Failsafe relay	1	Status Output
	Power LED	1	Status Output
	Alarm LED	1	Status Output
	Power supply terminal block	1	Power
RS900GF	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Fast Ethernet port (copper)	8	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (fiber)	2	Data Input, Data Output, Control Input, Status Output
	Failsafe relay	1	Status Output
	Power LED	1	Status Output
	Alarm LED	1	Status Output
	Power supply terminal block	1	Power
RS940GF	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper)	6	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (fiber or copper)*	2	Data Input, Data Output, Control Input, Status Output
	Failsafe relay	1	Status Output
	Power LED	1	Status Output
	Alarm LED	1	Status Output
	Power supply terminal block	1	Power
RSG2100F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Fast Ethernet port (copper or fiber)	up to 16	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper or fiber)	up to 3	Data Input, Data Output, Control Input, Status Output
	Mode button	1	Control Input
	Failsafe relay	1	Status Output

Device	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
	Port status indicator LED	32	Status Output
	Display mode LED (status, duplex, and speed)	3	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
	Power supply port	2	Power
RSG2200F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper and/or fiber)	up to 9	Data Input, Data Output, Control Input, Status Output
	Mode button	1	Control Input
	Failsafe relay	1	Status Output
	Port status indicator LED	32	Status Output
	Display mode LED (status, duplex, and speed)	3	Status Output
	Power LED	2	Status Output
	Alarm LED	1	Status Output
	Power supply port	2	Power
RSG2488F	Serial console port	1	Data Input, Data Output, Control Input, Status Output
	Ethernet console port	1	Data Input, Data Output, Control Input, Status Output
	Gigabit Ethernet port (copper and/or fiber)	up to 28	Data Input, Data Output, Control Input, Status Output
	IRIG-B port (BNC connectors)*	4	Data Input, Data Output
	GPS port (BNC connectors)*	1	Data Input
	Failsafe relay	1	Status Output
	Power module indicator LED	4	Status Output
	Alarm LED	1	Status Output
	Speed LED	1	Status Output
	Link/activity/sync LED	28	Status Output
	Power supply port	2	Power

^h* - optional

As described above, the modules have a number of LEDs that indicate various states and conditions. The descriptions for the LEDs are listed in [Table 7](#) below.

Table 7: Module LED Descriptions

Switch	LED	State	Description
M2100F M2200F RSG2100F RSG2200F	Port Status Indicators (Status Mode)	Green (Solid)	Link detected
		Green (Blinking)	Link activity
		Off	No link detected
	Port Status Indicators (Duplex Mode)	Green (Solid)	Full duplex mode
		Orange (Solid)	Half-duplex mode

Switch	LED	State	Description
	Port Status Indicators (Speed Mode)	Off	No link detected
		Green (Solid)	The port is operating at 1000 Mbps
		Green (Blinking)	The port is operating at 100 Mbps
		Orange (Solid)	The port is operating at 10 Mbps
	Display Mode (Status)	Off	No link detected
		On	When Status mode is selected (ON), the Port Status Indicator LEDs indicate when ports are active. When Status mode is not selected (OFF), these Port Status Indicator LEDs display either Duplex or Speed outputs.
	Display Mode (Duplex)	Off	When Duplex mode is selected (ON), the Port Status Indicator LEDs indicate when ports are operating in full or half-duplex mode. When Duplex mode is not selected (OFF), these Port Status Indicator LEDs display either Status or Speed outputs.
		On	
	Display Mode (Speed)	Off	When Speed mode is selected (ON), the Port Status Indicator LEDs indicate the port speed. When Speed mode is not selected (OFF), these Port Status Indicator LEDs display either Duplex or Status outputs.
		On	
	Power	Green (On)	The power supply is installed and supplying power
		Red (On)	The power supply fails
		Off	No power supply is installed
	Alarm	On	An alarm condition exists
		Off	No alarm condition exists
RS900F RS900GF RS940GF	Power	On	Power is being supplied to the device
		Off	No power is being supplied to the device
	Alarm	On	An alarm condition exists
		Off	No alarm condition exists
	Speed	Yellow	The port is operating at 100 Mbps
		Off	The port is operating at 10 Mbps
	Link/Activity	Yellow (Solid)	Link established
		Yellow (Blinking)	Link activity
		Off	No link detected
M969F	Link	Yellow (Solid)	Link detected
		Yellow (Blinking)	Link activity
		Off	No link detected
	Power	On	Power is being supplied to the device
		Off	No power is being supplied to the device
	Alarm	Red (On)	An alarm condition exists
		Off	No alarm condition exists

Switch	LED	State	Description
RSG2488F	Power Module Indicator (Top)	On	Power is being supplied to the device
		Off	No power is being supplied to the device
	Power Module Indicator (Bottom)	On	Power is being received by the module
		Off	No power is being received by the module
	Alarm	On	An alarm condition exists
		Off	No alarm condition exists
	Speed (RJ45)	Yellow (Solid)	The port is operating at 1000 Mbps
		Off	The port is operating at 10 or 100 Mbps
	Link/Activity (RJ45)	Yellow (Solid)	Link established
		Yellow (Blinking)	Link activity
		Off	No link detected
	Link/Activity (M12)	Green (Solid)	Link established
		Green (Blinking)	Link activity
		Off	No link detected
	Sync (BNC)	Green (On)	Signal locked
		Amber/Yellow (On)	Holdover
		Red (On)	Error
		Off	No signal detected
RS416F	Port Status Indicators (Status Mode for Ethernet ports)	Green (Solid)	Link detected
		Green (Blinking)	Link activity
		Off	No link detected
	Port Status Indicators (Duplex Mode for Ethernet ports)	Green (Solid)	Full duplex mode
		Orange (Solid)	Half-duplex mode
		Off	No link detected
	Port Status Indicators (Speed Mode for Ethernet ports)	Green (Solid)	The port is operating at 100 Mbps
		Orange (Solid)	The port is operating at 10 Mbps
		Off	No link detected
	Port Status Indicators (Status Mode for serial ports)	Green (Blinking)	Traffic detected
		Off	No traffic
	Port Status Indicators (Duplex Mode for serial ports)	Green (Solid)	Full duplex mode
		Orange (Solid)	Half-duplex mode
		Off	No link detected
	Port Status Indicators (Speed Mode for serial ports)	Green (Solid)	>19200 to <57600 bps
		Green (Blinking)	57600 bps or higher

Switch	LED	State	Description
		Orange (Solid)	<19200 bps
		Off	No link detected
Display Mode (Status)		On	When Status mode is selected (ON), the Port Status Indicator LEDs indicate when ports are active. When Status mode is not selected (OFF), these Port Status Indicator LEDs display either Duplex or Speed outputs.
		Off	
Display Mode (Duplex)		On	When Duplex mode is selected (ON), the Port Status Indicator LEDs indicate when ports are operating in full or half-duplex mode. When Duplex mode is not selected (OFF), these Port Status Indicator LEDs display either Status or Speed outputs.
		Off	
Display Mode (Speed)		On	When Speed mode is selected (ON), the Port Status Indicator LEDs indicate the port speed. When Speed mode is not selected (OFF), these Port Status Indicator LEDs display either Duplex or Status outputs.
		Off	
Power		Green (On)	The power supply is installed and supplying power
		Red (On)	The power supply fails
		Off	No power supply is installed
Alarm		On	An alarm condition exists
		Off	No alarm condition exists
RJ45 port (Speed)		Yellow	The port is operating at 1000 Mbps
		Off	The port is operating at 10 or 100 Mbps
RJ45 port (Link/Activity)		Yellow (Solid)	Link established
		Yellow (Blinking)	Link activity
		Off	No link detected
Serial port		Green	Link activity detected
		Off	No link detected
IRIG-B (BNC connections' Sync LED)		Off	No IRIG-B signal detected
		Red	Errors detected in received IRIG-B signal
		Amber/Yellow	Holdover (GPS lock has been achieved, but the receiver no longer sees the minimum number of required satellites)
		Green	Received IRIG-B signal is good

Section 2.4

Roles, Services, and Authentication

The sections below describe the modules' roles and services and define the authentication methods employed.

CONTENTS

- [Section 2.4.1, "Authorized Roles"](#)
- [Section 2.4.2, "Operator Services"](#)

- [Section 2.4.3, "Maintenance Mode"](#)
- [Section 2.4.4, "Additional Services"](#)
- [Section 2.4.5, "Authentication"](#)

Section 2.4.1

Authorized Roles

The modules support four roles that operators may assume: Crypto Officer (CO), User, Guest, and Maintenance.

- **Crypto Officer**

The CO role is responsible for initializing the modules for first use (including the configuration of passwords, certificates, public and private keys, and other CSPs). The CO is also responsible for the management and zeroization of all keys and CSPs. The CO is the only operator that can configure the modules into FIPS-Approved mode of operation. (**NOTE:** This role designation maps to the modules' "Admin" account.)

The CO also has access to all User and Guest services.

- **User**

The User role has the privileges to change basic settings, show module statistics, show the current status of the modules, clear statistics, and reset alarms. (**NOTE:** This role designation maps to the modules' "Operator" account.)

- **Guest**

The Guest role has the read-only privileges and can view only a limited selection of settings. (**NOTE:** This role designation maps to the modules' "Guest" account.)

- **Maintenance**

The Maintenance role has access to the module's hardware testing and diagnostics services. Please see [Section 2.4.3, "Maintenance Mode"](#) below for details.

Module operators can connect to the modules remotely via secure TLS and SSH sessions, while local sessions occur over the serial console port. The modules are capable of supporting multiple CO and multiple User/Guest operator sessions at any given time. Each remote session is secured by the session protocol and the operating system (OS) process and memory management functions, and is distinguished by session information. Local sessions are secured via the direct connection over the serial console port.

Section 2.4.2

Operator Services

Descriptions of the services available to module operators in the normal operational mode are provided in the [Table 8](#) below. The keys and CSPs listed in [Table 8](#) indicate the type of access required using the following notation:

- **R – Read**

The CSP is read

- **W – Write**

The CSP is established, generated, modified, or zeroized

- **X – Execute**

The CSP is used within an Approved or Allowed security function or authentication mechanism

Table 8: Operational Mode Services

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
Manage the flash file system	✓			View information about files in flash; defragment the flash file system	Command	Command response/ Status output	None
View product information	✓	✓	✓	View information about the device	Command	Command response/ Status output	None
View CPU diagnostics	✓	✓	✓	View CPU diagnostic information	Command and parameters	Command response/ Status output	None
View power supply status (RSG2488F only)	✓	✓	✓	View the current status of the power supplies	Command and parameters	Command response/ Status output	None
Restore factory defaults	✓			Restore the module to its original factory default settings	Command and parameters	Command response	CO Password – W User Password – W Guest Password – W
Manage SSL certificates	✓			Manage SSL certificates	Command and parameters	Command response/ Status output	CA Public Key – R/W TLS RSA Public Key – R/W TLS RSA Private Key – W
Manage SSH host key pairs	✓			Add or update SSH host keys	Command and parameters	Command response/ Status output	SSH RSA Public Key – R/W SSH RSA Private Key – R/W
Manage SSH public keys	✓			Add, view, update, or delete SSH public keys	Command and parameters	Command response/ Status output	SSH Public Key – R/W
Upload/download files	✓	✓		Download files from the module to a host computer using XMODEM via serial console	Command and parameters	Command response/ Status output	None
	✓			Upload files to the module from a host computer using XMODEM via serial console			
Manage logs	✓			View, clear, configure, and manage local logs and logging	Command and parameters	Command response/ Status output	None
Manage Ethernet stats	✓	✓		View Ethernet statistics; view Ethernet port statistics; clear Ethernet port statistics; view Ethernet MgmtPort statistics; clear Ethernet MgmtPort statistics	Command and parameters	Command response/ Status output	None

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
	✓			Configure RMON history controls; configure RMON alarms; configure RMON events			
Manage Ethernet ports	✓	✓		Configure port mirroring; reset port(s); view port status; view mgmt port status	Command and parameters	Command response/ Status output	None
	✓			Configure port parameters; configure port rate limiting; configure/view cable diagnostics parameters; clear cable diagnostics statistics; configure link detection			
Manage IP Interfaces	✓			Configure the Management or Switch IP interfaces	Command and parameters	Command response/ Status output	None
Manage IP gateways	✓			View, add, and delete IP gateways	Command and parameters	Command response/ Status output	None
Configure IP services	✓			Configure the Management or Switch IP interfaces	Command and parameters	Command response/ Status output	None
Manage remote monitoring	✓			Collect and view historical statistics related to the performance and operation of Ethernet ports	Command and parameters	Command response/ Status output	None
Reboot/Reset module	✓	✓		Reboot/reset the module via CLI (zeroizes keys/CSPs stored in SDRAM and performs self-tests)	Command	Command response/ Status output	All keys and CSPs stored in SDRAM – W
Clear data	✓			Clear banner file, system log, and configuration data and zeroize keys/CSPs in flash	Command	Command response/ Status output	All keys and CSPs stored in flash and SDRAM (except the Firmware Load Authentication Key, CA Public Key, and SSH Public Key) – W
Configure system information	✓			Configure basic information used to identify the device, its location, and its owner	Command and parameters	Command response/ Status output	None
Customize login screen	✓			Set a custom welcome message	Command and parameters	Command response/ Status output	None

