Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report
2014/87

Aruba Networks Mobility Controller

11 June 2014
Version 1.1

Amendment Record

Version	Date	Description
1.1	11/06/14	Final release

Executive Summary

The Target of Evaluation (TOE) is the Aruba Networks Mobility Controller (7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620) with ArubaOS 6.3.

The Aruba Networks Mobility Controller is a network device that serves as a gateway between wired and wireless networks and provides command–and–control over Access Points (APs) within the Aruba dependant wireless network. ArubaOS 6.3 is the underlying operating system of the Mobility Controller, which is available in modular chassis or network appliance models:

- Aruba 7000 and 6000 Series: The Aruba 7240, 7220, 7210 and 6000 with M3 blades are designed for corporate headquarters and large campus deployments;

- Aruba 3000 Series : The 3200, 3400 and 3600 are designed for small , medium and large enterprises; and

- Aruba 600 Series are designed for branch offices and similar deployments.

Key features include:

- Secure communication with remote administrators , authentication servers and audit servers;

- Secure management including authentication , verifiable updates and auditing; and

- Self verification of integrity and operation;

This report describes the findings of the IT security evaluation of Aruba Networks Mobility Controller for compliance with the NDPP v1.1.

The report concludes that the product has complied with the NDPP and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC and was completed on 6 May 2014.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) should provide physical security for the TOE; and

b) be aware that APs functionality is outside the scope of the scope of evaluation and was not tested in this case; and

c) ensure the hardware is delivered in tamper evident packaging.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Aruba Networks Mobility Controller for compliance with the NDPP v1.1 and

b) provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is the Aruba Networks Mobility Controller.

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Aruba Networks Mobility Controller (7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620) with ArubaOS 6.3.
Hardware Models	7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620
Software Version	ArubaOS 6.3.1.5-FIPS
Security Target	Aruba Networks Mobility Controller (7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620) with ArubaOS 6.3. Security Target Version 1.12 May 2014.

Protection Profile	US Government Protection Profile for Security Requirements for Network Devices version 1.1 June 8, 2012
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4, CCIMB-2012-09-004 with interpretations as of 24 September 2012.
Sponsor	Aruba Networks, Level 21, 201 Miller Street, North Sydney, NSW 2060, Australia.
Developer	Aruba Networks, Level 21, 201 Miller Street, North Sydney, NSW 2060, Australia.
Evaluation Facility	CSC Australia Pty Limited.

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Chapter 2 - Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architectural components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

The Target of Evaluation (TOE) is the Aruba Networks Mobility Controller (7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620) with ArubaOS 6.3. The Aruba Networks Mobility Controller is a network device that serves as a gateway between wired and wireless networks and provides command–and–control over Access Points (APs) within the Aruba dependant wireless network. ArubaOS 6.3 is the underlying operating system of the Mobility Controller, which is available in modular chassis or network appliance models:

- Aruba 7000 and 6000 Series: The Aruba 7240, 7220, 7210 and 6000 with M3 blades are designed for corporate headquarters and large campus deployments;

- Aruba 3000 Series : The 3200, 3400 and 3600 are designed for small , medium and large enterprises; and

- Aruba 600 Series are designed for branch offices and similar deployments.

Key features include:

- Secure communication with remote administrators , authentication servers and audit servers;

- Secure management including authentication , verifiable updates and auditing; and

- Self verification of integrity and operation.

2.3 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref [1]) contains no explicit security policy statements and this is not a requirement of the NDPP.

2.4 TOE Architecture

The TOE consists of the following major subsystems:

a) **ArubaOS 6.3.1.5-FIPS software.**

The Aruba OS 6.3.1.5-FIPS consists of a base software package with add on software modules that can be activated by installing the appropriate licenses

b) **Aruba Models.**

The difference in the models includes the physical appearance, number of ports, interfaces, throughput and processing speed.

Model	Maximum Access points	Throughput	Maximum users
7240	2048	40Gbs	65,536
7220	1024	40Gbs	32,768
7210	512	28.3Gbs	16,384
6000 with four M3 blades	2048	80Gbs	32,768
3600	128	4Gbs	8,192
3400	64	4Gbs	4,096
3200	32	3Gbs	2,048
650	16	2Gbs	512
620	8	800Mbs	256

