Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Cisco Converged Access v 3.6.1E

Certification Report
2015/92

2 July 2015
Version 1.0

Amendment Record

Version	Date	Description
1.0	2 July 2015	Final

Executive Summary

This report describes the findings of the IT security evaluation of Cisco Converged Access v3.6.1E against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Cisco Converged Access. The TOE is a product that is designed to combine a purpose-built switching and WLAN controller platforms with wireless access points to create a WLAN Access System. The WLAN Access System provides secure wireless access to a wired network by controlling the link between the wireless client and that wired network.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –** auditable events are stored in syslog files, which can be sent securely to an external server
- **Cryptological Support –** baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection –** The TOE is designed to forward packets (i.e. “information flows”) to source and destination entries as provided by TOE users
- **Identification and Authentication –** The TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management –** The TOE provides for an authorised Administrator role
- **Protection of the TSF –** The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access –** The TOE can be configured to terminate inactive sessions and
- **Trusted Path / Channels –** The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator.

The report concludes that the product has complied with the U.S Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems (WLANPP) Version 1.0, December 1, 2011and 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 29 May 2015.

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

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

b) Configure and Operate the TOE according to the vendor’s product administrator guidance

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

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 and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction 1

1.1 Overview 1

1.2 Purpose 1

1.3 Identification 1

Chapter 2 – Target of Evaluation 3

2.1 Overview 3

2.2 Description of the TOE 3

2.3 TOE Functionality 4

2.4 TOE Architecture 4

2.6 Clarification of Scope 5

2.6.1 Evaluated Functionality 6

2.6.2 Non-evaluated Functionality and Services 6

2.7 Security 6

2.7.1 Security Policy 6

2.8 Usage 7

2.8.1 Evaluated Configuration 7

2.8.2 Secure Delivery 7

2.8.3 Installation of the TOE 7

2.9 Version Verification 7

2.10 Documentation and Guidance 8

2.11 Secure Usage 8

Chapter 3 – Evaluation 9

3.1 Overview 9

3.2 Evaluation Procedures 9

3.3 Testing 9

3.3.1 Testing Coverage 9

3.4 Entropy Testing 9

3.5 Penetration Testing 9

Chapter 4 – Certification 10

4.1 Overview 10

4.2 Assurance 10

4.3 Certification Result 10

4.3 Recommendations 11

Annex A – References and Abbreviations 12

A.1 References 12

A.2 Abbreviations 14

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 Cisco Converged Access against the requirements of the Common Criteria (CC) and the Wireless Local Area Network PP (WLANPP) v1.0 (Ref 3).

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 6) 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 Cisco Converged Access.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco Converged Access
Software Version	IOS XE 3.6.1E
Hardware Platforms	Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1600i/e, 2600i/e, 3500i/e, 3600i/e (optional IEEE 802.11ac module) and 1552e.
Security Target	Cisco Converged Access Common Criteria Security Target Version: 1.0, May 28, 2015
Evaluation Technical Report	Converged Access Evaluation Technical Report (T0078) Reference: CSC-EFC-T0078-ETR

	Commercial-in-confidence Version 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Extended, July 2009, Version 3.1.Rev3
Methodology	Common Methodology for Information Technology Security July 2009, Version 3.1.Rev3
Conformance	WLANPP v1.0
Developer	Cisco Systems, Inc
Evaluation Facility	**CSC AUSTRALIA PTY LIMITED** ABN 18 008 476 944 217 Northbourne Ave TURNER ACT 2612 AUSTRALIA

Cisco WLAN Controller 5760

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 TOE is Cisco Converged Access.

The TOE consists of controllers which are switch platforms that provide connectivity and security services across multiple interconnected devices each operating in a fully-managed secure state where each controller can manage multiple Access Points, and each AP can support multiple concurrent connections from wireless clients.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit** – The TOE (the Cisco Converged Access in its certified configuration) can audit security-relevant events related to cryptographic functionality, identification and authentication, and administrative actions. Each security relevant audit event has the date, timestamp, event description, and subject identity by controlling the link between the wireless client and that wired network
- **Cryptological Support** – The TOE provides cryptography in support of IPsec connections to tunnel communications with AAA servers, Syslog servers, and NTP servers, SSHv2 for secure remote administration via CLI. The TOE can also use the X.509v3 certificates for authenticating sessions, and can act as a certification authority to sign and issue certificates to other devices
- **Security Management** – Through the CLI the TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Functions available to authorized administrators include, but are not limited to:
    - Enabling, disabling, and configuring audit collection
    - Modifying the behaviour of cryptographic functions
    - Configuring security of communications to/from an external servers including RADIUS and Syslog servers
    - Adding/removing/modifying administrative accounts including specifying maximum number of successive failed authentication attempts that will be permitted by remote administrators; Defining inactivity timeout limits for interactive interfaces to terminate inactive sessions
    - Creating custom login banners for interactive interfaces to be displayed at time of logon