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
Manage users	✓			Configure the three pre-defined user accounts	Command and parameters	Command response/ Status output	CO Password – R/W/X User Password – R/W/X Guest Password – R/W/X
Change password	✓			Modify existing passwords	Command and parameters	Command response/ Status output	CO Password – R/W User Password – R/W Guest Password – R/W
Enable/disable the web interface	✓			Enable/disable the web interface	Command and parameters	Command response/ Status output	None
Manage alarms	✓	✓		View latched alarms; clear latched alarms	Command and parameters	Command response/ Status output	None
	✓			Configure alarms			
Manage configuration file	✓			Download, store, and update device configuration file	Command and parameters	Command response/ Status output	None
Configure DHCP Relay Agent	✓			Set the DHCP server address and client ports	Command and parameters	Command response/ Status output	None
Manage VLANs	✓	✓		View VLAN summary	Command and parameters	Command response/ Status output	None
	✓			Configure global VLAN parameters; configure static VLANs; configure port VLAN parameters			
Manage Spanning Tree Protocol (STP)	✓	✓		Clear spanning tree statistics; view bridge RSTP statistics; view port RSTP statistics; view bridge MSTI statistics; view port MSTI statistics	Command and parameters	Command response/ Status output	None
	✓			Configure port RSTP parameters; configure eRSTP parameters; configure MST region identifier; configure bridge MSTI parameters; configure port MSTI parameters			
Manage Classes of Service (CoS)	✓			Configure CoS mappings	Command and parameters	Command response/ Status output	None
Manage Media Access Control (MAC) addresses	✓	✓		Purge MAC address table	Command and parameters	Command response/ Status output	None
	✓			Configure MAC address learning options; configure flooding options;			

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
				configure static MAC addresses			
Manage time services	✓			Manage time services	Command and parameters	Command response/ Status output	None
Manage network discovery	✓	✓		View LLDP global remote statistics; view LLDP neighbor information; view LLDP statistics	Command and parameters	Command response/ Status output	None
	✓			Configure global LLDP parameters; configure port LLDP parameters			
Manage multicast filtering	✓	✓		View IGMP group membership; view IGMP multicast forwarding; view multicast group summary	Command and parameters	Command response/ Status output	None
	✓			Configure IGMP parameters; configure global GMRP parameters; configure port GMRP parameters; configure static multicast groups			
Manage port security	✓	✓		View authorized MAC addresses	Command and parameters	Command response/ Status output	None
	✓			Configure ports security; configure 802.1X parameters			
Manage link aggregation	✓			Configure port trunks	Command and parameters	Command response/ Status output	None
Enter maintenance mode (zeroize)	✓			Reboot into the modules' maintenance mode (also zeroizes all keys and CSPs in flash and SDRAM except the Firmware Load Authentication Key, CA Public Key, and SSH Public Key)	Command and parameters	Command response	All keys and CSPs stored in flash and SDRAM (except the Firmware Load Authentication Key, CA Public Key, and SSH Public Key) – W
Upgrade/downgrade firmware	✓			Load new firmware and perform an integrity test using an RSA digital signature	Command	Command response/ Status output	Firmware Load Authentication Key – R/X
Perform self-tests on-demand	✓			Perform self-tests on-demand via CLI (zeroizes keys/CSPs stored in SDRAM)	Command	Command response/ Status output	All keys and CSPs stored in SDRAM – W

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
Show settings/status	✓	✓	✓	Show the system status, Ethernet status, alarms, system identification and configuration settings of the module	Command	Command response/ Status output	None
Terminate sessions	✓	✓	✓	Terminate an operator's own user session	Command	Command response/ Status output	None
Run commands/scripts	✓			Run commands or script files (text files containing a list of CLI commands to execute in sequence)	Command	Command response/ Status output	None
Perform network diagnostics	✓	✓	✓	Monitor connections, Ethernet ports, STP, and VLANs	Command	Command response/ Status output	None
Establish TLS session	✓	✓	✓	Establish web session using TLS and perform any of the services listed above	Command	Command response/ Status output	CO Password – X User Password – X Guest Password – X CA Public Key – R/X TLS RSA Public Key – R/W/X TLS RSA Private Key – W/X TLS DH Public Key – R/W/X TLS DH Private Key – W/X TLS ECDH Public Key – R/W/X TLS ECDH Private Key – W/X TLS Session Key – R/W/X TLS ECDSA Public Key – R/W/X TLS Authentication Key – R/W/ X DRBG Key – R/W/X DRBG 'V' Value – R/W/X DRBG Seed – R/W/X Entropy Input String – R/W/X
Establish SSH session	✓	✓	✓	Establish remote session using SSH protocol and perform any of the services listed above	Command	Command response/ Status output	CO Password – X User Password – X Guest Password – X SSH Public Key – R/X SSH Authentication Key – R/W/ X SSH Session Key – R/W/X SSH RSA Public Key – R/W/X SSH RSA Private Key – W/X SSH DH Public Key – R/W/X SSH DH Private Key – W/X SSH ECDH Public Key – R/W/X

Service	Operator			Description	Input	Output	Key/CSP and Type of Access
	CO	User	Guest				
							SSH ECDH Private Key – W/X SSH ECDSA Public Key – R/W/X DRBG Key – R/W/X DRBG 'V' Value – R/W/X DRBG Seed – R/W/X Entropy Input String – R/W/X
Perform encryption/ decryption service	✓	✓	✓	Encrypt or decrypt user data, keys, or management traffic	Command and parameters	Command response	TLS Session Key – X SSH Session Key – X IV – R/W DRBG Key – R/W/X DRBG 'V' Value – R/W/X DRBG Seed – R/W/X Entropy Input String – R/W/X
Authenticate data traffic	✓	✓	✓	Authenticate user data or management traffic	Command and parameters	Command response	TLS Authentication Key – X SSH Authentication Key – X
Enable the factory mode	✓			Enables factory mode, which includes several factory- level commands used for testing and troubleshooting	Command	Command response/ Status output	None
Display random numbers	✓			Display seeds or random numbers	Command	Command response/ Status output	None

All services listed in [Table 8](#) above require the operator to assume an authorized role, and the operator must authenticate to the module prior to being granted access to any of these services. For a full listing of module services, please refer to the *Siemens RUGGEDCOM ROS-F v4.2.2.F User Guide* available online and upon request from Siemens Customer Service.

Section 2.4.3

Maintenance Mode

The modules support a maintenance mode, which can only be accessed via the Console CLI shell. Maintenance mode consists of hardware testing and diagnostics services. The modules automatically boot into maintenance mode as a result of experiencing a critical error (see [Section 2.9.4, "Self-test Error Behavior and Recovery"](#)).

Entering maintenance mode causes a system reboot, which zeroizes all keys and CSPs in RAM. It then zeroizes the configuration, SSH host key pair, and TLS server certificate files in Flash memory. Further, all networking ports are placed in loopback, inhibiting all Ethernet traffic. The Web Interface will not respond, and remote logging will no longer occur.

[Table 9](#) lists the services available while in the maintenance mode.

Table 9: Maintenance Mode Services

Service	Description	Input	Device										Output	CSP and Type of Access	
			M2100F	M2200F	M969F	RS900F	RS900GF	RS940GF	RS92100F	RS92200F	RS92488F	RS416F			
Test hardware	Run the built in hardware self-tests; verify all previously read hardware IDs remain the same	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Clear device data	Clear the user data and logs (system and crash logs) from the device	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Clear screen	Clear the screen	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
View file directory	Print a list of the file directories to the screen	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Ethernet management	Manipulates Ethernet port PHY and forwarding capabilities; start a loopback test on the specified Ethernet port(s)	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Terminate session	Terminate this command line session	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Flash files	Flash file system commands	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Help information	Print a list of all commands and their information	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test crypto	Execute cryptographic algorithm self-tests	Command										✓		Command response/Status output	None
Test BCM	BCM diagnostic shell commands	Command										✓		Command response/Status output	None
Monitor BCM	Monitor BCM statistic counters	Command										✓		Command response/Status output	None
Test FPGA	Timesync FPGA debug interface; test Timesync FPGA	Command										✓		Command response/Status output	None
Test JTAG chain	Invoke self-tests on jtag chain; programs the PFGA	Command	✓	✓						✓	✓		✓	Command response/Status output	None
Test Marvell switch	Marvell Ethernet Switch register diagnostics	Command	✓	✓	✓	✓	✓	✓	✓	✓			✓	Command response/Status output	None

Service	Description	Input	Device										Output	CSP and Type of Access	
			M2100F	M2200F	M969F	RS900F	RS900GF	RS940GF	RSG2100F	RSG2200F	RSG2488F	RS416F			
Display SFP information	Displays SFP device data	Command										✓	✓	Command response/Status output	None
Test SPI	Run self-tests on SPI Flash device; read/write via SPI	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Show user spurious interrupt count	Display user spurious interrupt count	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Read file	Display the contents of a text file	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Show version	Print software versions	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test watchdog	Provides the ability to test watchdog(s)	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test clock	Run clock synthesizer diagnostics; execute clock synthesizer self-test; run Real-Time Clock (RTC) register diagnostics and test the RTC memory	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test memory	Run EEPROM diagnostics; execute EEPROM self-test; execute memory read/write tests; execute flash device self-test	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test temperature sensors	Execute temperature sensor self-test	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test power supply	Execute power supply self-tests; clear data log in power supply board; run power supply sequencer register diagnostics; execute power supply sequencer self-test	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Test LEDs	Execute LED self-tests; read and display LED Panel Control registers	Command	✓	✓						✓	✓	✓	✓	Command response/Status output	None
Test I2C	Execute I2C self-tests; read/write via I2C	Command	✓	✓						✓	✓	✓	✓	Command response/Status output	None
Test I/O pins	Execute I/O self-tests	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None

Service	Description	Input	Device								Output	CSP and Type of Access		
			M2100F	M2200F	M969F	RS900F	RS900GF	RS940GF	RS92100F	RS92200F			RS92488F	RS416F
Test SMI ⁱ	Use the SMI interface diagnostics; test SMI interface by writing and reading SMI device registers	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None
Reset switch	Perform a hard reset of the module	Command	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Command response/Status output	None

ⁱ Serial Management Interface

As none of the available services modify, substitute, or disclose keys and CSPs, module operators assume a maintenance role implicitly when transitioning to the maintenance mode. However, the Crypto Officer can also directly access the maintenance mode. Direct access to this mode requires the use of the Crypto Officer’s username and password, and is accomplished by doing the following:

1. Connect to the device via the Console Interface
2. Log in to the device as a CO via the Console Interface
3. Press **CTRL+S** to access the Console CLI shell
4. At the Console CLI prompt, enter “factory”
5. When prompted, answer “yes” and enter the CO password
6. At the Console CLI prompt, enter “maintenance”

To exit from the maintenance mode, the module must be reset/rebooted normally, and the CO must re-commission the module to bring it back to a normal operational state.

Section 2.4.4

Additional Services

The modules provide a limited number of services for which the operator is not required to assume an authorized role. [Table 10](#) lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table modify, disclose, or substitute cryptographic keys and CSPs or otherwise affect the security of the modules.

Table 10: Additional Services

Service	Description	Input	Output	Key/CSP and Type of Access
Authenticate operator	Log into the module	Command	Status output	CO Password – R/X User Password – R/X Guest Password – R/X
Reboot module	Reboot the module (zeroizes keys/CSPs stored in SDRAM and performs self-tests on demand)	Power cycle the module using power connectors or reset/mode button (where available)	Status output	All keys and CSPs stored in SDRAM – W

Section 2.4.5

Authentication

The modules support role-based authentication. Role assumption is explicit, and is based on the authentication credential employed. Module operators must authenticate to the module to assume an authorized role and access module services. When changing roles, the operator must first log out of their current role, and then re-authenticate to the module to assume the new role.

All operators authenticate to the module using a username and password. The password has a configurable minimum length that must be set to 8 (see [Section 3.1, "Initial Setup"](#) below), and may contain any combination of letters (uppercase and lowercase), digits (0 – 9), and special characters ("!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", "~", "`", "-", "_", "=", "+", "\\", "|", "]", "}", "[", "{", " ", "?", ";", ":", " ", "?", ".", ">", "<"), allowing for a total character space of 94 characters.

The modules enforce protection mechanisms against brute force attacks. In the module's default configuration, for each operator interface (TLS, SSH, and serial), the module allows 10 password authentication failures in a period of 5 minutes (the first authentication attempt starts a 5-minute timer). Every authentication attempt on that interface from the 11th onward is rejected for the lockout period of 60 minutes, even if the password is correct. The failure counter resets to 0 once the timer expires. Thus, an operator can make a maximum of 30 total authentication attempts in 5 minutes. If all 30 attempts fail, then the operator account is locked out across all interfaces.

Operators can also authenticate to the module using RSA public keys when connecting via SSH or TLS. This key can be 2048 or 3072 bits in length. [Table 11](#) provides the strength of the authentication mechanisms used by the modules.

