National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Motorola Solutions, Inc.

Air Defense 9.0 and AP-7131N Wireless Access Point

Report Number:	**CCEVS-VR-VID10508-2014**
Dated:	**March 31, 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

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 Air Defense Services Platform (ADSP) Version 9.0.0-83 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 ADSP portion of the TOE is a wireless networking security, assurance and management solution, designed to monitor and analyze the 802.11a/b/g/n metadata received from the attached AP-7131N devices. By analyzing this metadata, the ADSP system can detect violations of site-specific wireless security policies.

The AP-7131N Access Point (AP) portion of the TOE is a hardware device that operates both as an Access Point and a wireless IDS sensor. As an AP, the AP-7131N manages inbound and outbound traffic on an 802.11a/b/g/n wireless network providing secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. As a sensor, the AP-7131N monitors network traffic and forwards information to the ADSP server for analysis. The module protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol. The TOE has one (1) physical LAN port supporting two (2) unique LAN interfaces, one (1) physical WAN port, one (1) serial port, six (6) LEDs, one (1) reset button and six (6) antennas.

The Motorola Solutions ADSP Version 9.0 software runs on a pre-configured version of Community Enterprise Operating System (CENTOS) version 6.2; CENTOS runs only the required communications services with all unused ports and functions closed and/or turned off. The required services include SNMPv3, TLS 1.0, SSHv2, NTPv4, SCP, and HTTPS. The ADSP CENTOS is a guest OS that runs on a virtualization engine in the IT environment.

The evaluated configuration excludes the following ADSP features through licensing:

- AP Test
- Centralized Management
- Proximity and Analytics (aka Location Based Services)
- Vulnerability Assessment
- WEP Cloaking
- WLAN Management
- Feature Bundles:
  - Advanced Troubleshooting
  - Assurance Suite

Table 1: Operational Environment Components

Component	Description
Console	RS-232 Console Interface for local management of the AP
VM Server	VM Server running Red Hat Linux 6.2 with KVM Virtualization Engine or VMWare ESXi 5.0 and hosting a Virtual Machine with Minimum 2GB RAM and 2 vCPUs
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 For AP-7131N, Java Runtime Environment (JRE) version 1.6 or greater must be enabled in the web browser. For ADSP, Adobe Flash 10 or greater must be enabled in the web browser.
SFTP Server	SFTP Server supporting SSHv2 with DH Group 14, AES-CBC ciphers, and HMAC-SHA-1
NTP Server	NTPv4 Server Must support an IPsec tunnel with the AP Must support MD5 authentication with ADSP.
Syslog (optional for ADSP)	Syslog Server Must support an IPsec tunnel with the AP
RADIUS Server (optional, AP only)	RADIUS Server supporting an IPsec tunnel to protect communication with the AP
LDAP Server (optional, AP only)	LDAP Server supporting an IPsec tunnel to protect communication with the AP
SNMP Manager (optional)	SNMPv3 Client supporting AES/SHA-1-96 for authentication and privacy
Infrastructure Switch (optional)	Infrastructure Switch supporting q-bridge SNMP MIB variables

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 ADSP and AP-7131N Wireless Access Point
Protection Profile	None.
Security Target	Motorola AirDefense 9.0 and AP-7131N Wireless Access Point Security Target, Version 1.10, March 19, 2014
Dates of Evaluation	February 2013 – 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)	14-2247-R-0014 V1.0
Sponsor/Developer	Motorola Solutions, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino 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 February 12, 2013.

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 AP-7131N portion of the TOE has the ability to selectively generate audit records for 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.

The ADSP portion of the TOE has the ability to generate audit records for potentially security relevant events. The audit records can be viewed or exported by users with the “Reporting” permission. Audit records can be backed up to an external SFTP or SCP server supporting SSHv2.

The ADSP portion of the TOE utilizes its underlying CENTOS services to provide an audit capability that allows generating audit records for security critical events; the events that are audited are preconfigured and are not selectable by an administrator.

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 ADSP portion of the TOE provides attribute access control to limit access of users to allowed functions based on the permissions assigned each user.