- **Protection of the TSF** –The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of plaintext cryptographic keys and passwords. Additionally Cisco IOS XE and IOS are not general-purpose operating systems and access to the memory space is restricted to only system functions. System resources used to support administrative interfaces are protected by allowing authorized administrators to limit the number of concurrent sessions. The APs and Controllers will detect and drop (not forward) replayed packets received at network interfaces (including wireless radio interfaces)
- **TOE Access –** The TOE can be configured to terminate inactive sessions.
- **Trusted Path / Channels –** The wireless connections between the APs and wireless clients are secured using Wi-Fi Protected Access 2 (WPA2). Specifically, the TOE uses Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP), as defined in the WPA2 standard. TSF data (command and control data, audit data, etc.) transmitted among controllers and APs of the TOE are secured with DTLS (for CAPWAP over DTLS) using ciphersuites required by the WLANPP for the TLS connections.

2.3 TOE Functionality

The Cisco Converged Access TOE combines a purpose-built switching and WLAN controller platforms with wireless access points to create a WLAN Access System. This is combination of one or more controllers, with one or more wireless access points, and provides authentication services, encrypted communications, audit message generation, routing, switching, and bridging among connected wired and wireless networks.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- Access point
- Controller
- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operation.
- Flash memory (EEPROM), used to store the Cisco IOS or IOS XE software image
- USB port (v2.0) (note, none of the USB devices are included in the TOE)
    - Type A for Storage, all Cisco supported USB flash drives
    - Type mini-B as console port in the front
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile random-access memory (NVRAM) is used to store router configuration parameters that are used to initialize the system at start-up

- Physical network interfaces (minimally two) (e.g. multiple RJ45 10/100/1000 Mb Ethernet ports on Controllers, or Ethernet plus wireless radio interface on APs). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces

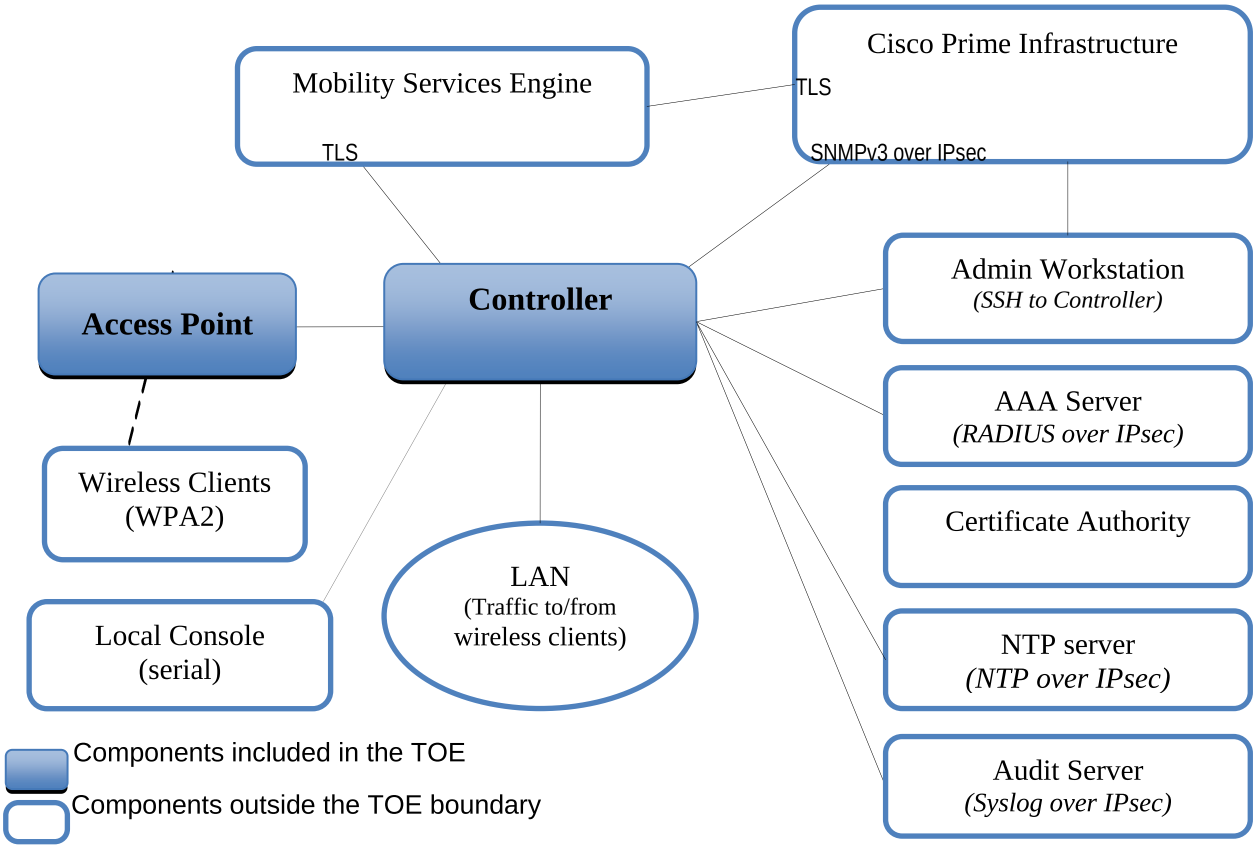
2.6 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Cisco 3650, 3850, and 5760 WLAN Controller Configuration Guide Preparative Procedures and Operational Guidance (Ref 5).

