National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Motorola Solutions, Inc.

RFS7000-GR Wireless LAN Switch and AP-7131N Wireless Access Point

Report Number: CCEVS-VR-VID10472-2014
Dated: March 28, 2014
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Paul A. Bicknell

The MITRE Corporation, Bedford, MA

Jean E. Petty

The MITRE Corporation, McLean, VA

Common Criteria Testing Laboratory

Kenji Yoshino

Kris Kolstad

Michelle Ruppel

Marvin Byrd

Ryan Day

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the RFS7000-GR Wireless LAN Switch: Hardware Model: RFS-7010-1000-WR, Rev. G with Software Version: 4.1.4.0-029GR and the AP-7131N Wireless Access Point: Hardware Models: AP-7131N-66040-FGR Rev. D and the AP-7131N-66040-FWW Rev. F with Software Version: 4.0.4.0-045GRN.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The AP-7131N devices protect data exchanged with wireless client devices using the IEEE 802.11i wireless security protocol; the RFS7000 provides additional capabilities for management and user data protection. In the evaluated configuration, one RFS7000-GR appliance manages multiple AP-7131N devices; supporting up to 1024 AP-7131N wireless access points.

The RFS7000-GR portion of the TOE is a rack-mounted hardware appliance in a 1U chassis; it includes four (4) Gigabit Ethernet ports, which provide network connectivity, and one (1) 100Mbit Ethernet port (unused). An RS-232 serial interface (using RJ-45 connector) is used for local administration; this is also referred to as the console.

The AP-7131N portion of the TOE has one (1) LAN, one (1) WAN port, one (1) serial port, six (6) LEDs, one (1) reset button and six (6) antennas. An RS-232 serial interface (using RJ-45 connector) is used for local administration; this is also referred to as the console.

The TOE supports two (2) deployment options, a standalone deployment and a Mesh deployment. In the standalone deployment, all AP-7131Ns are connected directly to the LAN and/or WAN wired networks. Wireless users connect to the AP via the 802.11a/b/g/n wireless communication link.

In a Mesh deployment, only one (1) AP-7131N must be connected directly to the LAN and/or WAN wired network; this AP is configured as a base bridge. Another AP-7131N, configured as a client bridge, can connect to the wired network through the base bridge via 802.11a/b/g/n wireless communication link. An AP-7131N can be configured as both base bridge and client bridge, allowing the AP to act as a repeater; the Mesh configuration supports as many as three (3) repeaters connected in series. All client and base bridges are capable to serve as fully functional APs, connecting to wireless users via 802.11a/b/g/n. Each client bridge must authenticate itself to the corresponding base bridge using Pre-Shared Keys (PSK).This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

In either configuration, the AP-7131N(s) interacts with a RFS7000-GR switch; receiving configuration data from the RFS7000-GR, allowing the RFS7000-GR to manage the AP-7131N(s) remotely. The RFS7000-GR does not have its own radio interfaces; it uses the radio interfaces of the adopted APs.

Table 1: Operational Environment Components

Component	Description
Console	RS-232 Console Interface for local management of the TOE
SSH Client	SSHv2 client supporting DH Group 14, AES-CBC ciphers, and HMAC-SHA-1
HTTPS Client	Web Browser supporting TLSv1 with RSA/AES-CBC/SHA-1 cipher suites and Java Runtime Environment version 1.6 or greater
SFTP Server	SFTP Server supporting SSHv2 with DH Group 14, AES-CBC ciphers, and HMAC-SHA-1
NTP Server	NTPv4 Server supporting an IPsec tunnel to protect communication with the TOE
Syslog Server	Syslog Server supporting an IPsec tunnel to protect communication with the TOE
RADIUS Server (optional)	RADIUS Server supporting an IPsec tunnel to protect communication with the TOE
LDAP Server (optional)	LDAP Server supporting an IPsec tunnel to protect communication with the TOE
SNMP Manager (optional)	SNMPv3 Client supporting AES/SHA-1-96 for authentication and privacy

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 2: Product Identification

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Motorola Solutions RFS7000-GR Wireless LAN Switch and AP-7131N Wireless Access Point
Protection Profile	None.
Security Target	Motorola RFS7000 Wireless LAN Switch and AP-7131N Wireless Access Point Security Target, Version 1.51, March 25, 2014
Dates of Evaluation	November 2012 – March 2014
Conformance Result	Pass
Common Criteria Version	3.1 Revision 3
Common Evaluation Methodology (CEM) Version	3.1 Revision 3
Evaluation Technical Report (ETR)	14-2359-R-0012 V1.1
Sponsor/Developer	Motorola Solutions, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino Kris Kolstad Michelle Ruppel Marvin Byrd Ryan Day
CCEVS Validators	Paul A. Bicknell Jean E. Petty

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before November 2, 2012.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access
- Trusted Path/Channel
- Intrusion Detection
- Protection of the TSF

4.1 Security Audit

The TOE has the ability to selectively generate audit records from potentially security relevant events and transmit these records to the audit server in the environment. The TOE is dependent on the audit server for the storage, the tools to review audit logs, the protection of audit logs from overflow, and the restriction of access to audit logs. The network connection between the TOE and the external audit server is secured using IPSec security protocol.

4.2 Cryptographic Support

The TOE provides cryptographic mechanisms to protect TSF code and data, including mechanisms to encrypt, decrypt, hash, digitally sign data, and perform cryptographic key agreement. The evaluated configuration uses NIST CAVP validated cryptographic algorithms.

4.3 User Data Protection

The TOE protects user data, i.e., only that data exchanged with wireless client devices, using the IEEE 801.11i standard wireless security protocol, mediates the flow of information passing to and from the WAN port, and ensures that resources used to pass network packets through the TOE do not contain any residual information.

The TOE implements a firewall that filters traffic addressed to the TOE as well as traffic passing through the TOE; e.g., all packets flowing to/from the LAN ports on the RFS7000. An administrative user can develop a set of policies that are composed of rules that dictate requirements to be satisfied to pass network packets. The rules can be based on the packet

protocol validity, and/or specific elements in the packet contents such as presumed address, user identity, presumed address of source subject, presumed address of destination subject, transport layer protocol, and the TOE interface on which traffic arrives and departs.

4.4 Identification and Authentication

The TOE keeps a local database of administrator usernames and passwords and utilizes password-based authentication to authenticate administrators connecting remotely using the SSH protocol, HTTPS GUI, or locally using a serial console connection. The TOE also provides a capability to authenticate administrator against an external RADIUS authentication server. When a pre-defined number of unsuccessful authentication attempts for a remote interface (SSH or HTTPS) has been reached, the remote interface is disabled until re-enabled using the local console connection.

The TOE requires the SNMP administrator be authenticated using a username and password before access to the TOE is granted; all SNMP administrator authentication is done locally. Prior to any SNMP access being allowed, the SNMP administrators' access must be configured by the administrator via the CLI or Web UI; SNMP administrators can be added or deleted as required by the administrator.

The TOE requires wireless users and Mesh connected APs to authenticate before access to the wired network is granted by the TOE. The TOE can authenticate wireless users utilizing the RFS7000 internal RADIUS server, or an external RADIUS authentication server; both implement the EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. The trusted channel between the TOE and the external authentication server is protected using the IPsec/IKE security protocol with pre-shared keys. EAP-TLS uses a client certificate for user authentication; the username is embedded in the certificate. EAP-TTLS and EAP-PEAP use a password for user authentication.

4.5 Security Management

The management of the security relevant parameters of the TOE is performed by the authorized administrator; the TOE provides the following management interfaces:

- Command Line Interface (CLI) via
  - Local RS-232 console connection,
  - Remote SSH interface via the LAN, WAN ports, and 802.11 wireless interface
- Remote HTTPS JAVA based Web UI via the LAN, WAN ports, and 802.11 wireless
- Remote SNMPv3 interface via the LAN, WAN ports, and 802.11 wireless

The SNMPv3 interface supports a limited set of administrative functions; these allow an administrator to manage network performance, find and solve network problems, plan for network growth, and gather information from its network components.

The TOE supports the following administrative user roles:

1. Crypto-officer – Cryptographic functions and network management
2. Monitor – Read-only access
3. System Administrator – General system configuration administrative access

4. Web Administrator – Web authorization for hotspot user access
5. Superuser – Administrative root access
6. SNMP administrator – Remote administrative access
7. Wireless user – Wireless users can pass data through the TOE but do not have direct access

4.6 TOE Access

The TOE displays an advisory/warning message before establishing a user session.

The TOE terminates administrative sessions after an administrator configurable time interval of inactivity is reached for SSH, Local CLI, and Web UI sessions.

4.7 Trusted Path/Channel

The TOE utilizes SSH, SNMPv2, and TLS to provide trusted paths with authorized administrative users.

The TOE utilizes IPsec and SSH to provide trusted channels to the servers providing authentication services, remote audit, NTP synchronization, and the import/export of configuration files.

4.8 Intrusion Detection

The TOE provides rogue AP detection, i.e., any unauthorized active AP operating within the radio coverage of an authorized AP. When a rogue-AP is detected, the administrative user is notified with a SNMP trap and a syslog message.

4.9 Protection of the TSF

All remote interfaces to the TOE are protected by secure channels; however, the TOE and its underlying hardware and firmware are required to be physically protected from unauthorized access.

The TOE provides the capability to run a set of self-tests on power-on and on demand to verify the correct operation of the TOE's underlying hardware, TOE software and cryptographic modules. Additional cryptographic tests are performed during normal operation. The security of network data is maintained by zeroizing the memory location corresponding to a network packet, after the packet has been processed by the TOE.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all

	administrator guidance.
A.TOE_NO_BYPASS	Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.ACCIDENTAL_CRYPTO_COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.

T.UNAUTHORIZED_ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.
T.UNAUTH_ACCESS_POINT	An attacker may place an unauthorized AP in the radio coverage area of an 802.11 wireless network allowing the attacker to remotely access or attack the network, or configure the unauthorized AP to appear like an authorized AP, giving the attacker access to the Wireless Client's data.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.CRYPTOGRAPHY_VALIDATED	Only NIST CAVP validated cryptographic algorithms are acceptable for key generation and key agreement, and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
P.NO_AD_HOC_NETWORKS	In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

6 Documentation

This section details the documentation that is delivered to the customer.

The TOE is shipped to the user for deployment. The guidance documents are provided through a secure webpage download, and apply to the CC Evaluated configuration.

Document	Revision	Date

Document	Revision	Date
Motorola Solutions RFS7000GR Series RF Switch CLI Reference Guide	72E-161313-01 Revision B	3/2014
Motorola Solutions RFS7000GR Series RF Switch System Reference Guide	72E-161314-01 Revision B	3/2014
Motorola Solutions RFS7000-GR and Adaptive AP7131N-GR Common Criteria Supplement	72E-170134-01 Revision A	3/2014
Motorola Solutions RFS7000GR Series RF Switch Installation Guide	72-161315-01 Revision B	3/2014
RFS7000GR-MIBS-4.1.4.0.zip	N/A	N/A

7 IT Product Testing

This section describes the testing efforts of the Evaluation Team.

7.1 Evaluation Team Independent Testing

The evaluation team used the Vendor's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Vendor's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the Vendor's test plan and procedures

The evaluation team completed a subset of the Vendor's test cases and specified additional tests. Each TOE Security Function was exercised at least once and the evaluation team verified that each test passed. The additional test coverage was determined using the analysis of the Vendor test coverage and the ST.

7.2 Evaluation Team Vulnerability Analysis and Penetration Testing

The evaluation team performed a Vulnerability Analysis of the TOE to identify any obvious vulnerabilities of the product and to demonstrate that they are not exploitable in the intended environment for the TOE operation. The evaluation team conducted a public domain search for vulnerabilities and analysis of vendor design documentation to identify potential vulnerabilities.

Based on the results of the Vulnerability Analysis and Design Documentation Analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with a basic attack potential. The evaluation team conducted penetration testing using the same test configuration that was used for the independent testing.

8 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 + ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in March 2014.

9 Validator Comments/Recommendations

The consumer should note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Please note further that certain network related functionality, including functionality provided by the TOE environment, is excluded the evaluation and no claims are made relative to their security.

Also note that the Security Target for this product describes the security aspects of the RFS7000-GR Wireless LAN Switch operating together with one or more AP-7131N Wireless Access Point(s) operating in adaptive mode, connected together via LAN. The AP-7131N is fully described as a standalone device in a separate Security Target, which is included by reference. The consumer should review both Security Targets to fully understand the security functionality evaluated. To assist the consumer in understanding the scope of this evaluation, both Security Targets are included for this product listing.

10 Security Target

Motorola RFS7000 Wireless LAN Switch and AP-7131N Wireless Access Point Security Target, Version 1.51, March 25, 2014.

Note that the Security Target above references Motorola AP-7131N Wireless Access Point Security Target, Version 1.68, March 11, 2014.

11 Terms

11.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.