Table 2: TOE Chassis and appliance numbers

Aruba mobility controllers are hardware appliances consisting of a multicore network processor, Ethernet interfaces and required supporting circuitry and power supplies enclosed in a metal chassis. The software running on the Mobility Controller is called ArubaOS which consists of two main components, the control plane (CP) and the data plane (DP), both implemented on multiple cores within a single processor. The Control Plane which implements functions which can be handled at a lower speeds such as the Mobility Controller system management, user authentication, internet key exchange and audit logging. The control plane runs the Linux operating system along with various user space applications.
Data Plane implements functions that must be handled at high speeds such as switching functions (forwarding, VLAN Tagging/enforcement, bridging) termination of 802.11 associations/sessions, tunnel termination (IPsec) and deep packet inspection

functions and cryptographic acceleration. The data plane runs a lightweight, propriety real-time OS which is known as “SOS” The Control Plane and Data plane are inseparable. The Control Plane provides the following functions:

a) Monitors and manages critical system resources , including processes, memory and flash;
b) Manages system configuration and licensing;
c) Manages an internal data base used to store licenses and user authentication information;
d) Provides network anomaly detection, hardware monitoring, mobility management, wireless management and radio frequency management services;
e) Provides a Command Line Interface.
f) Provides a web based (HTTPs/TLS) management UI for the mobility controller;
g) Provides authentication services for the system management interfaces; and
h) Provides Syslog services by sending logs to the operating environment.

Administrators do not have access to the Linux command shell or operating system.

The data plane is further subdivided into two subcomponents: Fast Path and Slow Path. The Fast Path implements high speed packet forwarding and sends packets to the Slow Path.

The data plane is implemented on a multi-core processor. The SOS contains an Ethernet Driver, a serial driver, a logging facility, semaphore support, and a crypto driver. In the Aruba 6000 with M3 controller card, an FPGA is also used to control and monitor the switch fabric, Ethernet interface hardware and provide security functionality such as filtering.

The DP and CP run on different hardware platforms but the security functionality remains the same, regardless of the model. The difference in the platforms is in the processors, memory capacity, physical interfaces and FPGA implementation. These differences are based on performance and scalability requirements.

2.5 Clarification of Scope

The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

The TOE provides the following evaluated security functionality:

a) Protected communications

The TOE protects the following information flows.

- **WebUI:** Communications with the administrative user interface (WebUI) is protected using TLS/HTTPS.
- **CLI:** Remote administration visa the command Line interface (CLI) is protected using SSHv2.
- **Syslog:** Syslog Messages are protected using IPsec.
- **Radius:** Radius authentication messages are protected using IPSec.

b) Verifiable updates:

Updates are digitally signed and verified on installation utilising digital signatures.

c) System monitoring and logging:

The TOE maintains an audit log of administrative and security relevant events. Logs can optionally be delivered to a Syslog server.

d) Secure administration:

The TOE provides administrative interfaces for configuration and monitoring. The TOE authenticates administrators and implements session timeouts.

e) Residual Information Clearing:

The TOE ensures the network packets sent from the TOE do not include data left over from processing of previous network information.

f) Self-test:

The TOE performs both power-up and conditional self-tests to verify the correct and secure operation.

g) Cryptographic support:

The TOE uses cryptographic functions provided by FIPS 140-2 validated modules.

- CMVP Certificate #1727
- CMVP Certificate #1865

The entropy design description, justification, operation and health tests are assessed and documented in Aruba Mobility Controller Entropy Information (Ref [14]).

2.5.2 Non-evaluated Functionality and Services.

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB). Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

The following components are in the environment and are required by the TOE to support the evaluated configuration.

Non TOE Components	Description
Access Points	Wireless clients connect to the APs which are connected to the TOE.
Authentication Server	The TOE can utilise a Radius server to authenticate users.
Audit server	The TOE can utilise a Syslog server to store audit records.
Time server	The TOE can utilise a Network Time Protocol (NTP) server to synchronise its system clock with a central time source.
Web browser	The remote administrator can use a web browser to access the web GUI interface.
SSH client	The remote administrator can use the SSH client to access the CLI.

Table 3: Non TOE components

2.6 Usage

2.6.1 Evaluated Configuration

This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

The TOE is generally performs command and control within the Aruba dependant wireless network architecture consisting of one or more Aruba mobility controller. The TOE consists of the software ArubaOS 6.3.1.5-FIPS. The hardware models in scope for this evaluation are as follows.

TOE Components	
Description	**Identification**
Hardware	Aruba Networks model 7240
	Aruba Networks model 7220
	Aruba Networks model 7210
	Aruba Networks model 6000 with four M3 blades
	Aruba Networks model 3600
	Aruba Networks model 3400
	Aruba Networks model 3200
	Aruba Networks model 650
	Aruba Networks model 620

Table 4: TOE Components

2.6.2 Delivery Procedures

Hardware

The customer should ensure the hardware is delivered in tamper evident packaging.

Software

For software, the customer will access Aruba support portal to download images. The customer will be prompted for their login and password. Initial start-up procedures are detailed in the Aruba 6.3. Quick Start Guide (Ref [3]).

2.6.3 Determining the Evaluated Configuration

To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE component hardware models in the Security Target and by following the guidance (Ref [3]).

2.6.4 Documentation

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased.

a) ArubaOS 6.3 Quick Start Guide, Ref 0511320-01;
b) ArubaOS 6.3.x User Guide, Ref 0511497-00;
c) ArubaOS 6.3.x Syslog Messages, Ref 0511324-01;
d) ArubaOS 6.3.x Command Line Interface, Ref 0511500-00;
e) ArubaOS 6.3.1.5 Release Notes, Ref 0511467-05; and
f) Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy.