Table 11: Authentication Mechanism Used by the Modules

Authentication Type	Strength
Password	<p>Once properly configured, the minimum length of the password is 8 characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. Assuming a minimum password length of 8 characters, the chance of a random attempt falsely succeeding is:</p> <ul style="list-style-type: none"> • 1: (94⁸), or • 1: 6,095,689,385,410,816 • Which is less than 1:1,000,000 as required by FIPS 140-2 <p>In a 5-minute window, the module limits the number of failed authentication attempts to 30 (10 per interface) before locking the account across all interfaces for 60 minutes. Thus, assuming all 30 attempts are made in one minute, the probability that a random attempt will succeed or a false acceptance will occur in one minute is:</p> <ul style="list-style-type: none"> • 1: (94⁸ / 30), or • 1: 203,189,646,180,360 • Which is less than 1:100,000 as required by FIPS 140-2
Public Key	<p>The RSA public key used for public key authentication can be 2048 or 3072 bits, yielding an equivalent 112 or 128 bits of strength (respectively). Assuming the minimum key size, the chance of a random authentication attempt falsely succeeding is:</p> <ul style="list-style-type: none"> • 1: (2¹¹²), or • 1: 5.1922968585348276285304963292201e+33 • Which is less than 1:1,000,000 as required by FIPS 140-2 <p>The number of authentication attempts per minute is limited by the bandwidth available over the serial connection, which is a maximum of 115,200 bits per second (or 6,912,000 bits per minute). For a 112-bit key, this results in no more than 61,714 authentication attempts per minute. Thus, the probability that a random attempt will succeed or a false acceptance will occur in one minute is:</p> <ul style="list-style-type: none"> • 1: (2¹¹² / 61,714), or • 1: 84,134,829,350,468,736,891,637,170,321 • Which is less than 1:100,000 as required by FIPS 140-2

The feedback of authentication data to a module operator is obscured during authentication. The modules provide feedback by displaying a “rounded dot” (•) symbol when an operator is entering his password via the Web GUI, and an “x” symbol when using the Console Interface or Console CLI over a serial port. No feedback is provided when authenticating via the Console Interface or Console CLI over an SSH connection.

The modules provide the ability for an operator to change roles and require re-authentication of an operator to assume a new role. In order to change roles, an operator is required to first log out and then log in with an account with appropriate permissions for the desired role.

The modules do not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Only an authenticated CO can modify operator authentication credentials.

Section 2.5

Physical Security

Each of the RUGGEDCOM ROS-F Devices consists of production-grade components that include standard passivation techniques. Each device is encased in a hard metal enclosure (the M969F and RSG2488F enclosures are cast aluminum, while the remaining switch/server enclosures are galvanized steel).

There are only a limited set of ventilation holes provided in the module enclosures. Internal baffles cover the ventilation holes, which makes it impossible to view internal components of the module. Tamper-evident seals are applied to the enclosures to provide physical evidence of unauthorized attempts to open the enclosure or remove module components. The tamper-evident seals must be inspected periodically for signs of tampering. The placement of the tamper-evident seals can be found in [Chapter 3, Secure Operation](#) of this document.

Note that no additional labels are provided upon receipt. Further additional labels cannot be ordered from Siemens. Thus, if any evidence of tampering is observed on the module enclosures or tamper-evident seals, the modules shall be considered to be in a non-compliant state. Upon such discovery, the CO shall immediately take the module out of operation and return to Siemens.

Section 2.6

Operational Environment

The modules employ a non-modifiable operating environment. Only the modules’ RUGGEDCOM ROS-F firmware is executed by their processors. The modules do not provide a general-purpose operating system to module operators.

Only the modules’ firmware image can be executed. A method to update the firmware with a new digitally-signed image is provided. Prior to installing the new image, its associated 2048-bit RSA signature is checked. If the signature check is failed, the new firmware is ignored and the current firmware remains loaded. If the signature check is passed, the new image will be installed and executed after the device is reset. Any firmware loaded into this module that is not listed in this document is out of the scope of this validation and will mean that the module is not operating in a FIPS-Approved mode of operation.



NOTE

The FIPS compliant products are shipped from the factory in FIPS mode. There is no operational non-FIPS mode.

Only FIPS-validated firmware may be loaded to maintain the module’s validation.

Section 2.7

Cryptographic Key Management

Table 12 below describes the keys and CSPs supported by the modules.

Table 12: Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Initialization Vector (IV) ^j	128-bit value	For encryption: Generated internally (using an Approved DRBG with a cryptographically-strong entropy source) For decryption: Generated externally and enters the module in encrypted form	For encryption: exits the module in encrypted form For decryption: never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used with AES-CTR for encrypting or decrypting payload data between an authorized external entity and the module
SSH Public Key	2048, 3072-bit RSA key	Public key of an external entity: Enters the module in plaintext	Never exits the module	Stored in a file on the flash memory in plaintext form	Command via CLI or when updated with a new one	Used for public key-based authentication
SSH Session Key	128, 256-bit AES key	Generated internally via DH or ECDH key agreement	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for encryption or decryption of SSH session packets
SSH Authentication Key	160-bit HMAC key	Generated internally via DH or ECDH key agreement	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for authentication of SSH session packets
TLS Session Key	128, 256-bit AES key	Generated internally via FIPS-Approved DRBG or entered into the module in encrypted form during TLS session negotiation	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for encryption or decryption of TLS session packets
TLS Authentication Key	160, 256, 384-bit HMAC key	Generated internally via FIPS-Approved DRBG or entered into the module in encrypted form during TLS session negotiation	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for authentication of TLS session packets
CA Public Key	2048, 3072-bit RSA key	Enters the module in plaintext	Never exits the module	Stored in a file on the flash memory in plaintext form	When updated with a new one	Used to provide the chain of authority and authenticity for

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
						enabling SSL communications
TLS RSA Public Key	2048, 3072-bit key	The module's public key is generated internally or enters the module encrypted through an SFTP rowansfer; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Stored in a file on the flash memory in plaintext form	Command via CLI; when updated with a new one; on factory reset	Used for TLS key negotiation; TLS authentication, signature verification, and certificate generation
TLS RSA Private Key	2048, 3072-bit key	Internally generated using DRBG, entered into the module in encrypted form	Never exits the module	Stored in a file on flash memory with write-only permissions	Command via CLI or when updated with a new one; on factory reset	Used for TLS key negotiation; TLS authentication, signature and certificate generation
SSH RSA Public Key	2048, 3072-bit key	The module's public key is generated internally or enters the module encrypted through an SFTP rowansfer; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Stored in a file on the flash memory in plaintext form	Command via CLI; when updated with a new one	Used for SSH and SFTP key negotiation; SSH authentication, signature verification, and certificate generation
SSH RSA Private Key	2048, 3072-bit key	Internally generated using DRBG, entered into the module in encrypted form	Never exits the module	Stored in a file on flash memory with write-only permissions	Command via CLI or when updated with a new one	Used for SSH and SFTP key negotiation; SSH authentication, signature and certificate generation
TLS DH Public Key	2048-bit key	The module's public key is generated internally; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of TLS Session and Authentication keys
TLS DH Private Key	2048-bit key	Generated internally	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of TLS Session and Authentication keys
SSH DH Public Key	2048-bit key	The module's public key is generated internally; public	The module's public key exits the module in plaintext; public	Plaintext in SDRAM	Reboot or session termination	Used for generation of SSH Session and

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
		key of an external entity enters the module in plaintext	key of an external entity never exits the module			Authentication keys
SSH DH Private Key	2048-bit key	Generated internally	Never exits the module	Plaintext in SDRAM	Reboot or session termination	Used for generation of SSH Session and Authentication keys
TLS ECDH Public Key	Public key of ECDH protocol (supported curves of P-256, P-384, P-521)	The module's public key is generated internally; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of TLS Session and Authentication keys
TLS ECDH Private Key	Private key of ECDH protocol (supported curves of P-256, P-384, P-521)	Generated internally	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of TLS Session and Authentication keys
TLS ECDSA Public Key	Public key of ECDSA protocol (supported curves of P-256, P-384, P-521)	The module's public key is generated internally; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of TLS Session and Authentication keys
SSH ECDH Public Key	Public key of ECDH protocol (supported curves of P-256, P-384, P-521)	The module's public key is generated internally; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Plaintext in SDRAM	Reboot or session termination	Used for generation of SSH Session and Authentication keys
SSH ECDH Private Key	Private key of ECDH protocol (supported curves of P-256, P-384, P-521)	Generated internally	Never exits the module	Plaintext in SDRAM	Reboot or session termination	Used for generation of SSH Session and Authentication keys
SSH ECDSA Public Key	Public key of ECDSA protocol (supported curves of P-256, P-384, P-521)	The module's public key is generated internally; public key of an external entity enters the module in plaintext	The module's public key exits the module in plaintext; public key of an external entity never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of SSH Session and Authentication keys
DRBG Seed	384-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of random numbers

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Entropy Input String	256-bit value	Continually polled from various system resources to accrue entropy by NDRNG	Never exits the module	Plaintext in SDRAM	Reboot or session termination; on factory reset	Used for generation of random numbers
DRBG Key	256-bit AES key	Generated internally during DRBG instantiation	Never exits the module	Plaintext in SDRAM	Reboot; on factory reset	Internal state value used with the CTR_DRBG
DRBG 'V' Value	128-bit internal state value	Generated internally during DRBG instantiation	Never exits the module	Plaintext in SDRAM	Reboot; on factory reset	Internal state value used with the CTR_DRBG
CO Password	Strong of 8 – 19 characters (alphanumeric and special characters)	Initial password are hardcoded into the module; password changes entered into module via console, SSH, or TLS	Initially hardcoded password never exits the module; changed password never exits the module	Plaintext (hashed ^k) in flash memory and in SDRAM	Zeroized when the password is updated with a new one; changed password zeroized on factory reset	Used for authentication of the Crypto Officer
User Password	Strong of 8 – 19 characters (alphanumeric and special characters)	Initial password are hardcoded into the module; password changes entered into module via console, SSH, or TLS	Initially hardcoded password never exits the module; changed password never exits the module	Plaintext (hashed) in flash memory and in SDRAM	Zeroized when the password is updated with a new one; changed password zeroized on factory reset	Used for authenticating the User
Guest Password	Strong of 8 – 19 characters (alphanumeric and special characters)	Initial password are hardcoded into the module; password changes entered into module via console, SSH, or TLS	Initially hardcoded password never exits the module; changed password never exits the module	Plaintext (hashed) in flash memory and in SDRAM	Zeroized when the password is updated with a new one; changed password zeroized on factory reset	Used for authenticating the Guest
Firmware Load Authentication Key	Hardcoded RSA 2048-bit public key with SHA-256	Hardcoded in release image	Never exits the module	Image in flash memory	The Flash location is write-protected in hardware at the factory (i.e., not writeable by end user) and is not zeroized.	Used for verification of RSA signature of firmware image digest

^j Generation of the IV follows technique #1 described in FIPS Implementation Guidance A.5.

^k Passwords are hashed and stored in the Flash memory. They are temporarily loaded into the memory in hashed form for comparison during a login.

Section 2.8

EMI / EMC

The RUGGEDCOM ROS-F Devices were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

Section 2.9

Self-tests

Cryptographic self-tests are performed automatically (without operator intervention) by each module during the boot sequence (at power-up, upon hot reboots, and after power cycles) and during runtime as certain conditions exist. While the module is in a self-test condition, all data output via the module's data output interfaces is inhibited.

The following sections list the self-tests performed by the modules, their expected error status, and error state recovery.

CONTENTS

- [Section 2.9.1, "Power-up Self-tests"](#)
- [Section 2.9.2, "Conditional Self-tests"](#)
- [Section 2.9.3, "Critical Functions Self-Tests"](#)
- [Section 2.9.4, "Self-test Error Behavior and Recovery"](#)

Section 2.9.1

Power-up Self-tests

The RUGGEDCOM ROS-F Devices perform the following self-tests at power-up:

- Firmware integrity check with an Error Detection Code (SHA-256 hash)
- Known Answer Tests (KATs)
 - AES-CBC encrypt KAT
 - AES-CBC decrypt KAT
 - AES-GCM encrypt KAT
 - AES-GCM decrypt KAT
 - AES-CTR encrypt KAT
 - AES-CTR decrypt KAT
 - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
 - HMAC (with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) KAT
 - Counter DRBG KAT
 - RSA signature generation/verification KAT
 - Primitive "Z" computation KAT
 - ECDSA Sign/verify PCT

Once all self-tests have passed, a success message is written to the system log file (`syslog.txt`).

Section 2.9.2

Conditional Self-tests

The modules perform the following conditional self-tests:

- Continuous RNG test for NDRNG
- Continuous RNG test for DRBG
- RSA pairwise consistency test
- Firmware load test using RSA signature verification
- ECDH public key assurance test

Section 2.9.3

Critical Functions Self-Tests

The DRBG Instantiate, Generate, Reseed, and Uninstantiate tests (described in Section 11.3 of NIST SP 800-90A) are performed by the modules at start-up or anytime the DRBG is instantiated.

In addition, the modules perform a series of entropy tests against their NDRBG to verify the correct operation of the entropy collection mechanism during module operation. This test suite consists of the following tests (performed at the frequency indicated):

- Repetition Count Test (at power-up, conditionally, and on-demand)
- Adaptive Proportion Test (at power-up and on-demand)
- Arithmetic Mean Value Test (at power-up and on-demand)
- Entropy Value Test (at power-up and on-demand)
- "Stuck-at-constant-failure" Test (conditionally, when seeding or reseeding the DRBG)

Section 2.9.4

Self-test Error Behavior and Recovery

If one of the power-up self-tests fails, the module will enter a soft error state, and the following will occur:

- An error message appears
- A failure message is written to the system log
- An alarm indicator LED (if equipped) will blink 5 times
- The device is automatically rebooted, clearing all keys and CSPs in SDRAM

If the conditional firmware load test fails, the device will ignore the new image and continue operating with the currently-loaded image.