The scope of the evaluation was limited to those claims made in the Security Target - Cisco Converged Access Common Criteria Security Target, Version: 1.0, May 28 2015. (Ref 6).

Figure 1: Sample TOE Deployment



2.6.1 Evaluated Functionality

All tests performed during the evaluation were taken from WLANPP (Ref 3) and sufficiently demonstrate the security functionality of the TOE.

2.6.2 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 4) 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).

The following components are considered outside of the scope of the TOE:

- Wireless clients
- Local console(serial)
- Mobility Services Engine
- Cisco Prime Infrastructure
- Admin workstation
- AAA Server
- Certificate authority
- NTP Server
- Audit server
- LAN

2.7 Security

2.7.1 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 6) contains a summary of the functionality to be evaluated:

- Security Audit
- Cryptographic Support
- User Data Protection / Information Flow Control
- Identification and Authentication – note that Telnet and FTP are considered to be out of scope
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

2.8 Usage

2.8.1 Evaluated Configuration

The TOE consists of both software and hardware. The hardware is comprised of the following: Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1600i/e, 2600i/e, 3500i/e, 3600i/e (optional IEEE 802.11ac module), and 1552e. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software release IOS XE 3.6.1E installed on the controller(s), which includes AP images of IOS 15.3(3)JN3 that gets installed to APs as they join a controller. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Configuration Guide (Ref 5).

2.8.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- Shipment of 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
- For hardware components; using the packing slip and information on the stickers, 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
- For Software, the customer will access CCO (Cisco Connection Online) to download 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.

2.8.3 Installation of the TOE

The Configuration Guide (Ref 5) contains all relevant information for the secure configuration of the TOE.

2.9 Version Verification

The verification of the TOE is largely automatic, including the verification using SHA1 hashes. The TOE cannot load a modified image.

2.10 Documentation and Guidance

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. All guidance material is available for download at **www.cisco.com.** All Common Criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.11 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.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE
- Information cannot flow between the wireless client and the internal wired network without passing through the TOE
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 WLANPP (Ref 3), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3, Parts 2 and 3 (Ref 1 and 2).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (Ref 12).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Cisco Converged Access configuration guide (Ref 5).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the WLANPP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 10).

3.5 Penetration Testing

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. The analysis conducted by the evaluators and the subsequent testing indicated that the TOE will resist an attack by an attacker possessing Basic attack potential.

Chapter 4 – Certification

4.1 Overview

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

4.2 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). PPs provide assurance by a full security target and an analysis of the SFR 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 WLANPP 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.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the certifiers and of the Evaluation Technical Report (Ref 7) the Australasian Certification Authority **certifies** the evaluation of the Cisco Converged Access product performed by the Australasian Information Security Evaluation Facility, CSC.

CSC **has determined** that Cisco Converged Access uphold the claims made in the Security Target (Ref 6) and **has met** the requirements of WLANPP v1.0.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the WLANPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.3 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 4) 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, the ACA also 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) Configure and Operate the TOE according to the vendor's product administrator guidance

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

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July,2009 Version 3.1 Revision 3

2. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009, Version 3.1 Revision 3

3. US Government approved Protection Profile – Protection Profile for Wireless Local Area Networks (WLANPP) version 1.0, 01 December , 2011

4. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. Guidance Documentation:

   - Cisco 3650, 3850, and 5760 WLAN Controller Configuration Guide Preparative Procedures and Operational Guidance for the Common Criteria Certified Configuration Version 1.0.

6. Security Target – Cisco Converged Access Common Criteria Security Target, Version: 1.0, May 28, 2015

7. Evaluation Technical Report Cisco Converged Access Evaluation Technical Report (T0078) Reference: CSC-EFC-T0078-ETR Commercial-in confidence version 1.0 22 May 2015.

8. Test documentation

   - CSC Workbook , Document Reference CFC-T078-WS-OPE 5.0
   - CSC Workbook , Document Reference CFC-T078-WS- AS-IND 2.0
   - CSC Workbook , Document Reference CFC-T078-WS-AS_ST 8.0
   - CSC Workbook , Document Reference CFC-T078-WS- AS-VAN 2.0
   - CSC Workbook , Document Reference CFC-T078-WS-WLAN_CMC 1.0
   - CSC Workbook , Document Reference CFC-T078-WS-WLAN_PRE 1.0

9. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

10. Cisco NGWC Entropy Information Version .03, May 2015

11. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

12. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 3, dated: July 2009.

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
IDM	IPS Device Manager
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy