



Australian Government
Department of Defence

Australasian Information Security Evaluation Program

**Maintenance Report Supplementing
Certificate Report 2015/92**

**03 September 2015
Version 1.0**

Commonwealth of Australia 2015

Reproduction is authorised provided
that the report is copied in its entirety.

Amendment Record

Version	Date	Description
1.0	03/09/15	Public Release

Table of Contents

1. Table of Contents.....	iv
2. Chapter 1 – Introduction	1
<i>1.1: Purpose.....</i>	<i>1</i>
<i>1.2: Identification</i>	<i>1</i>
3. Chapter 2 – IAR Summary.....	2
<i>2.1: Description of changes</i>	<i>2</i>
<i>2.2: Documentation Updated.....</i>	<i>2</i>
4. Chapter 3 - Assurance Continuity	3
<i>3.1 Assurance Continuity Result.....</i>	<i>3</i>
5. References, Abbreviations and Glossary	4
<i>A.1 References</i>	<i>4</i>
<i>A.2 Abbreviations</i>	<i>4</i>
<i>A.3 Glossary</i>	<i>4</i>

Chapter 1 – Introduction

1.1: Purpose

This document is an addendum to the Certification Report (Ref [1]) that describes the relevant baseline evaluation of the Cisco Converged Access.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Cisco for the Cisco Converged Access against the requirements contained in the Assurance Continuity: CCRA Requirements (Ref [2]).

Cisco provided information about their assurance continuity activities in the form of an Impact Analysis Report (IAR). The IAR (Ref [3]) list the changes made to the certified TOE, the evidence updated as the result of the changes and the security impact of the changes.

This report should be read in conjunction with:

- a) The certified TOE's Certification Report (Ref [1]).
- b) The certified TOE's Security Target v1.0 (Ref [4]) which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.
- c) The new Security Target, Cisco Converged Access Security Target Version 1.1 dated, August 18, 2015 (Ref [5]) which includes the updated version numbers. The scope has not changed.

1.2: Identification

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
Maintained TOE	Cisco Converged Access with IOS XE 3.6.1E
Developer	Cisco Systems
Certified TOE	Cisco Converged Access with IOS XE 3.6.1E
Security Target	Cisco Converged Access, Common Criteria Security Target version 1.0 May 28, 2015
Updated Security Target	Cisco Converged Access, Common Criteria Security Target version 1.1 August 18, 2015
Certificate Number	2015/92

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 1.4 of the Security Target (Ref [5])

Chapter 2 – IAR Summary

2.1: Description of changes

The Impact Analysis Report (IAR) indicated that the following minor changes have been made to the Cisco Converged Access.

Table 2: Model Changes

Certified version	Changed version
Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1600i/e, 2600i/e, 3500i/e, 3600 i/e (optional IEEE 802.11ac module) and 1552e	Cisco Catalyst 3650, 3850, and WLC 5760 with APs 1600i/e, 2600i/e, 2700i/e, 3500i/e, 3600i/e (optional 3000M monitor and IEEE 802.11ac modules), 3700i/e/p, and 1552e

The overall impact of the software changes is minor. These changes involved additional access points which are part of the ongoing scaling of the product.

2.2: Documentation Updated

The updated Security Target is ‘Cisco Converged Access Common Criteria Security Target version 1.1 August 18, 2015’ (Ref [5]). It has been updated to reflect additional access points. Two of the FIPS certificates number references have been updated.

The updated guidance is Cisco Converged Access Configuration Guide, Preparative Procedures and Operational Guidance for the Common Criteria Certified Configuration version 1.0 August 2015 (Ref [6]).

Chapter 3 - Assurance Continuity

3.1 Assurance Continuity Result

After consideration of the Impact Analysis Report (IAR) provided by Cisco Systems, Australasian Certification Authority (ACA) has determined that the proposed changes are minor. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is maintained for Cisco Converged Access with IOS XE 3.6.1E.

References, Abbreviations and Glossary

A.1 References

1. Certification Report 2015/92, Australasian Certification Authority 2 July 2015 version 1.0
2. Assurance Continuity: CCRA requirements, Common Criteria Interpretation Management Board, CCIMB-2012-06-01, Version 2.1, June 2012
3. Cisco Converged Access - Impact Analysis Report - For Common Criteria Assurance Maintenance- Update of Cisco Converged Access running IOS XE 3.6.1E Version .01, Aug 18 2015
4. Cisco Converged Access Security Target Version 1.0, May 28, 2015
5. Cisco Converged Access Security Target Version 1.1, August 18, 2015
6. Cisco Converged Access Configuration Guide, Preparative Procedures and Operational Guidance for the Common Criteria Certified Configuration version 1.0 August 2015.

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
ASD	Australian Signals Directorate
PP	Protection Profile
IAR	Impact Analysis Report
TOE	Target of Evaluation

A.3 Glossary

3000M	An add-on module which offloads monitoring services from the client/data serving radios, providing always-on spectrum analysis functions. This helps avoid Radio Frequency (RF) interference and provides better coverage and performance on the wireless network.
-------	--