2.6.5 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

a) A.NO_GENERAL_PURPOSE

It is assumed that there is no general purpose computing capabilities. (E.g. compilers or user applications) available on the TOE other than those services necessary for the operation, administration and support of the TOE.

b) A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

c) A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance.

In addition, the following organisational security policy must be in place:

d) 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.

Chapter 3 - Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the US Government Protection Profile for Security Requirements for Network Devices version 1.1 June 8, 2012 (Ref [4]), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 (Refs [5], [6] and [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (CEM) (Ref [8]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9], [10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Testing

Testing is determined in the Assurance activities in the Protection Profile.

Mapping of Testing to NDPP requirements	
Test ID	**Requirement in NDPP**
TOE Access	FAU_GEN.1
	FTA_SSL_EXT.1
	FTA__SSL.3
	FTA_SSL.4
	FTA_TAB.1
Identification and authentication	FAU_GEN.1
	FIA_PMG.EXT.1
	FIA_UIA_EXT.1
	FIA_UAU_EXT.2
	FIA_UAU.7
Protection of the TOE Security Functions	FAU_GEN.1
	FPT_STM
	FPT_TUD_EXT.1
Trusted Path	FAU_STG_EXT.1

	FAU_GEN.1
	FPT_ITC.1
	FTP_TRP.1
Protocol conformance IPSec	FCS_IPSEC_EXT.1.2
	FCS_IPSEC_EXT.1.3
	FCS_IPSEC_EXT.1.4
	FCS_IPSEC_EXT.1.5
	FCS_IPSEC_EXT.1.6
	FCS_IPSEC_EXT.1.7
	FCS_IPSEC_EXT.1.8
	FAU_GEN.1
Protocol conformance TLS	FCS_TLS_EXT.1
	FCS_HTTPS.EXT.1
	FAU_GEN.1
Protocol conformance SSH	FCS_SSH.EXT.1.3
	FCS_SSH.EXT.1.7
	FAU_GEN.1

Table5: Testing Requirements

3.4 Penetration Testing

The evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. These vulnerabilities discovered and migrated are:

- Click Jacking: during testing the evaluators discover that the WebUI had the potential to be susceptible to the click jacking vulnerability. Following the resolution of the vulnerability the evaluators retested and confirmed that the Click Jacking vulnerability had been removed.
- Cross Sites Requests Forgery: during testing the evaluators discover that the TOE had the potential to be susceptible to XSRF. Following the resolution of the vulnerability the evaluators retested and confirmed that the XSRF vulnerability had been removed.
- Cross Sites Scripting: during testing the evaluators discover that the TOE had the potential to be susceptible to XSS. Following the resolution of the vulnerability the evaluators retested and confirmed that the XSS vulnerability had been removed.

3.4 Entropy

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref [14]).

3.5 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority certifies the evaluation of Aruba Networks Mobility Controller performed by the Australasian Information Security Evaluation Program. CSC has found that Aruba Networks Mobility Controller (Aruba Networks upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the NDPP.

Certification is not a guarantee of freedom from security vulnerabilities.

3.6 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles. PPs provide assurance by a full security target and an analysis of the SFRs in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by testing as outlined in the NDPP assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

3.7 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that users and administrators:

a) should provide physical security for the TOE;

b) be aware that Firewall functionality is outside of the scope of evaluation and was not tested; and

c) ensure the hardware is delivered in tamper evident packaging.

Annex A - References and Abbreviations

A.1 References

1. ST – Security Target for Aruba Networks Mobility Controller (7240, 7220, 7210, 6000, 3600, 3400, 3200, 650, 620) with ArubaOS 6.3 version 1.12, May 2014.

2. 2014 Australian Government Information Security Manual (ISM), Australian Signals Directorate, (available at www.asd.gov.au).

3. User Guidance:

    a) ArubaOS 6.3 Quick Start Guide, Ref 0511320-01

    b) ArubaOS 6.3.x User Guide, Ref 0511497-00

    c) ArubaOS 6.3.x Syslog Messages, Ref 0511324-01

    d) ArubaOS 6.3.x Command Line Interface, Ref 0511500-00

    e) ArubaOS 6.3.1.5 Release Notes, Ref 0511467-05

    f) Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy

4. US Government approved Protection Profile - Protection Profile for Network Devices version 1.1 June 8, 2012.

5. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 Revision 4 CCMB-2012-09-001.

6. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002.

7. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4 CCMB-2012-09-003.

8. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

9. AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.

10. AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.

11. AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.

12. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

13. Aruba Network Mobility Controller, Evaluation Technical Report Reference CSC-EFC-T0074-ETR Version 1.0 (Copyright CSC), 2 June 2014.

14. Aruba Mobility Controller Entropy Documentation version 1.3, 6 November 2013.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
ASD	Australian Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TLS	Transport Layer Security