The AP-7131N portion of 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 AP-7131N portion of the TOE implements a firewall that filters traffic addressed to the TOE as well as traffic passing through the TOE. 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 AP-7131N portion of the TOE keeps a local database of administrator usernames and passwords and utilizes password-based authentication to authenticate administrators connecting remotely using SSH protocol, 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 administrator has been reached, the remote interface (SSH or HTTPS) is disabled until re-enabled using the local console connection.

The AP-7131N portion of 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 AP-7131N portion of the TOE can authenticate wireless users utilizing an internal RADIUS server (only accessible to by the TOE), or an external RADIUS authentication server; both implement EAP-TLS, EAP-TTLS and EAP-PEAP authentication protocols. The trusted channel between the TOE and the external authentication server is protected using 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.

The ADSP portion of the TOE only allows administrative access. All administrative users must be authenticated prior to performing any action. The TOE also enforces password complexity rules when administrative users create or change passwords. These rules can be configured by an administrator with the "System Configuration" permission. When a pre-defined number of unsuccessful authentication attempts for a remote administrator has been reached, the remote administrator's account is disabled until re-enabled by an administrator with the "System Configuration" permission.

4.5 Security Management

The management of the security relevant parameters of the AP-7131N portion 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 AP-7131N's 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 ADSP portion of the TOE provides a limited CLI that is used for basic device management functions such as setting the network configuration and restarting the server.

The ADSP portion of the TOE provides a HTTPS Flash based Web UI that is used for all other management functions.

The ADSP portion of the TOE supports the following permissions that can be assigned to administrative users:

1. System Configuration
2. Device Tuning
3. Network Management
4. Alarm Criticality
5. Alarm Management
6. Network Management
7. Appliance Management
8. Threat Mitigation
9. Reporting

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, TLS, and SNMPv3 to provide trusted paths with authorized administrative users.

The AP7131N portion of 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.

The ADSP portion of the TOE utilizes SSH and SNMPv3 to provide trusted channels to a server providing remote audit backup, import/export of TSF data, and port suppression/ACL commands.

The TOE utilizes a TLS trusted channel for intra-TSF communications.

4.8 Intrusion Detection

The TOE provides the following WIDS functions:

- Traffic Analysis:
  - Provides the ability to analyze data received by the TOE or the TOE IT Environment regarding information related to security events.
- Reaction:
  - Provides the creation of alarms upon detection of a security violation that may constitute threats to the network. Also allows automatic or manual mitigation of detected security threats.
- Restricted Data Review:
  - Allows data collected and analyzed against Allowable Use Policies to be reviewed by an authorized administrator.
- Data Collection:
  - Provides collection of events occurring on monitored IT systems whose occurrence indicates a potential violation of the TSP.

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 a 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.
T.ATTACK	An attacker denies the service of a wireless Access Point by flooding it with traffic, without being detected.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE and to the IT Environment.
T.POLICY_VIOLATE	An attacker gains unauthorized use of the network by broadcasting wireless network traffic in violation of the Allowable Use Policies, without being detected.
T.SECURITY_BYPASS	The TOE might be subject to malicious tampering or bypass of its security mechanisms.
T.TOE_FAILURE	The TOE software or hardware fails to operate, allowing adversaries to attack the wireless network undetected.

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.

6.1 Guidance Documentation

Document	Revision	Date
ADSP Common Criteria Supplement	MN000765A01 Rev. A	3/19/2014
Motorola Solutions AP-7131N-FGR Access Point Installation Guide	72-161312-01 Revision B	March 2014
Motorola Solutions AP-7131N-FGR Product Reference Guide	72E-161311-01 Revision B	March 2014
Motorola Solutions AP7131N-GR Common Criteria Supplement	72E-170133-01 Revision A	March 2014
AP7131N-GR MIBS 4.0.4.0	N/A	N/A

6.2 Security Target

Document	Revision	Date
Motorola AirDefense 9.0 and AP-7131N Wireless Access Point Security Target	1.10	3/19/2014
Motorola AP-7131N Wireless Access Point Security Target	1.68	3/11/2014

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 has 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 from the evaluation and no claims are made relative to their security.

Also note that the Security Target describes the security aspects of the Air Defense Services Platform (ADSP) operating together with one or more AP-7131N Wireless Access Point(s) operating as both Access Point and as a WIDS sensor, connected together via LAN. The AP-7131N operating as Access Point 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 AirDefense 9.0 and AP-7131N Wireless Access Point Security Target, Version 1.10, March 19, 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.