Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

2012/81

13 Aug 2012

Version 1.0

Amendment Record

Version	Date	Description
1.0	13/08/2012	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Cisco Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS). The TOE is designed as a number of hardware and software products operating together to provide secure wireless access to a wired and wireless network.

2 This report describes the findings of the IT security evaluation of Cisco Systems' Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS), to the Common Criteria (CC) evaluation assurance level EAL4+ ALC_FLR.2. The report concludes that the product has met the target assurance level of EAL4+ ALC_FLR.2, conformant to the *US Government Wireless Local Area Network (WLAN) Access System Protection Profile (PP) For Basic Robustness Environments, Version 1.1* 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 16 July 2012.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Operate the TOE according to the user guidance; and

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

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

5 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

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

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS), against the requirements of the Common Criteria (CC) evaluation assurance level EAL4+ ALC_FLR.2 and the *US Government Wireless Local Area Network (WLAN) Access System Protection Profile (PP) For Basic Robustness Environments, Version 1.1*; and

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

8 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

9 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.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Cisco Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS), release 7.0.230.0
Software Version	7.0.230.0
Security Target	Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target, Version 1.0, July 2012
Evaluation Level	EAL4+ ALC_FLR.2

Evaluation Technical Report	Evaluation Technical Report for Cisco Unified Wireless Network & Wireless Intrusion Prevention System, 2.0
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCIMB-2009-07-001, July 2009 with interpretations as of 28 June 2011.
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, CCIMB-2009-07-004, July 2009 with interpretations as of 28 June 2011.
Conformance	Common Criteria Part 2 extended Common Criteria Part 3 augmented (EAL4 + ALC_FLR.2) The TOE is conformant to the following Protection Profile: US Government Wireless Local Area Network (WLAN) Access System Protection Profile (PP) For Basic Robustness Environments, Version 1.1, pp_wlan_as_br_v1.1, July 25 2007
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, California United States
Developer	Cisco Systems Inc. 170 West Tasman Drive San Jose, California United States
Evaluation Facility	CSC Australia – AISEF 217 Northbourne Avenue Turner, ACT 2612 Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 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

11 The TOE is the Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) developed by Cisco Systems. Its primary role is to provide secure wireless access to a wired and wireless network.

12 The TOE provides end-to-end wireless encryption, centralised WLAN management, Authentication, Authorisation and Accounting (AAA) policy enforcement, and a basic Wireless Intrusion Prevention System (wIPS).

13 The TOE Wireless Intrusion Prevention (wIPS) capabilities include IDS signature detection, rogue Access Point (AP) and client detection and containment, and 802.11 management frame protection (MFP).

2.3 Security Policy

14 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.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) **Access Point (AP) Subsystem**:

The AP subsystem is a security boundary enforcement point for the wireless LAN access system. This subsystem in coordination with the Controller subsystem enforces what wireless clients may access the IT systems and resources connected to the wired network.

The AP subsystem is the encryption and decryption module for wireless clients and devices. The AP subsystem provides wireless intrusion detection (IDS) analysis though signature analysis, presence and location tracking of ad hoc 802.11 devices, rogue APs, rogue clients and authorised wireless devices as well as MFP for protection against spoofed or exploited 802.11 management frames.

b) **Wireless LAN Controller Subsystem**:

The Wireless LAN Controller subsystem is the main point of control of the wireless LAN access system. The Controller subsystem is responsible for the wireless control and configuration, security control and configuration, data forwarding and wireless IDS.

The Controller subsystem supports management, auditing, IDS, rogue detection, and information flow control.

The Controller subsystem provides the capability to define the security profiles for the AP subsystem. The security profiles defined by the Controller include RADIUS server information, the type of 802.11i security to use, and the IDS and rogue detection features that will be enforced by the AP subsystem.

The Controller subsystem maintains the store of these profiles for the AP subsystem and provides one external interface to allow for management and configuration of security profiles.

16 The Developer's Architectural Design identifies the following components of the TOE:

a) Cisco Aironet access points (APs):

i) 1131, 1242 AG Series;

ii) 1522, 1524 AG Series (outdoor mesh); and

iii) 1142, 1252, 1262, 3502e, 3502i AGN Series.

Running Cisco IOS version 12.4(23c)JA4 (downloaded to the AP from the Controller) and including the Cisco FIPS kit part number AIRLAP-FIPSKIT to ensure APs are configured to be physically secure.

b) Cisco Wireless LAN Controllers:

i) 4402, 4404; and

ii) 5508.

Running software version 7.0.230.0 and including the Cisco FIPS kit part number AIRWLC4400-FIPSKIT or AIRCT5508-FIPSKIT

c) Cisco Catalyst 6500 Wireless Integrated Services Modules:

i) WiSM; and

ii) WiSM2.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

a) **Administration:**

The TOE Provides administrator support functionality that enables a human user to configure and manage TOE components. Management functions include configuration of cryptographic keys, encryption settings, audit settings, authentication credentials and the use of authentication servers. The TOE only allows administration of TOE components to occur from the wired network.

b) **Audit:**

The TOE's audit data viewing capability provides administrator support functionality that enables administrators to view audit records and selective view audit records along with allowing them to selectively choose what events they want audited.

c) **Encryption:**

The TOE provides end-to-end encryption capabilities between wireless clients, trusted access points and trusted nodes that reside within the TOE boundary. Also provides encryption to protect communication between TOE components, remote administration and communication with external components such as other WLAN System components including Wireless Control Server (WCS), Network Control Server (NCS), Mobility Services Engine (MSE), and non-WLAN systems such as syslog servers (over TLS).

d) **Identification and Authentication:**

The TOE provides I&A support of all wireless client hosts connecting to the trusted wired network from the wireless network. Also provides all I&A for administrators prior to accessing TOE functionality in the form of user name and password via serial console, over SSH, or over HTTPS/TLS.

e) **Information Flow Control:**

The TOE provides control of information by enforcing the wireless encryption scheme that has been administratively configured, the policy determines whether Access Points and Controllers will encrypt or decrypt communications with wireless clients.

f) **Self Protection:**

The TOE maintains control of user sessions and the actions carried out during the sessions, thereby protecting itself from unauthorised users. The TOE also performs a number of self checks during initial start-up such as cryptographic module testing and integrity checks of configuration files.

g) **Wireless Intrusion Prevention System (wIPS):**

The wIPS functionality of the TOE provides Intrusion Detection System (IDS) signature detection, generation of audit messages related to IDS signature detection, measurement and collection of wireless signal strength (for use in wireless device location tracking) as well as IPS functionality including containment of rogue wireless devices through transmission of targeted de-authentication attacks to prevent rogue devices from connecting to other wireless devices.

2.5.2 Non-evaluated Functionality and Services

19 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.

20 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).

21 The functions and services that have not been included as part of the evaluation are provided below:

a) All wireless hosts connecting to the wired network from the wireless network are excluded from the TOE's physical boundary;

b) Administrator Management Hosts (HTTPS and SSH clients) are not included in the TOE's physical boundary; and

c) A number of Identification & Authentication (I&A) methods supported by the TOE, that are not deemed secure enough to use in the evaluated configuration, have been omitted from the TOE's logical boundary. These exclusions are listed in section 2.6.1 of the Security Target (Ref [1]).

2.6 Usage

2.6.1 Evaluated Configuration

22 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 these defined evaluated configurations. Australian Government users should refer to the ISM (Ref [2]) to ensure that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

23 The TOE is comprised of the following software components:

a) **Cisco IOS version 12.4(23c)JA4** (downloaded to the AP from the Controller) and including the Cisco FIPS kit part number AIRLAP-FIPSKIT to ensure APs are configured to be physically secure, running on Cisco Aironet Access Point hardware.

b) **Cisco Unified Wireless Network software version 7.0.230.0** and including the Cisco FIPS kit part number AIRWLC4400-FIPSKIT or AIRCT5508-FIPSKIT, running on Cisco Wireless LAN Controller and Cisco Wireless Services Module hardware.

24 The TOE is comprised of the following hardware components:

a) **Access Point**: Cisco Aironet 1131, 1242 AG Series; 1522, 1524 AG Series (outdoor mesh); and 1142, 1252, 1262, 3502e, 3502i AGN Series

b) **Controller**: Cisco Wireless LAN Controller 4402, 4404, 5508; and Cisco Catalyst 6500 Wireless Integrated Services Module WiSM, WiSM2.

25 A full explanation of the evaluated configuration may be found in the user guidance documents:

Preparative Procedures and Operational User Guidance for the Common Criteria evaluated configuration of Cisco WLAN v7.0.230.0 at EAL4+, June 2012. (Ref [3])

2.6.2 Delivery procedures

26 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

27 Shipment of hardware units from Cisco Distributors to the user is via a commercial courier company who will pick up the unit from the distribution site and deliver it directly to the user. Using the packing slip and information on device labels, the customer must check that the product number and serial numbers on the received hardware match what was

ordered. Any discrepancies must be immediately reported to Cisco using the contact information on the packing slip.

28 For software, the customer will access the Cisco Connection Online (CCO) website to download software images. Customers will be prompted for their login and password. To create an account on CCO, a user must have a valid support contract with Cisco and access to the contract number. Access control on the CCO site controls what software images a user account is allowed to download. Encryption using SSL protects the software images as they are being downloaded from the Cisco web server to the user's computer.

2.6.3 Determining the Evaluated Configuration

29 To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE component hardware models provided in this report and at the beginning of the guidance document (Ref [3]). This document is made available on the Cisco website for download.

30 In addition to verifying model numbers for hardware components, the software versions must also be verified by the customer recipient. Software versions can be checked by following the "*Identifying the Evaluated Hardware and Software*" instruction included in the user guidance.

2.6.4 Documentation

31 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available for download online from the developer's website:

a) Preparative Procedures and Operational User Guidance for the Common Criteria evaluated configuration of Cisco WLAN v7.0.230.0 at EAL4+, June 2012 (Ref [3]).

2.6.5 Secure Usage

32 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.

33 The following assumptions were made:

a) **No Evil**: Administrators are non-hostile, appropriately trained and follow all administrator guidance.

b) **No General Purpose**: There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

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

d) **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.

e) **Client Protect**: Wireless clients and/or their hosts are configured to not allow unauthorised access to networking services of the wireless client or to stored TOE authentication credentials.

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

a) **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.

b) **Accountability**: The authorised users of the TOE shall be held accountable for their actions within the TOE.

c) **Cryptography**: The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

d) **Cryptography Validated**: Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (encryption, decryption signature, hashing, key exchange, and random number generation services).

e) **Encrypted Channel**: The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorised to join the network.

f) **No Ad Hoc Networks**: There will be no ad hoc 802.11 or 802.15 networks allowed.

g) **Wireless Location Policy**: The TOE will support location tracking for all 802.11 devices transmitting within the RF environment.

Chapter 3 - Evaluation

3.1 Overview

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

3.2 Evaluation Procedures

36 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9] and [10]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

3.3 Functional Testing

37 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

38 The developer 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. This analysis included a search for possible vulnerability sources in publicly available information.

39 Given the nature of the product and the absence of similar products, the evaluators considered it unlikely public domain exploits or vulnerabilities specifically targeting the product would be identified. The evaluators confirmed this hypothesis via the search indicated in the above paragraph, and therefore focused their efforts on the technologies employed by the TOE, including the underlying network protocols and open source software used in the TOE.

40 The analysis conducted by the evaluators and the subsequent testing indicated that the TOE will resist an attacker with an attack potential consistent with the requirements of an EAL4 + ALC_FLR.2 assurance level.

Chapter 4 - Certification

4.1 Overview

41 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

42 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) performed by the Australasian Information Security Evaluation Facility, CSC.

43 CSC has found that Unified Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4+ ALC_FLR.2.

44 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

45 EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

46 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

47 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

48 This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

4.4 Recommendations

49 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.

50 The ACA recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Operate the TOE according to the user guidance (Ref [3]); and

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

Annex A - References and Abbreviations

A.1 Reference

[1] Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target, Version 1.0, July 2012

[2] 2012 Australian Government Information Security Manual (ISM), Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation:

a) Preparative Procedures and Operational User Guidance for the Common Criteria evaluated configuration of Cisco WLAN v7.0.230.0 at EAL4+, June 2012

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

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002

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

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

[8] AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.

[9] AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.

[10] AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.

[11] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[12] Evaluation Technical Report for Cisco Unified Wireless Network & Wireless Intrusion Prevention System

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ALC_FLR	Assurance component: Life Cycle, Flaw Remediation
AP	Access Point
CC	Common Criteria
CCO	Cisco Connection Online
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GCSB	Government Communications Security Bureau
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification & Authentication
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISM	Australian Government Information Security Manual
LAN	Local Area Network
MFP	Management Frame Protection
NIST	National Institute of Standards and Technology, United States
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
wIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WiSM	Wireless Services Module