National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

AirDefense Enterprise Version 7.2

Report Number: CCEVS-VR-VID10236-2008

Dated: 10 March 2008

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)

Jandria Alexander (Senior Validator)

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

SAIC Inc.

Columbia, Maryland

Table of Contents

TABLE OF CONTENTS III

1. EXECUTIVE SUMMARY 1

1.1. INTERPRETATIONS 3

2. IDENTIFICATION 4

3. SECURITY POLICY 5

3.1.1. Security Audit 5
3.1.2. Identification and Authentication (I&A) 5
3.1.3. Self Protection 5
3.1.4. Management 5
3.1.5. Traffic Analysis 6

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE 7

4.1. PERSONNEL SECURITY ASSUMPTIONS 7
4.2. PHYSICAL SECURITY ASSUMPTIONS 7
4.3. OPERATIONAL SECURITY ASSUMPTIONS 7
4.4. THREATS COUNTERED AND NOT COUNTERED 8
4.5. ORGANIZATIONAL SECURITY POLICIES 8
4.6. CLARIFICATION OF SCOPE 8

5. ARCHITECTURAL INFORMATION 10

5.1. EVALUATED CONFIGURATION 10
5.2. HARDWARE/SOFTWARE COMPONENTS 11

6. DOCUMENTATION 12

7. IT PRODUCT TESTING 13

8. EVALUATED CONFIGURATION 14

9. RESULTS OF THE EVALUATION 15

10. VALIDATOR COMMENTS 16

11. ANNEXES 17

12. SECURITY TARGET 18

13. GLOSSARY 19

14. BIBLIOGRAPHY 20

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (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. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of AirDefense Enterprise 7.2, the target of evaluation (TOE), conducted by SAIC Incorporated, the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated.

The evaluation by SAIC was performed in accordance with the United States evaluation scheme and was completed in October 2007. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was prepared by Apex Assurance Group, LLC. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the AirDefense Enterprise 7.2 Security Target.

The AirDefense Enterprise 7.2 (ADE 7.2) is a wireless network security solution designed to remotely monitor the traffic received from any 802.11a/b/g source. By monitoring this traffic, the AirDefense Enterprise 7.2 system can detect attacks and violations of site-specific wireless security policies defined within the ADE 7.2 user interface.

The AirDefense Enterprise 7.2 system runs on a single, purpose-built, dedicated server appliance which is termed the 2270 appliance, and also includes separate, purpose built remote sensors that can range from 1 to 300 on one single server appliance. The 2270 Server appliance runs a pre-configured version 2.4.32 of the Red Hat Linux Operating System that has been tuned to only run a few key services (SNMP, SSL, syslog and HTTPS), with all other ports and functions closed and/or turned off. The core AirDefense Enterprise 7.2 (ADE 7.2) server software runs on top of the Red Hat kernel.

The 2270 Server appliance processes all of the collected wireless network traffic messages from each of the Remote Sensors that are connected to it. The Server can detect wireless attacks and violations of site-specific wireless security policies (i.e., allowable use policies) that can be crafted by a site administrator or manager. Users access the correlated data through the AirDefense Management GUI, which is accessible via a secure, remote, web-based administration Java

application. Users log into the AirDefense Management GUI to view all security relevant information, including traffic analysis summaries that are presented on the main "dashboard", review the system audit events, and review all alarms or policy violations.

The M510 and M520 remote sensors are also dedicated stand alone devices that are tuned for listening to all wireless 802.11a/b/g traffic that is present within its field of reception. These dedicated sensors run an embedded, pre-configured version of the Red Hat operating system that has been modified to only have specific services active. The AirDefense Sensor Software version 4.5.0.13 runs on top of the Red Hat OS and provides the services to collect information from the wireless devices and transmit it to the server for processing. The sensors communicate with the remote server appliance over a **wired** network utilizing a dedicated AES encrypted TCP/IP socket connection.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non –TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment.

The TOE makes use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules are asserted by the vendor to operate correctly. No independent certification under National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 was performed on this product. In addition, the cryptographic functions of the TOE were not evaluated further during the CC evaluation. **NOTE:** Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

The TOE recognizes four roles; Administrator, Manager, Network Operator and Guest. These roles have differing privileges to view and modify Trusted Security Function Data. It should be noted that even the "Guest" role has the ability to view (but not modify) some security data via the "Dashboard". It may be important for users of this system to carefully consider how to use the "Guest" role.

The technical information included in this report was obtained from the Evaluation Technical Report for AirDefense Enterprise 7.2 (ETR) Parts 1 and 2 produced by SAIC.

1.1. Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that no international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) are applicable to this evaluation. The TOE is also compliant with all International interpretations with effective dates on or before March 30, 2007.

The Evaluation Team also determined that there were no applicable NIAP interpretations that were applicable to this evaluation on or before March 30, 2007.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	AirDefense Enterprise 7.2
Protection Profile	None
Security Target	*Security Target for Common Criteria Evaluation: AirDefense Enterprise 7.2*, Version 1.9, dated February 8, 2008.
Dates of evaluation	March 2007 through October 2007
Evaluation Technical Report	*Evaluation Technical Report for AirDefense Enterprise 7.2, Part 1,* Version 1.1, Dated 31 December 2007 and *Evaluation Technical Report for AirDefense Enterprise 7.2, Part 2(Proprietary),* Version 1.3, Dated 20 February 2008
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on March 30, 2007
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on March 30, 2007
Sponsor	AirDefense, Inc., 4800 North Point Parkway Suite 100, Alpharetta, GA 30022
Developer	AirDefense, Inc., 4800 North Point Parkway Suite 100, Alpharetta, GA 30022
Evaluators	Dan Campbell and Eve Pierre of SAIC Incorporated
Validation Team	Jandria Alexander and Mike Allen of The Aerospace Corporation

3. SECURITY POLICY

The security policies enforced by the AirDefense Enterprise 7.2 TOE are described in the following sections.

3.1.1. Security Audit

The TOE generates audit records of security relevant events including user authentication as well as configuration changes by an administrator, such as creating, modifying, or deleting a policy. Authenticated users with the Admin role are able to review audit events through the AirDefense Management GUI interface.

3.1.2. Identification and Authentication (I&A)

The TOE performs the I&A function for the AirDefense Management GUI interface. There are 4 user roles, which are Admin, Manager, Network Operator, and Guest. The TOE requires the users to be authenticated before any access to the management interfaces is granted. Authentication requires a valid username and password combination.

3.1.3. Self Protection

The TOE protects security functions via the Server and Sensor Operating Systems, which maintain a security domain for their own execution. The TOE protects the TSF in the scope of control of the respective OS from interference and tampering by untrusted subjects. The TOE also provides secure communication between components by requiring the use of SSL communications (HTTPS) between the Server and the AirDefense Management GUI and a SSL/TLS tunnel between the Server and Sensor(s). The cryptographic functions implemented to achieve these secure communications are **not** FIPS certified but are vendor asserted.

3.1.4. Management

The TOE provides the ability for the Administrator to create and manage Allowable Use Policies. These policies are created and managed through the web-based administrative interface. The attributes that these policies can be based on are: wireless authentication mode, channel (wireless broadcast frequency), connection rate, Service Set Identifier (SSID) broadcast status, wireless protocol (e.g. WEP), access point ID, host ID, date, and time of day.

A graphical user interface supports creating the policies. The Administrator uses HTTPS pull-down menus to specify the attributes they wish to include in a policy, then an input field or pull-down menu to specify the value that the attribute must meet.

The TOE associates users with one of four roles (Admin, Manager, Network Operator, and Guest), and each role has a specific set of available services. The user in the admin role is responsible for the overall configuration and administration of the TOE. The other roles are more restricted.

3.1.5. Traffic Analysis

The TOE controls the flow of information in a wireless network by comparing various parameters of connected devices against allowable use policies defined by the administrator. If the device is not allowed for use on the wireless network, the TOE will create an alarm and drop the device from the network (if configured to do so). All of the authorized user roles except the "Guest" role have the ability to view and clear alarms.

Additionally, alarms are generated when traffic analysis suggests that an identity theft attack is detected or when traffic that doesn't match Allowable Use Policies is detected.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. Personnel Security Assumptions

The following personnel assumptions are identified in the Security Target:

Table 2 – Personnel Assumptions

A.PASSWORD	Administrators will use passwords that conform to the administrator guidance.
A.NOEVIL	The administrator is competent and will install and configure the TOE according to the administrator guidance.

4.2. Physical Security Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Physical Assumptions

A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation of the hardware.

4.3. Operational Security Assumptions

The following operational security assumptions are identified in the Security Target:

Table 4 – Physical Assumptions

A.NETWORK	There will be a wired network that supports TCP communications connecting the Server to the Remote Sensors. This network functions properly.
A.SINGLE_POINT	All wireless communications received by the sensors flow through the server.

4.4. Threats Countered and Not Countered

The TOE and Operating IT Environment are designed to fully or partially counter the following threats:

Table 5 – Threats Countered

T.ADMIN_NOAUTH	An attacker gains administrative privileges to the TOE by accessing the TOE through its administrative interface, and this access occurs without notice.
T.ATTACK	An attacker denies the service of a wireless Access Point by flooding it with traffic, without being detected.
T.COMP_MANAGE	Data may be compromised while traversing the connection between the TOE components.
T.NO_ACCOUNT	An administrator might perform actions for which they are not accountable.
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.SEC_BYPASS	The TOE might be subject to malicious tampering or bypass of its security mechanisms.

4.5. Organizational Security Policies

There are no applicable organizational security policies

4.6. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- The Command Line Interface (CLI) is used only during the installation and initial configuration of the TOE. As specified in the Administrative Guidance, only the AirDefense Management GUI should be used once the TOE is running in the evaluated configuration.

- Encryption of communications using SSL between the Sensors and the Server components and between the AirDefense Management GUI and the Server is required. The evaluation team did verify that communication between the components is encrypted. Testing did confirm the presence of encrypted communication; however the encryption mechanisms used have not been FIPS certified.

- The following guidance is provided on user roles:
  - Administrative Users: Have both read and write privileges throughout the TOE, in every module within the server GUI application. These privileges include deleting users, adding new users to the TOE, configuring policies, sensor configurations, configuring alarm priorities, clearing alarms, enabling notifications performing system backups and restores and reviewing the audit log.
  - Manager Users: have the same privileges as the Admin role, with the exception that a Manager cannot view or modify user accounts or access to the audit logs.
  - Network Operator Users: have read-only access to the Alarm Manager but can clear alarms and have read-only access to the policy manager, but has no access to Alarm Configurations or to the Appliance Manager module which includes user account management, notifications, database backups and restores and access to the audit logs.
  - Guest Users: only have read-only access to the following AirDefense Enterprise GUI program areas: Dashboard, Alarm Manager, Sensor Manager and Policy Manager, no other system areas can be viewed or accessed.

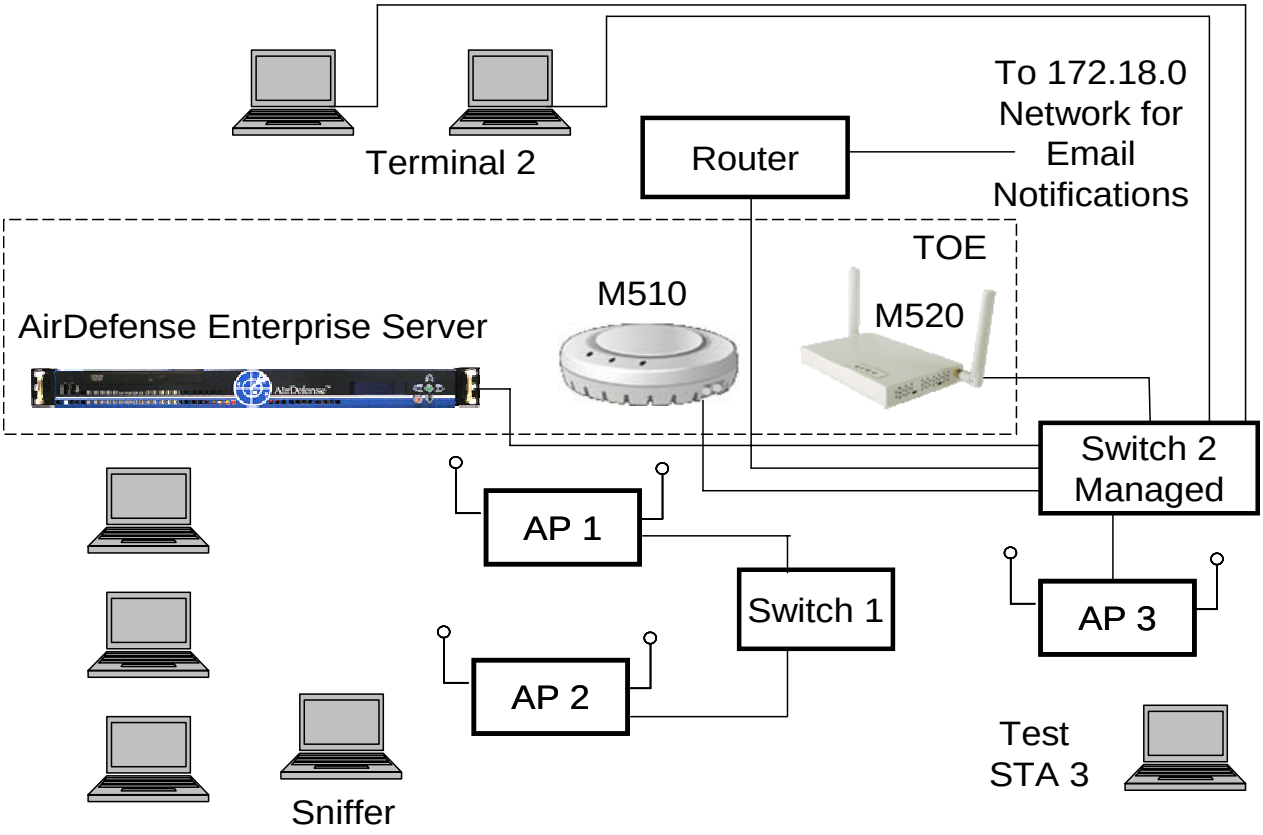
5. ARCHITECTURAL INFORMATION

The AirDefense Enterprise 7.2 (ADE 7.2) is a wireless network security solution designed to remotely monitor the traffic received from any 802.11a/b/g source. By monitoring this traffic, the ADE 7.2 system can detect identity theft attacks and violations of site-specific wireless security policies defined within the ADE 7.2 user interface.

The ADE 7.2 system runs on a single, purpose-built, dedicated server appliance which is termed the 2270 appliance, and also includes one or more separate, purpose built remote sensors (M510 and M520) that can range from 1 to 300 connected to a single server appliance. The 2270 Server appliance runs a pre-configured version 2.4.32 of the Red Hat Linux Operating System that has been tuned to only run a few key services, with all other ports and functions closed or turned off. The core ADE 7.2 server software runs on top of the Red Hat Kernel.

5.1. Evaluated Configuration

Figure 1 - Test Evaluated Configuration



The Red Hat services that are present in the operation of the server include SNMP functions, SSL functions, internal syslog functions, and HTTPS Web services. Running on top of this Red Hat kernel is the core ADE 7.2 server software.

The 2270 Server appliance processes all of the collected wireless network traffic messages from each of the Remote Sensors connected to it. The Server can detect wireless identity thefts, and violations of site-specific wireless security policies (allowable use policies) that can be crafted by a site administrator or manager. Users access the correlated data through the AirDefense Management GUI, which is accessible via a secure, remote, web-based administration Java application. Users log into the AirDefense Management GUI to view all security relevant information, including traffic analysis summaries that are presented on the main dashboard, review the system audit events, and review all alarms or policy violations.

The M510 and M520 remote sensors are also dedicated stand alone devices that are tuned for listening to all wireless 802.11a/b/g traffic that is present within its field of reception. These dedicated sensors run an embedded, pre-configured version of the Red Hat operating system that has been modified to only have specific services. The AirDefense Sensor Software version 4.5.0.13 runs on top of the Red Hat OS and provides the services to collect information from the wireless devices and transmit it to the server for processing. The sensors communicate with the remote server appliance over a **wired** network utilizing a dedicated AES encrypted TCP/IP socket connection.

5.2. Hardware/Software Components

Table 6 identifies software and hardware components and indicates whether each component is in the TOE or the Environment:

Table 6 – Enterprise 7.2 Components

Component	Description	TOE	Environment
Server Software	Processes all network traffic received by the hardware network interface, and provides a secure, web-based administration interface	✓	
Server Hardware	Dedicated, purpose-built hardware devices for running AirDefense Server Software	✓	
AirDefense Management GUI	Web-based application for managing Server and Sensor Software	✓	
Management Workstation	Runs Web-based AirDefense Management GUI via browser connection to Server software		✓
Sensor Software	Receives wireless traffic and sends the encrypted headers to the Server for processing. These communications are encrypted to protect their integrity.	✓	
Sensor Hardware	Dedicated, purpose-built hardware devices for running AirDefense Sensor Software	✓	

6. DOCUMENTATION

Following is a list of useful documents supplied by the developer and shipped with the product.