If one of the other conditional self-tests fails, the module will enter a soft error state, and the following will occur:

- A failure message is written to the system log
- An alarm indicator LED (if equipped) will blink 5 times

- All open files are closed
- The database is closed
- The device is automatically rebooted, clearing all keys and CSPs in SDRAM

Upon reboot, all power-up self-tests will be executed. If the failed self-test is not one of the power-up self-tests, the device will automatically perform the failed conditional self-test as well. Successful execution of the failed self-test will clear the soft error state, and the module will return to normal operation. Another self-test failure will trigger another reboot and recovery attempt.

The module will perform a maximum of 10 attempts at recovery. If no resolution is found after 10 attempts, the module will reboot into a critical error state, where all cryptographic operations are halted and none of the module's data output services are available for use. Additionally, the module is reset to the factory default configuration. Upon reset, the following data is zeroized:

- all configuration files
- server certificates and SSH host key pairs stored in flash
- keys and CSPs stored in SDRAM

However, if the module runs for an hour without experiencing an error or is power-cycled, the failure counter is reset to zero.

To clear the critical error state, the Crypto Officer must access the module via the local Console Interface. At this point, the CO can only view system logs or run hardware tests in an attempt to determine the cause of the self-test failure. If the CO cannot determine the cause of the critical error condition, they must contact Siemens Customer Support to resolve the issue and return the module to a normal operational state.

Section 2.10

Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The RUGGEDCOM ROS-F Devices meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in the FIPS-Approved mode of operation.

CONTENTS

- [Section 3.1, "Initial Setup"](#)
- [Section 3.2, "Crypto Officer Guidance"](#)
- [Section 3.3, "User Guidance"](#)
- [Section 3.4, "Additional Guidance and Usage Policies"](#)
- [Section 3.5, "Non-FIPS-approved Mode"](#)

Section 3.1

Initial Setup

The modules are delivered in an operational state, but require initialization steps to be placed in the FIPS-Approved mode of operation. The CO is responsible for inspection, initialization, and security-relevant configuration and management activities for each module. To configure the modules for their FIPS-Approved mode of operation, the CO must:

1. Inspect all physical security mechanisms
2. Ensure insecure protocols are disabled
3. Replace the default passwords for all operator types
4. Provision SSH public key(s)
5. Replace the default SSH host key pair
6. Provision an SSL server certificate
7. Reboot the device

Detailed guidance for performing these configuration tasks can be found in the *Siemens RUGGEDCOM ROS-F v4.2.2.F User Guide* and in this FIPS 140-2 Security Policy. To initialize each module, follow the steps below to complete the initial setup.

- **Inspect all physical security mechanisms**

The modules are delivered with all physical security mechanisms pre-installed. The CO shall ensure that the number of labels applied to each module is as follows:

- M2100F/RSG2100F: **9**
- M2200F/RSG2200F: **7**
- RS416F: **7**
- M969F: **1**

- RS900F: **5**
- RS900GF: **5**
- RS940GF: **4**
- RSG2488F: **10**

The CO shall inspect the modules to ensure that the proper number of mechanisms is in place and show no signs of tampering.

[Figure 11](#) through [Figure 18](#) below show the label locations for each module. Alternate hardware configurations are available for the following devices: RSG2100F, M2100F, RSG2200F, M2200F and RS416F (i.e. LED panel at the front or rear). Regardless of hardware configuration, the label positions shown remain the same.

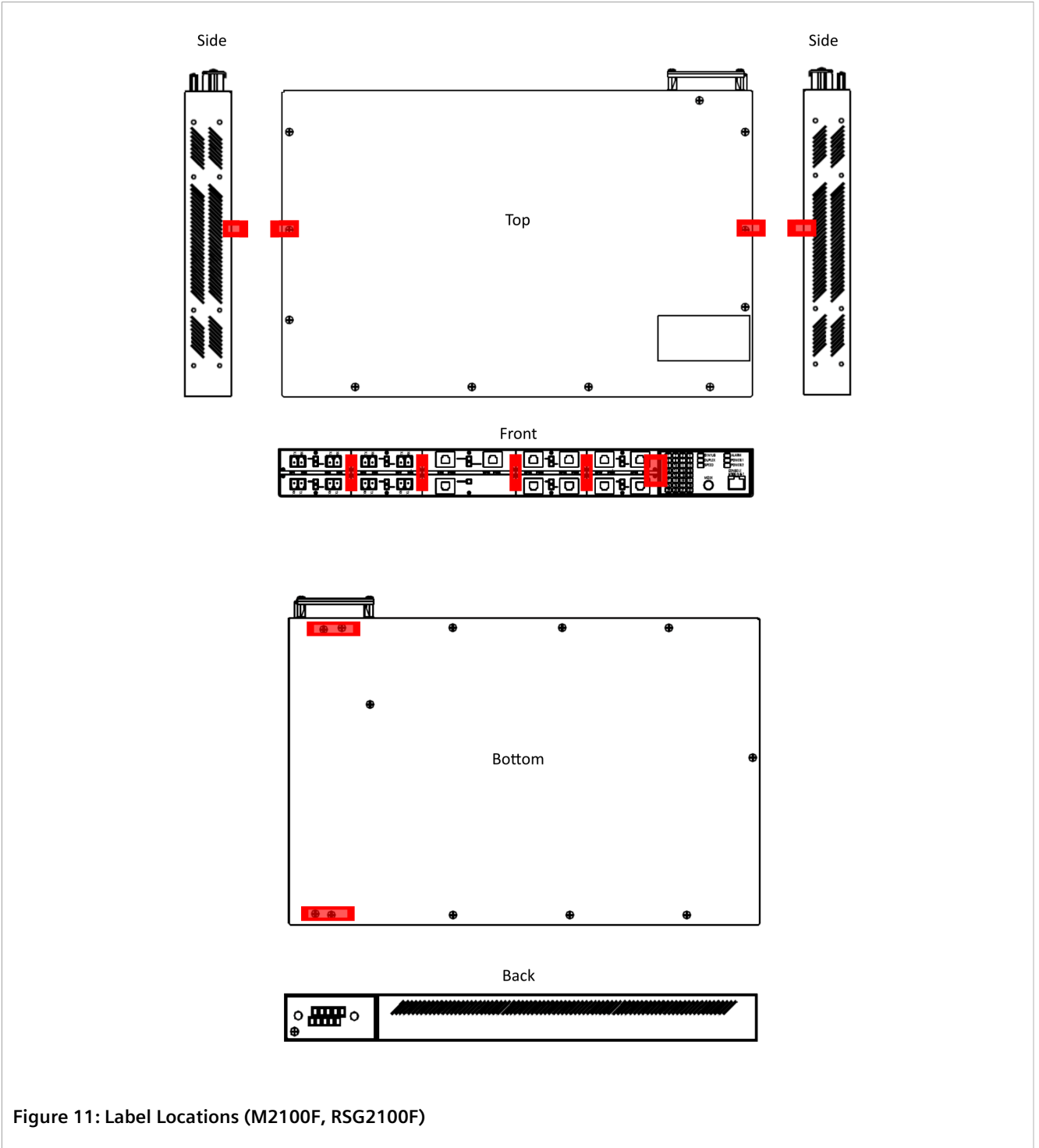
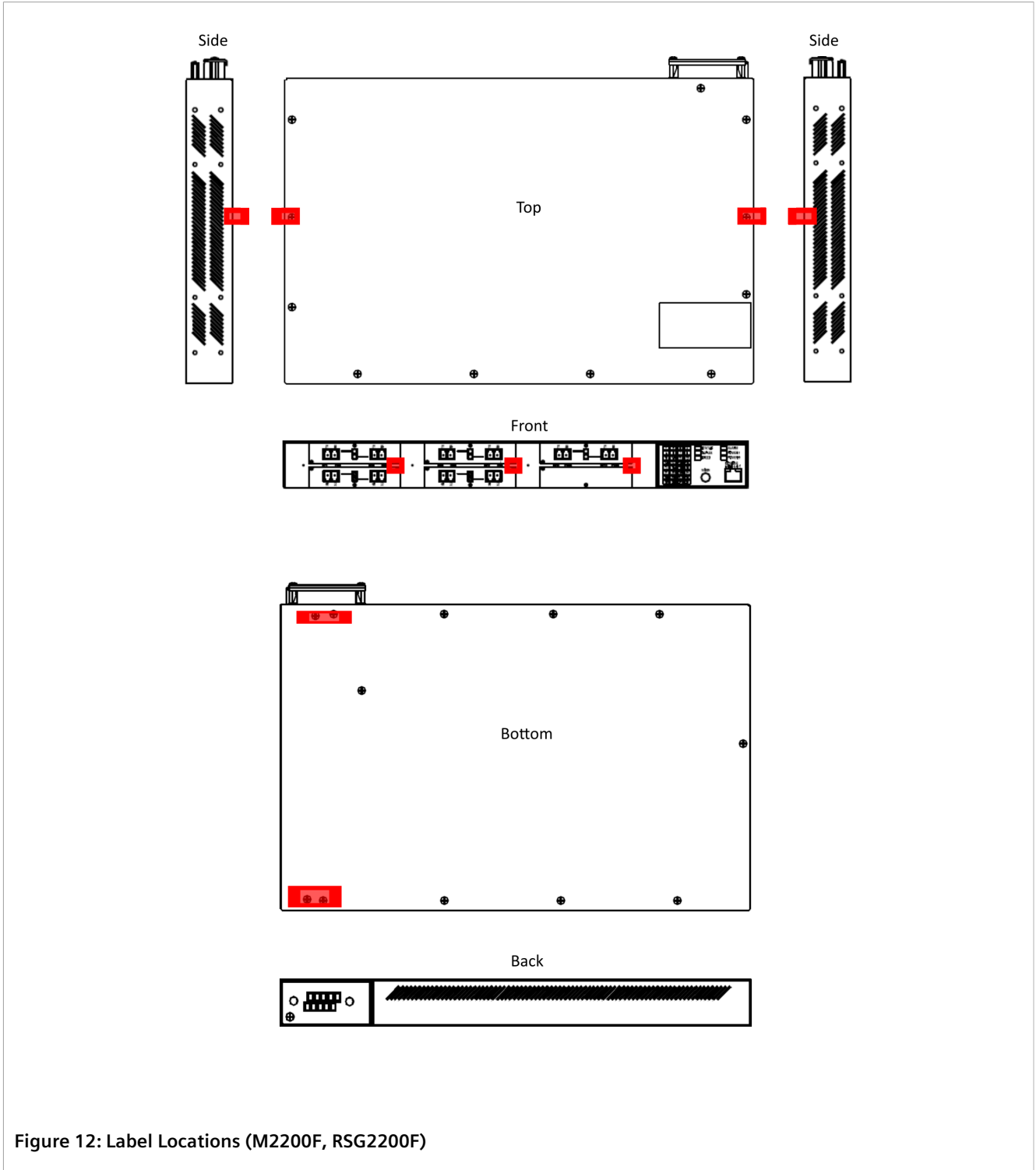


Figure 11: Label Locations (M2100F, RSG2100F)



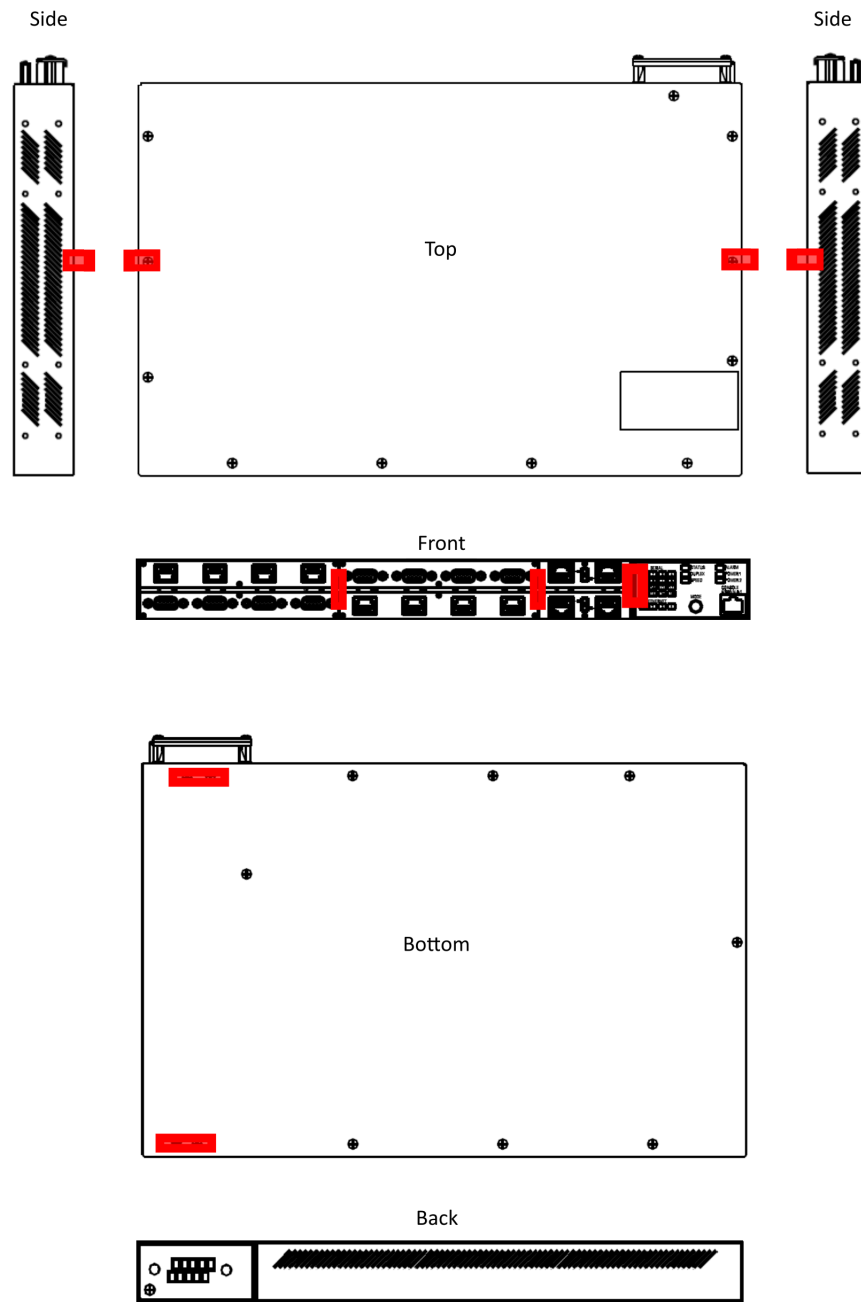


Figure 13: Label Locations (RS416F)

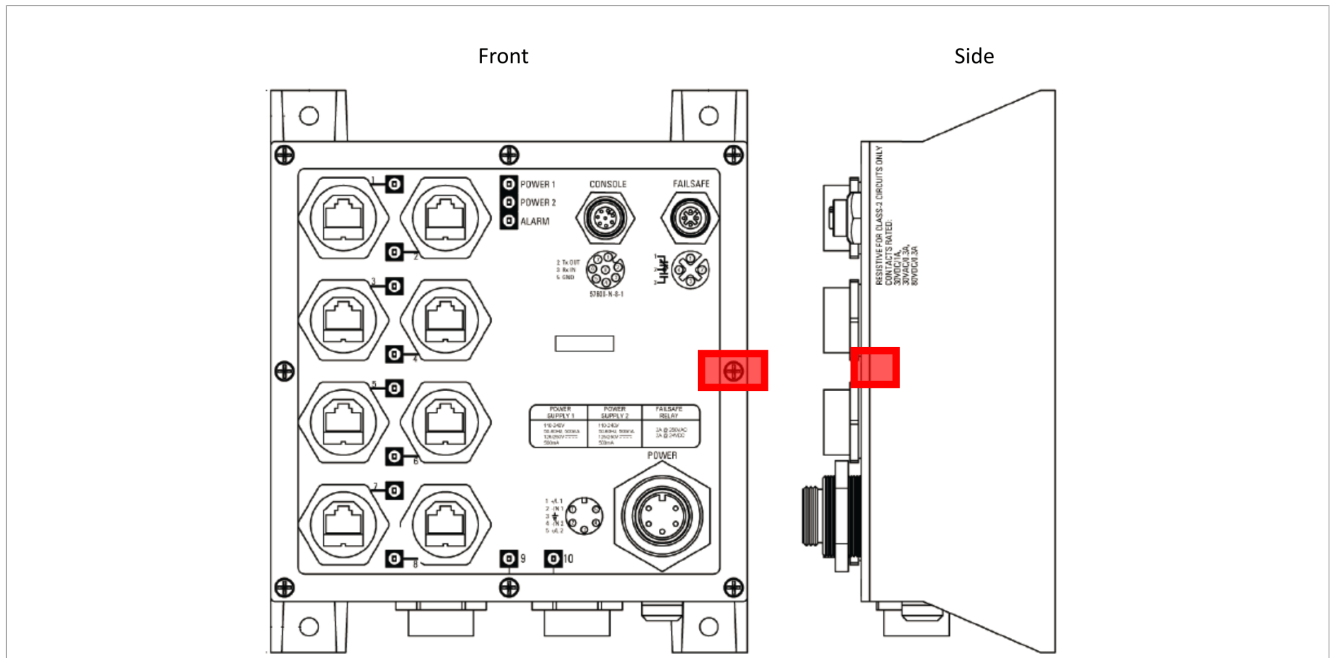


Figure 14: Label Locations (M969F)

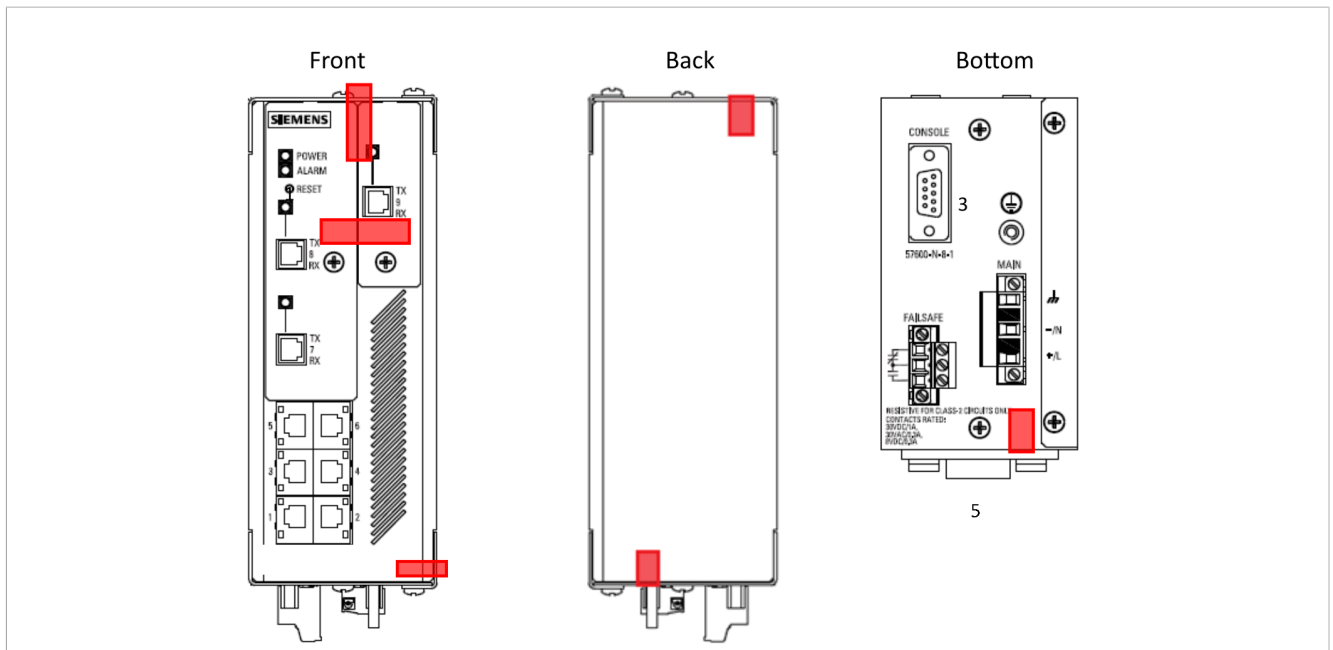
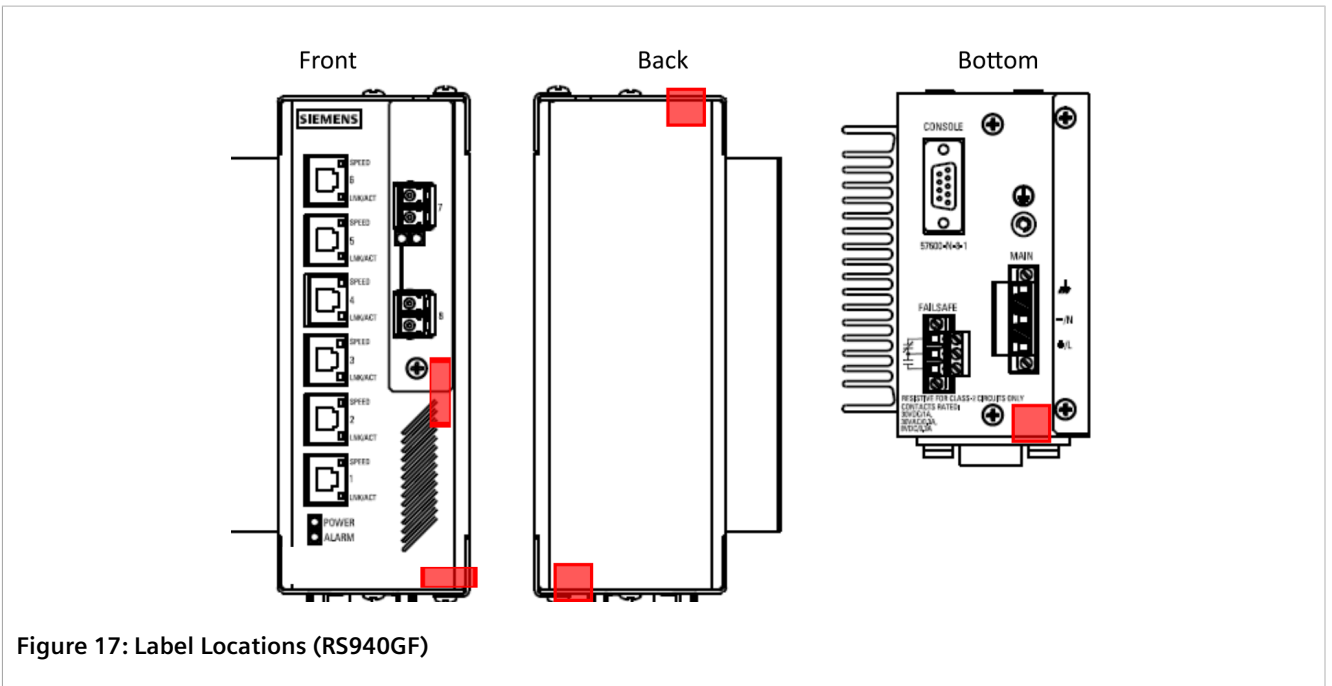
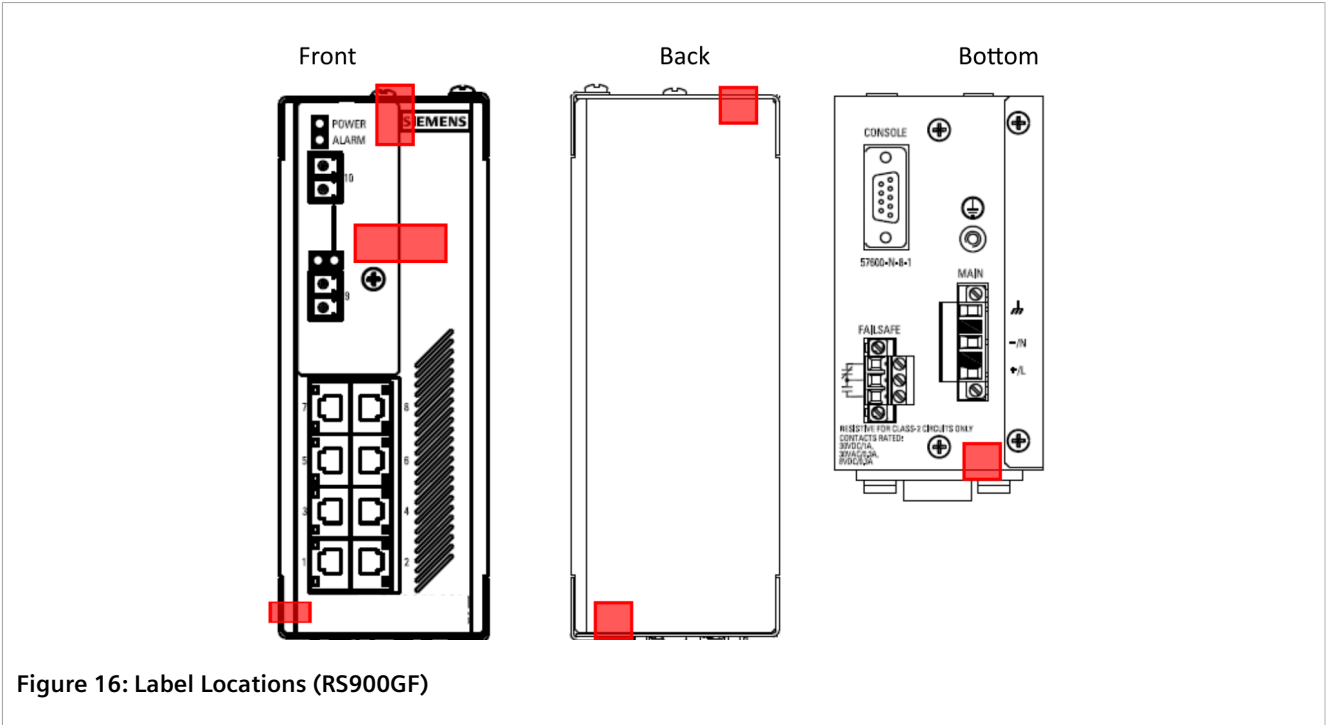


Figure 15: Label Locations (RS900F)



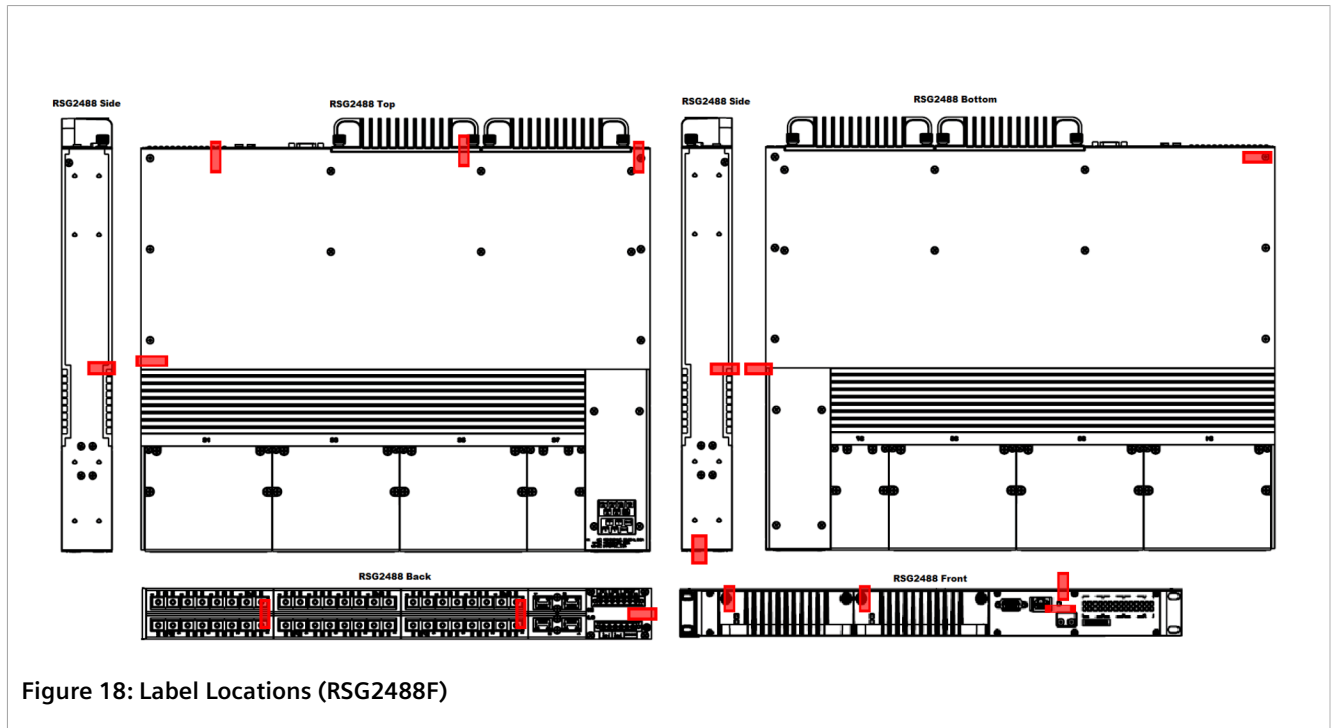


Figure 18: Label Locations (RSG2488F)

- **Ensure insecure protocols are disabled**

The following insecure protocols are disabled by default:

- RADIUS
- TACACS+
- RSH
- Telnet
- TFTP¹
- ModBus management
- Remote Syslog
- SNMPv1, SNMPv2, and SNMPv3

The CO shall ensure that these protocols are set to “disabled” while operating in the FIPS-Approved mode.

- **Replace the default passwords for all operator types**

The modules allow for up to three operator types to be configured locally on the device. The modules are delivered with default passwords pre-configured for each operator type. Prior to commissioning the modules, the CO shall replace the default passwords using the following steps:

1. Log on to the device as the CO
2. Navigate to **Administration » Configure Passwords**. The **Configure Passwords** form appears.
3. For “Auth Type”, select “local”
4. Enter the username and password for the “Guest”, “Operator”, and “Admin” accounts (see [Section 3.2.6, “Password Complexity”](#) below for password complexity policies)
5. For “Clear Private Data Option”, select “Enabled”

¹TFTP - Trivial File Transfer Protocol

6. For "Password Minimum Length", enter at least a value of "8"
7. For "Max Failed Attempts", enter at most a value of "10"
8. For "Lockout Time", enter at least a value of "60 min"
9. For "Failed Attempts Window", enter at most a value of "5 min"
10. Click **Apply**

- **Provision SSH public key(s)**

The modules can perform public key user authentication to establish secure remote sessions via SSH. SSH user public key entries are stored in a flash file called `sshpub.keys`. For FIPS mode, the CO shall create a public key file locally via a host computer and upload it directly to the `sshpub.keys` file, which will replace the content in flash with the uploaded content. Alternatively, the CO can upload the locally-created file to the `sshaddpub.keys` file, which will keep any existing entries in the `sshpub.keys` file and append the new entries.

The public key file shall be uploaded to the module using SFTP or Xmodem. To verify that the upload was successful, the CO can log into the CLI and check the system log.

Note that RUGGEDCOM ROS-F v4.2.2.F allows up to 16 key entries to be stored.

- **Replace the default SSH host key pair**

The modules are delivered with a pre-configured SSH host key pair stored in a flash file called `ssh.keys`. The CO shall replace the default key pair by (1) creating a valid key pair locally and uploading it to the `ssh.keys` file or (2) generating a new key pair.

To generate a new SSH host key pair using the following steps:

1. Log on to the device (using the Console Interface) as the CO
2. Press **CTRL+S** to access the Console CLI shell
3. At the Console CLI prompt, enter "sshkeygen rsa N", where N is the number of bits in length (2048 or 3072)

- **Provision an SSL server certificate**

In order to enable the secure web server, the CO must obtain and provision a valid X.509v3 TLS server certificate, its full chain of trust, and valid and active OCSP responders:

1. The TLS server certificate or certificate chain, `ssl.crt`, must be signed by an issuer that is present in the trust store
2. The issuing certificate(s) must be installed in the trust store, `sslpub.certs`
3. The TLS server certificate and every intermediate issuing certificate must have an OCSP responder URL, and all OCSP responders must be active and responsive

The CO must provision and activate these components in the following order:

1. The OCSP responder(s) must be provisioned and activated
2. The trust store (`sslpub.certs`) must be provisioned to the ROS-F device
3. The TLS server certificate (`ssl.crt`) can now be provisioned to the device

Please refer to the Siemens RUGGEDCOM ROS-F v4.2.2.F User Guide for further details.

The CO shall make sure the switch can reach out to the corresponding OCSP server that checks the revocation status of the SSL certificate. The verification of revocation status is configurable through the CLI.

**NOTE**

If the OCSP server is not reachable, RUGGEDCOM ROS-F will immediately remove the installed certificate during boot up.

After these changes are complete, the CO shall reboot the device so the changes will go into effect. Once rebooted, the devices are properly configured for their FIPS-Approved mode of operation.

Section 3.2

Crypto Officer Guidance

The Crypto Officer is responsible for ensuring that the modules are operating in their FIPS-Approved mode of operation. When configured according to the Crypto Officer guidance in this Security Policy, the modules only run in their FIPS-Approved mode of operation.

The Crypto Officer shall configure the modules via the Web GUI or Console Interface as prescribed in this Security Policy. Please refer to the Security Recommendations section of the *Siemens RUGGEDCOM ROS-F v4.2.2.F User Guide* for further details regarding this and other security-related guidance.

CONTENTS

- [Section 3.2.1, "Monitoring Status"](#)
- [Section 3.2.2, "Physical Inspection"](#)
- [Section 3.2.3, "On-demand Self-test Execution"](#)
- [Section 3.2.4, "CSP Zeroization"](#)
- [Section 3.2.5, "Upgrading/Downgrading Firmware"](#)
- [Section 3.2.6, "Password Complexity"](#)

Section 3.2.1

Monitoring Status

The CO shall be responsible for regularly monitoring the modules' status for FIPS-Approved mode of operation. When configured according to the Crypto Officer's guidance, the modules only operate in the FIPS-Approved mode.

The module's operational status is indicated with LEDs as described in [Table 7](#) above. A CO logged in via the Web Interface or Console Interface can view the operational status on the remote terminal window.

Section 3.2.2

Physical Inspection

For the modules to operate in their FIPS-Approved mode of operation, the pre-installed tamper-evident labels must be in place as specified in [Section 3.1, "Initial Setup"](#). Upon receipt, the CO shall inspect the module to ensure labels have been properly installed. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO is also responsible for the following:

- Securing and having control at all times of any unused tamper-evident labels
- Direct control and observation of any changes to the module where the tamper-evident labels are removed or applied to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO is also required to periodically inspect the modules for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of tampering. If evidence of tampering is found during periodic inspection, the CO must zeroize the keys and contact Siemens Customer Service for guidance.

Section 3.2.3

On-demand Self-test Execution

Although power-up self-tests are performed automatically during module power up, they can also be manually launched on demand. Self-tests can be executed by power-cycling the modules, using the reset button (on devices so equipped), or executing any of the device reboot/reset commands. If one of the power-up self-tests fails, the devices will exhibit the behavior described in [Section 2.9.1, “Power-up Self-tests”](#) above.

Additionally, the cryptographic algorithm self-tests can be launched directly by performing the following steps:

1. Log in to the device as a CO via the Console Interface
2. Press **CTRL+S** to access the Console CLI shell
3. At the Console CLI prompt, enter “factory”
4. When prompted, answer “yes” and enter the CO password
5. At the Console CLI prompt, enter “cryptest”

Each cryptographic algorithm self-test will be run in sequence. If all tests pass, the following message will appear:

```
“Cryptographic algorithm self tests passed”
```

Section 3.2.4

CSP Zeroization

To zeroize keys/CSPs in SDRAM, Crypto Officers and Users can perform the reset/reboot service by performing the following steps:

1. Log on to the device via the Web GUI
2. Navigate to **Diagnosics » Reset Device**. The **Reset Device** form appears.
3. Click **Confirm**

In order to zeroize all plaintext secret and private keys/CSPs in both flash and SDRAM, the CO shall access the modules using the maintenance mode (refer to [Section 2.4.3, “Maintenance Mode”](#) above for more details). Entering the “maintenance” CLI command will automatically zeroize all server certificates (`ssl.crt`), SSH host key pairs (`ssh.keys`), and device configuration (`config.csv`) files stored in flash. Upon completion of the deletion process, the module will perform an automatic reboot into maintenance mode, which will zeroize all keys and CSPs stored in SDRAM.

Once the “maintenance” command is invoked, the effect is immediate and will not allow sufficient time to compromise any stored plaintext CSPs.

Section 3.2.5

Upgrading/Downgrading Firmware

The CO shall be responsible for upgrading or downgrading the modules' firmware as necessary. The RUGGEDCOM ROS-F Devices only accept firmware that has been digitally-signed by Siemens. Note the following policies:

- After the new firmware has been uploaded and passed the digital signature test, the CO shall reset the device to complete the installation
- To verify the correct firmware version was installed, the CO shall access the Console CLI and enter "version" at the Console CLI prompt
- When downgrading, the CO shall not downgrade the RUGGEDCOM ROS-F firmware to a version prior to 4.2.2.F when encryption is enabled
- Before downgrading, the CO shall restore the device to factory defaults

The modules' operational status is indicated with LEDs as described in [Table 7](#) above. A CO logged in via the Web Interface or Console Interface can view the operational status on the remote terminal window.

» Firmware Upgrade

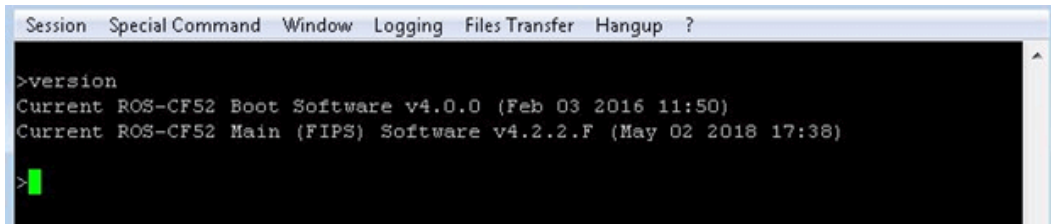
The CO can obtain binary firmware releases, including updates, by submitting a Support Request via the [Siemens Industry Online Support](https://support.industry.siemens.com) [https://support.industry.siemens.com] website. For more informatoin, refer to <https://support.industry.siemens.com/My/ww/en/requests>.

RUGGEDCOM ROS-F firmware image files are cryptographically signed using the private Siemens RUGGEDCOM product key. The corresponding public key is built in to the RUGGEDCOM ROS-F firmware image. When a firmware image file is uploaded to a ROS-F device, the device verifies its signature to ensure the uploaded file is genuine (i.e. cryptographically signed by Siemens RUGGEDCOM) and intact. The device will reject any firmware update file that is not signed by Siemens. An uploaded firmware image file that succeeds validation is sorted in non-volatile Flash memory. On every device start-up, the system verifies the firmware signature anew, and halts if verification fails.

A CO can update the device by transferring the firmware image binary using Secure File Transfer Protocol (SFTP). See *Uploading/Downloading Files* in 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 *Resetting the Device* in the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* to reset the device. All firmware is signed by Siemens, and the device will reject any firmware updates that are not signed by Siemens.

The device stores upgrades in the non-volatile flash memory until it 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. Or follow the instructions in *Viewing Product Information* in the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* to verify the FIPS-validated software is running on the device.

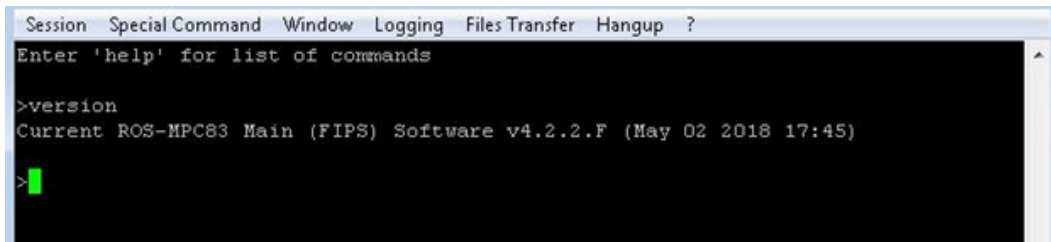
See the *Upgrade/Downgrading Firmware* section of the *Siemens RUGGEDCOM ROS v4.2.2.F User Guides* for more details on the upgrade process. On devices with ColdFire CPUs, the output of this command will show the currently installed versions of the Boot software and the Main software. Each of these is updated separately as shown here:



```
Session Special Command Window Logging Files Transfer Hangup ?
>version
Current ROS-CF52 Boot Software v4.0.0 (Feb 03 2016 11:50)
Current ROS-CF52 Main (FIPS) Software v4.2.2.F (May 02 2018 17:38)
>
```

Figure 19: Boot/Main Software

On PowerPC-based RUGGEDCOM ROS-F devices, only the main software version will be shown. If an upgrade image has been uploaded and its signature verified, but a system reset has not yet occurred the **version** command will show a *Next* entry that lists the version that is loaded but not yet active.



```
Session Special Command Window Logging Files Transfer Hangup ?
Enter 'help' for list of commands
>version
Current ROS-MPC83 Main (FIPS) Software v4.2.2.F (May 02 2018 17:45)
>
```

Figure 20: Main Software

Section 3.2.6

Password Complexity

Crypto Officers shall follow the password complexity policy below.

- The password must be between 8 and 19 characters in length
- The password may contain any combination uppercase and lowercase letters, digits, and special characters, allowing for a total of 94 possible characters
- A password must have:
 - At least one digit
 - At least one lower-case letter
 - At least one upper-case letter
 - At least one special character
- The password must not include the username or any four continuous characters found in the username. For example, if the username is "Subnet25", the password may not be "subnet25admin", "subnetadmin" or "net25admin". However, "net-25admin" and "Sub25admin" are permitted.
- The password must not have more than three continuously incrementing or decrementing numbers. For example, "Sub123" and "Sub19826" are permitted, but "Sub12345" is not.

Section 3.3

User Guidance

While the CO is responsible for ensuring that the modules' physical security mechanisms are in place and that the devices are running in their FIPS-approved mode of operation, users should also monitor device status. Any changes in the status of the devices should immediately be reported to the Crypto Officer.

Section 3.4

Additional Guidance and Usage Policies

The notes below provide additional guidance and policies that must be followed by module operators:

- **Use of insecure protocols**

The following insecure protocols are disabled by default: RADIUS, TACACS+, RSH, Telnet, TFTP, ModBus management, Remote Syslog, SNMPv1, SNMPv2, and SNMPv3. To maintain compliance with FIPS requirements, these protocols shall not be enabled.

- **Line card replacement**

As noted earlier, the RUGGEDCOM ROS-F Devices are modular by design. While most device configurations are fixed once they leave the factory, the RUGGEDCOM RSG2488F Ethernet Switch comes equipped with line cards that are field-replaceable. Operators in the field can order the desired line card(s) directly from Siemens Customer Support using the appropriate part numbers.

Because these line cards play a role in maintaining the module's physical security, they are secured in place using tamper-evident labels. Thus, replacing a line card necessitates the replacement of any tamper-evident label affixed to the line card as well. When an operator orders a line card, it will be delivered with the number of tamper-evident labels required for proper installation. Module operators must follow the guidance below to ensure continued compliance with FIPS requirements.

1. Zeroize all keys and CSPs on the module
2. Remove power from the module
3. Remove the line card to be replaced
4. Remove any remaining bits of the now-broken tamper-evident label from the module chassis
5. Install the replacement line card in the open slot
6. Using isopropyl alcohol, clean the chassis surface in the area where the replacement tamper-evident label will be placed
7. Affix the replacement tamper-evident label to the chassis (refer to [Figure 18](#) above for label locations). Allow 24 hours for the seal to fully cure.
8. Apply power to the module

For more detailed line card removal and installation instructions, please refer to the *Siemens RUGGEDCOM RSG2488F Hardware Installation Guide*.

Section 3.5

Non-FIPS-approved Mode

When configured according to the Crypto Officer guidance in this Security Policy, the modules do not support a non-FIPS-Approved mode of operation.

4 Acronyms

Table 13 provides definitions for the acronyms used in this document.

Table 13: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CoS	Class of Service
CSE	Communications Security Establishment
CSP	Critical Security Parameters
CTR	Counter Mode
CVL	Component Validation List
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
EC	Elliptical Curve
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptical Curve Diffie-Hellman
ECDSA	Elliptical Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
°F	Fahrenheit

Acronym	Definition
FTP	File Transfer Protocol
GB	Gigabytes
GBIC	Gigabit Interface Converter
GCM	Galois Counter Mode
GMRP	Generic Attribute Registration Protocol (GARP) Multicast Registration Protocol
GUI	Graphical User Interface
HMAC	(Keyed-)Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
I2C	Inter-Integrated Circuit
I/O	Input/Output
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IP66	Ingress Protection Rating 66
IP67	Ingress Protection Rating 67
IRIG	Inter-Range Instrumentation Group
KAT	Known Answer Test
LC	Lucent Connector
LED	Light emitting diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MB	Megabytes
Mbps	Megabits per second
MHz	Megahertz
MIL-STD	Military Standard
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
RADIUS	Remote Authentication Dial-In User Service

Acronym	Definition
RCDP	RUGGEDCOM Discovery Protocol
ROS	Rugged Operating System
RSA	Rivest-Shamir-Adleman
RSH	Remote Shell
SC	Subscriber Connector
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMI	Serial Management Interface
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
U	Unit
VLAN	Virtual Local Area Network

5 Appendix A

This section lists the specific configurations for each device that were not tested as part of this validation. The following sections specify the non-security relevant line card components and the configurations of each device. Note that these components, except the faceplates, are excluded from FIPS 140-2 requirements.

CONTENTS

- [Section 5.1, "RSG2100F"](#)
- [Section 5.2, "M2100F"](#)
- [Section 5.3, "RSG2200F"](#)
- [Section 5.4, "M2200F"](#)
- [Section 5.5, "RSG2488F"](#)
- [Section 5.6, "M969F"](#)
- [Section 5.7, "RS900F"](#)
- [Section 5.8, "RS900GF"](#)
- [Section 5.9, "RS416F"](#)
- [Section 5.10, "RS940GF"](#)

Section 5.1

RSG2100F

[Table 14](#) below lists RSG2100F Module's excluded configurations.

Table 14: RSG2100F Excluded Configurations

Component Configuration	Component Description
A04, B04, C04, D04, G04, H04, J04, K04	2 x 100FX - Multimode, 1300nm, SC
A05, B05, C05, D05, G05, H05, J05, K05	2 x 100FX - Multimode, 1300nm, LC
A06, B06, C06, D06, G06, H06, J06, K06	2 x 100FX - Multimode, 1300nm, MTRJ
A07, B07, C07, D07, G07, H07, J07, K07	2 x 100FX - Singlemode, 1310nm, ST, 20km
A08, B08, C08, D08, G08, H08, J08, K08	2 x 100FX - Singlemode, 1310nm, SC, 20km
A09, B09, C09, D09, G09, H09, J09, K09	2 x 100FX - Singlemode, 1310nm, LC, 20km
A10, B10, C10, D10, G10, H10, J10, K10	2 x 100FX - Singlemode, 1310nm, SC, 50km
A11, B11, C11, D11, G11, H11, J11, K11	2 x 100FX - Singlemode, 1310nm, LC, 50km
A12, B12, C12, D12, G12, H12, J12, K12	2 x 100FX - Singlemode, 1310nm, SC, 90km

Component Configuration	Component Description
E02	2 x 1000SX - Multimode, 850nm, LC, 500m
E03	2 x 1000LX - Singlemode, 1310nm, SC connectors, 10km
E04	2 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
E05	2 x 1000LX - Singlemode, 1310nm, SC connectors, 25km
E06	2 x 1000LX - Singlemode, 1310nm, LC connectors, 25km
E07	2 x 1000LX SFP - Blank
E08	2 x 1000SX SFP, Multimode, 850nm, LC, 500m
E09	2 x 1000LX SFP, Singlemode, 1310nm, LC, 10km
E10	2 x 1000LX SFP, Singlemode, 1310nm, LC, 25km
E11	2 x 1000LX SFP, Singlemode, 1550nm, LC, 70km
E12	2 x 1000LX GBIC
E13	2 x 1000LX GBIC, Singlemode, 1310nm, SC, 10km
E14	2 x 1000LX GBIC, Singlemode, 1310nm, SC, 25km
E15	2 x 1000LX GBIC, Singlemode, 1550nm, SC, 70km
E16	2 x 10/100/1000TX micro-D
E17	2 x 1000TX, SFP, RJ45
F01	1 x 10/100/1000Tx RJ45
F03	1 x 1000LX - Singlemode, 1300 nm, SC connectors, 10km
F04	1 x 1000LX - Singlemode, 1300 nm, LC connectors, 10km
F05	1 x 1000LX - Singlemode, 1300 nm, SC connectors, 25km
F06	1 x 1000LX - Singlemode, 1300 nm, LC connectors, 25km
F07	1 x 1000LX SFP - Blank
F08	1 x 1000LX SFP - Multimode, 850nm, LC, 500m
F09	1 x 1000LX SFP - Singlemode, 1310nm, LC, 10km
F10	1 x 1000LX SFP - Singlemode, 1310nm, LC, 25km
F11	1 x 1000LX SFP - Singlemode, 1550nm, LC, 70km
F12	1 x 1000LX GBIC - Blank
F13	1 x 1000LX GBIC - Singlemode, 1310nm, SC, 10km
F14	1 x 1000LX GBIC - Singlemode, 1310nm, SC, 25km
F15	1 x 1000LX GBIC - Singlemode, 1550nm, SC, 70km
F16	1 x 10/100/1000TX micro-D

Section 5.2

M2100F

Table 15 below lists M2100F Module's excluded configurations.

Table 15: M2100F Excluded Configurations

Component Configuration	Component Description
A01, B01, C01, D01, G01, H01, J01, K01	2 x 10/100Tx Micro-D
A04, B04, C04, D04, G04, H04, J04, K04	2 x 100FX - Multimode, 1310nm, LC
A06, B06, C06, D06, G06, H06, J06, K06	2 x 100FX - Singlemode, 1310nm, LC, 20km
A07, B07, C07, D07, G07, H07, J07, K07	2 x 100FX - Singlemode, 1310nm, LC, 50km
A08, B08, C08, D08, G08, H08, J08, K08	2 x 100FX - Singlemode, 1310nm, LC, 90km
E02	2 x 1000SX - Multimode, 850nm, LC, 500m
E03	2 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
E04	2 x 1000LX - Singlemode, 1310nm, LC connectors, 25km
F01	1 x 10/100/1000Tx, Micro-D
F02	1 x 1000SX - Multimode, 850nm, LC, 500m
F03	1 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
F04	1 x 1000LX - Singlemode, 1310nm, LC connectors, 25km

Section 5.3

RSG2200F

Table 16 below lists RSG2200F Module's excluded configurations.

Table 16: RSG2200F Excluded Configurations

Component Configuration	Component Description
A03, B03, C03, D03	2 x 1000LX - Singlemode, 1310nm, SC connectors, 10 km
A04, B04, C04, D04	2 x 1000LX - Singlemode, 1310nm, LC connectors, 10 km
A05, B05, C05, D05	2 x 1000LX - Singlemode, 1310nm, SC connectors, 25 km
A07, B07, C07, D07	2 x 1000LX SFP - Blank
A09, B09, C09, D09	2 x 1000LX SFP - Singlemode, 1310nm, LC, 10km
A10, B10, C10, D10	2 x 1000LX SFP- Singlemode, 1310nm, LC, 25km
A11, B11, C11, D11	2 x 1000LX SFP - Singlemode, 1550nm, LC, 70km(2)
A12, B12, C12, D12	2 x 1000LX GBIC - Blank,
A13, B13, C13, D13	2 x 1000LX GBIC- Singlemode, 1310nm, SC, 10km
A14, B14, C14, D14	2 x 1000LX GBIC - Singlemode, 1310nm, SC, 25km
A15, B15, C15, D15	2 x 1000LX GBIC - Singlemode, 1550nm, SC, 70km(2)

Component Configuration	Component Description
A16, B16, C16, D16	2 x 100FX - Multimode, 1300nm, ST
A17, B17, C17, D17	2 x 100FX - Multimode, 1300nm, SC
A18, B18, C18, D18	2 x 100FX - Multimode, 1300nm, LC
A19, B19, C19, D19	2 x 100FX - Multimode, 1300nm, MTRJ
A20, B20, C20, D20	2 x 100FX - Singlemode, 1310nm, ST, 20km
A21, B21, C21, D21	2 x 100FX - Singlemode, 1310nm, SC, 20km
A22, B22, C22, D22	2 x 100FX - Singlemode, 1310nm, LC, 20km
A23, B23, C23, D23	2 x 100FX - Singlemode, 1310nm, SC, 50km
A24, B24, C24, D24	2 x 100FX - Singlemode, 1310nm, LC, 50km
A25, B25, C25, D25	2 x 100FX - Singlemode, 1310nm, SC, 90km
A26, B26, C26, D26	2 x 100FX - Singlemode, 1310nm, LC, 90km
A27, B27, C27, D27	2 x 1000TX, SFP, RJ45
E01	1 x 10/100/1000 Tx RJ45
E02	1 x 1000SX - Multimode, 850nm, LC, 500m
E03	1 x 1000LX - Singlemode, 1310nm, SC connectors, 10km
E04	1 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
E05	1 x 1000LX - Singlemode, 1310nm, SC connectors, 25km
E06	1 x 1000LX - Singlemode, 1310nm, LC connectors, 25km
E07	1 x 1000LX SFP - Blank
E08	1 x 1000SX SFP -Multimode, 850nm, LC, 500m
E09	1 x 1000LX SFP -Singlemode, 1310nm, LC, 10km
E10	1 x 1000LX SFP -Singlemode, 1310nm, LC, 25km
E11	1 x 1000LX SFP -Singlemode, 1550nm, LC, 70km
E13	1 x 1000LX GBIC - Blank
E14	1 x 1000LX GBIC -Singlemode, 1310nm, SC, 10km
E15	1 x 1000LX GBIC -Singlemode, 1310nm, SC, 25km
E16	1 x 1000LX GBIC -Singlemode, 1550nm, SC, 70km
E17	1 x 100FX - Multimode, 1300nm, ST
E18	1 x 100FX - Multimode, 1300nm, SC
E19	1 x 100FX - Multimode, 1300nm, LC
E21	1 x 100FX - Singlemode, 1310nm, ST, 20km
E22	1 x 100FX - Singlemode, 1310nm, SC, 20km
E23	1 x 100FX - Singlemode, 1310nm, LC, 20km
E24	1 x 100FX - Singlemode, 1310nm, SC, 50km

Component Configuration	Component Description
E25	1 x 100FX - Singlemode, 1310nm, LC, 50km
E26	1 x 100FX - Singlemode, 1310nm, SC, 90km
E27	1 x 100FX - Singlemode, 1310nm, LC, 90km

Section 5.4

M2200F

Table 17 below lists M2200F Module's excluded configurations.

Table 17: M2200F Excluded Configurations

Component Configuration	Component Description
A03, B03, C03, D03	2 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
E01	1 x 10/100/1000Tx, Micro-D
E02	1 x 1000SX - Multimode, 850nm, LC, 500m
E03	1 x 1000LX - Singlemode, 1310nm, LC connectors, 10km
E04	1 x 1000LX - Singlemode, 1310nm, LC connectors, 25km
E05	1 x 10/100/1000Tx, Micro-D, with special short jackscrews

Section 5.5

RSG2488F

Table 18 below lists RSG2488F Module's excluded configurations.

Table 18: RSG2488F Excluded Configurations

Component Configuration	Component Description
A02, B02, C02, D02, E02, F02	4 x 10/100/1000Tx FastConnect
A03, B03, C03, D03, E03, F03	4 x 10/100/1000Tx M12 A-Coded
A06, B06, C06, D06, E06, F06	4 x 1000LX - Singlemode, 1310nm, SC , 10km
A07, B07, C07, D07, E07, F07	4 x 1000LX - Singlemode, 1310nm, LC , 10km
A08, B08, C08, D08, E08, F08	4 x Blank SFP
A10, B10, C10, D10, E10, F10	4 x 1000LX SFP - Singlemode, 1310nm, LC, 10km
A11, B11, C11, D11, E11, F11	4 x 1000LX SFP - Singlemode, 1300nm, LC, 25km
A12, B12, C12, D12, E12, F12	4 x 1000LX SFP - Singlemode, 1550nm, LC, 70km
A13, B13, C13, D13, E13, F13	4 x 100FX - Multimode, 1300nm, ST, 2 km
A14, B14, C14, D14, E14, F14	4 x 100FX - Multimode, 1300nm, SC, 2km
A15, B15, C15, D15, E15, F15	4 x 100FX - Singlemode, 1310nm, ST, 20km

Component Configuration	Component Description
A16, B16, C16, D16, E16, F16	4 x 100FX - Singlemode, 1310nm, SC, 20km
A17, B17, C17, D17, E17, F17	4 x 100FX Singlemode, 1310nm, LC, 20km
A18, B18, C18, D18, E18, F18	4 x 100FX Singlemode, 1310nm, SC, 50km
A19, B19, C19, D19, E19, F19	4 x 100FX - Multimode, 1300nm, LC, 2km
A20, B20, C20, D20, E20, F20	4 x 100FX Singlemode, 1310nm, LC, 50km
A21, B21, C21, D21, E21, F21	4 x 100FX Singlemode, 1310nm, SC, 90km
A22, B22, C22, D22, E22, F22	4 x 100FX Singlemode, 1310nm, LC, 90km
A23, B23, C23, D23, E23, F23	4 x 1000LX Singlemode, 1310nm, SC, 25km
G62, H62	2 x 10/100/1000Tx FastConnect
G63, H63	2 x 10/100/1000Tx M12 A-Coded
G65, H65	2 x Blank SFP
G67, H67	2 x 1000SX SFP - Multimode, 850nm, LC, 500m
G68, H68	2 x 1000LX SFP - Singlemode, 1310nm, LC, 10km
G69, H69	2 x 1000LX SFP - Singlemode, 1310nm, LC, 25km
G70, H70	2 x 1000LX SFP - Singlemode, 1310nm, LC, 70km
G71, H71	2 X 100FX SFP - Multimode, 1310nm, LC 2km

Section 5.6

M969F

Table 19 below lists M969F Module's excluded configurations.

Table 19: M969F Excluded Configurations

Component Configuration	Component Description
A01	1x100FX Multimode, LC connectors 1300nm - no ports
A02	1x1000SX Multi Mode, LC connectors 850nm -no ports
A03	1x100FX Single Mode, LC connectors 20km -no ports
A04	2x100FX Multimode, LC connectors 1300nm
A05	1x100FX Singlemode, LC connectors 90km -no ports
A06	1x100FX Singlemode LC connectors 50km -no ports
A07	1x1000LX Singlemode, LC connectors 10km -no ports
A08	1x1000LX Singlemode, LC connectors 25km -no ports
A10	2x100FX Singlemode, LC connectors 90km
A11	2x100FX Singlemode, LC connectors 20km
A12	2x100FX Singlemode, LC connectors 50km

Component Configuration	Component Description
A13	2x1000LX Singlemode, LC connectors 10km
A14	2x1000LX Singlemode, LC connectors 25km

Section 5.7

RS900F

Table 20 below lists RS900F Module's excluded configurations.

Table 20: RS900F Excluded Configurations

Component Configuration	Component Description
A01	2 x 10/100TX,
A02	1 x 100FX - Multimode, 1300nm, MTRJ connector, and 1x no port
A03	2 x 100FX - Multimode, 1300nm, MTRJ connector
A04	1 x 100FX - Multimode, 1300nm, SC connector, and 1x no port
A05	2 x 100FX - Multimode, 1300nm, SC connector
A06	1 x 100FX - Multimode, 1300nm, SC connector, and 1 x 100FX - Singlemode, Standard 20km
A07	1 x 100FX - Multimode, 1300nm, ST connector, and 1x no port
A08	2 x 100FX - Multimode, 1300nm, ST connector
A10	1 x 100FX - Multimode, 1300nm, ST connector, and 1 x 100FX - Singlemode, Standard 20km
A11	1 x 100FX - Multimode, 1300nm, LC connector, and 1x no port
A12	2 x 100FX - Multimode, 1300nm, LC connector
A13	1 x 100FX - Multimode, 1300nm, LC connector, and 1 x 100FX - Singlemode, Standard 20km
A14	1 x 100FX - Singlemode, 1310nm, ST connector, Standard 20km, and 1x no port
A15	2 x 100FX - Singlemode, 1310nm, ST connector, Standard 20km
A16	1 x 100FX - Singlemode, 1310nm, LC connector, Standard 20km, and 1x no port
A17	2 x 100FX - Singlemode, 1310nm, LC connector, Standard 20km
A18	1 x 100FX - Singlemode, 1310nm, LC connector, Standard 20km, and Intermediate Reach 50km
A19	1 x 100FX - Singlemode, 1310nm, LC connector, Standard 20km, and Long Reach 90km
A20	1 x 100FX - Singlemode, 1310nm, LC connector, Intermediate Reach 50km, and 1x no port
A21	2 x 100FX - Singlemode, 1310nm, LC connector, Intermediate Reach 50km
A22	1 x 100FX - Singlemode, 1310nm, LC connector, Long Reach 90km, and 1x no port
A23	2 x 100FX - Singlemode, 1310nm, LC connector, Long Reach 90km
A24	1 x 100FX - Singlemode, 1310nm, SC connector, Standard 20km, and 1x no port
A25	2 x 100FX - Singlemode, 1310nm, SC connector, Standard 20km

Component Configuration	Component Description
A26	1 x 100FX - Singlemode, 1310nm, SC connector, Standard 20km, and Intermediate Reach 50km
A27	1 x 100FX - Singlemode, 1310nm, SC connector, Standard 20km, and Long Reach 90km
A28	1 x 100FX - Singlemode, 1310nm, SC connector, Intermediate Reach 50km, and 1x no port
A29	2 x 100FX - Singlemode, 1310nm, SC connector, Intermediate Reach 50km
A30	1 x 100FX - Singlemode, 1310nm, SC connector, Intermediate Reach 50km, and Long Reach 90km
A31	1 x 100FX - Singlemode, 1310nm, SC connector, Long Reach 90km, and 1x no port
A32	2 x 100FX - Singlemode, 1310nm, SC connector, Long Reach 90km
B01	1 x 10/100TX
B02	1 x 100FX - Multimode, 1300nm, MTRJ connector
B04	1 x 100FX - Multimode, 1300nm, ST connector
B05	1 x 100FX - Multimode, 1300nm, LC connector
B06	1 x 100FX - Singlemode, 1310nm, ST connector, Standard 20km
B07	1 x 100FX - Singlemode, 1310nm, LC connector, Standard 20km
B08	1 x 100FX - Singlemode, 1310nm, LC connector, Intermediate Reach 50km
B09	1 x 100FX - Singlemode, 1310nm, LC connector, Long Reach 90km
B10	1 x 100FX - Singlemode, 1310nm, SC connector, Standard 20km
B11	1 x 100FX - Singlemode, 1310nm, SC connector, Intermediate Reach 50km
B12	1 x 100FX - Singlemode, 1310nm, SC connector, Long Reach 90km

Section 5.8

RS900GF

Table 21 below lists RS900GF Module's excluded configurations.

Table 21: RS900GF Excluded Configurations

Component Configuration	Component Description
A01	Dual 1000X SFP
A02	Dual 1000SX Multimode, LC 850nm, 500m
A03	Dual 1000LX Singlemode, LC 1310nm, 10km
A05	Dual 1000LX Singlemode, SC 1310nm, 10km
A06	Dual 1000LX Singlemode, SC 1310nm, 25km

Section 5.9

RS416F

Table 22 below lists RS416F Module's excluded configurations.

Table 22: RS416F Excluded Configurations

Component Configuration	Component Description
A01, B01, C01, D01	4 x RS232/RS422/RS485, via DB9
A02, B02, C02, D02	4 x RS232/RS422/RS485, via RJ45
E02, F02	2 x 10FL - Multimode, 850nm, ST
E03, F03	2 x 100FX - Multimode, 1300nm, ST
E04, F04	2 x 100FX - Multimode, 1300nm, SC
E05, F05	2 x 100FX - Multimode, 1300nm, LC
E06, F06	2 x 100FX - Multimode, 1300nm, MTRJ
E07, F07	2 x 100FX - Singlemode, 1300nm, ST, 20km
E08, F08	2 x 100FX - Singlemode, 1300nm, SC, 20km
E09, F09	2 x 100FX - Singlemode, 1300nm, LC, 20km
E10, F10	2 x 100FX - Singlemode, 1300nm, SC, 50km
E11, F11	2 x 100FX - Singlemode, 1300nm, LC, 50km
E12, F12	2 x 100FX - Singlemode, 1300nm, SC, 90km
E13, F13	2 x 100FX - Singlemode, 1300nm, LC, 90km

Section 5.10

RS940GF

Table 23 below lists RS940GF Module's excluded configurations.

Table 23: RS940GF Excluded Configurations

Component Configuration	Component Description
A01	Dual 10/100/1000TX RJ45
A02	Dual 1000X SFP, (Mini-GBIC). Order SFP Optics Separately
A04	Dual 1000LX Singlemode, LC 1310nm, 10km
A05	Dual 1000LX Singlemode, LC 1310nm, 25km
A06	Dual 1000LX Singlemode, SC 1310nm, 10km
A07	Dual 1000LX Singlemode, SC 1310nm, 25km