- AirDefense User Guide, Release 7.2, Issue 1.3, April 2007
- Sensor Quick Start Guide for Enterprise 7.2
- Server Quick Start Guide for Enterprise 7.2
- User Quick Start Guide for Enterprise 7.2
- Pre-Installation Check List AirDefense Server

The security target used is:

- Security Target for Common Criteria Evaluation: AirDefense Enteprise 7.2, February 8, 2008, Version 1.9.

7. IT PRODUCT TESTING

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed the entire vendor test suite, and devised an independent set of team tests and penetration tests using the test configuration shown in Figure 1 above. The vendor tests, team tests, and penetration tests confirmed the security functional requirements in the ST. The tests were conducted using:

- AirDefense 2270 Server Appliance running the AirDefense Enterprise 7.2 Software
- M510 and M520 Sensor Appliances
- 2 Windows XP workstation for the AirDefense Management GUI/SSH terminals
- Network devices: Linksys RT31P2 Router, HPProcure2626 and Symbol WS2000 Switch devices; 3 Cisco Aironet a/b/g devices as Testing Station; Dell/Cisco a/bg as the Attacking Station; Netgear EN104TP as Ethernet Hub; Symbol AP300, Symbol Spectrum 24 and Cisco AP1200 as the 3 Access Points.

The basic test configuration ran the AirDefense Management GUI application to access the Server; to configure the data correlation rules and allowable use policies used by the Server to analyze the information collected by the sensor. The GUI wasi used to review the analyzed data and to generate reports.

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions.

All of the developer tests were run and the results were found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

8. EVALUATED CONFIGURATION

The evaluated configuration is the 2270 server appliance, the M510 and M520 Sensor appliances and a Windows Workstation where the AirDefense Management GUI is installed.

9. 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 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

The SAIC Inc. Common Criteria Testing Laboratory has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished in October 2007. A final passing Validation Oversight Review (VOR) was completed on March 3, 2008.

10. VALIDATOR COMMENTS

The validation team's observations support the evaluation team's conclusion that the AirDefense Enterprise 7.2 product meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

The validation team notes that the claims made and successfully evaluated for the product represent a more limited set of requirements than what might be used for a "normal" product deployment. Specifically, no claims are made for protection of data transmission between the TOE and non –TOE components such as the web browser and the network devices in spite of the fact that it will mostly likely be configured and setup in a distributed fashion over a network whose traffic could well be less than benign. It then becomes quite necessary for the administrators to fulfill the requirements levied on the environment, that is, use of encryption between the sensors and the server.

The TOE makes use of cryptographic modules in order to fulfill some security functions. The Cryptographic modules are asserted by the vendor to operate correctly. No independent certification under National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 was performed on this product. In addition, the cryptographic functions of the TOE were not evaluated further during the CC evaluation. **NOTE:** Users should ensure that they select a product that meets their needs, including FIPS 140-2 compliance, if appropriate.

The TOE recognizes four roles; Administrator, Manager, Network Operator and Guest. These roles have differing privileges to view and modify Trusted Security Function Data. It should be noted that even the "Guest" role has the ability to view (but not modify) some security data via the "Dashboard". It may be important for users of this system to carefully consider how to use the "Guest" role.

11. ANNEXES

None

12. SECURITY TARGET

The security target for this product's evaluation is *Security Target for Common Criteria: AirDefense Enterprise 7.2*, Version 1.9, February 8, 2008.

13. GLOSSARY

There were no special definitions or terms used other than those documented in the CC and CEM.

14. BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, Version 2.3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.
3. Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.
4. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.
5. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.
6. Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.
7. Evaluation Technical Report for AirDefense Enterprise 7.2 Part 1, Version 1.1, December 31, 2007
8. Evaluation Technical Report for AirDefense Enterprise 7.2 Part 2 (Proprietary), Version 1.3, February 20, 2008
9. Security Target for Common Criteria: AirDefense Enterprise 7.2, Version 1.9, February 8, 2008.
10. AirDefense Test Case Execution Guide Enterprise 7.2, Version 1.3, October 9, 2007.
11. AirDefense Vulnerability Assessment Document AirDefense Enterprise 7.2, Version 1.5, December 26, 2007.
12. NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001