Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

2012/79

2 May 2012

Version 1.0

Amendment Record

Version	Date	Description
1.0	02/05/2012	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Microsoft Forefront Identity Manager (FIM) 2010. The TOE is an enterprise identity management solution designed to manage identities, credentials, and associated attributes across heterogeneous environments. The TOE provides centralised management of identities and security policies, and synchronisation across a range of products in a network environment. The TOE can be configured to provide support for additional products via a set of APIs and a codeless identity provisioning system. Note that Forefront Identity Manager 2010 includes a Certificate Management service, but that this is explicitly excluded from the TOE.

2 This report describes the findings of the IT security evaluation of Microsoft's Forefront Identity Manager 2010, to the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3. The report concludes that the product has met the target assurance level of EAL4 + ALC_FLR.3 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 stratsec and was completed on 30 March 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 administrator guidance (Ref [3]);
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved; and
d) Test and verify Management agents as trusted prior to installation.

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, Forefront Identity Manager 2010, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3; 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	Microsoft Forefront Identity Manager 2010
Software Version	Build 4.0.3547.2 (KB2028634 hotfix)
Security Target	Forefront Identity Manager 2010 Security Target v1.0 24 March 2012
Evaluation Level	EAL4 + ALC_FLR.3
Evaluation Technical Report	Microsoft Forefront Identity Manager 2010, Evaluation Technical Report, Version 1.0, 23 April 2012
Criteria	Common Criteria for Information Technology Security Evaluation Parts 1, 2 & 3, July 2009 Version 3.1 Revision 3 Final

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004
Conformance	Common Criteria Part 2 conformant Part 3 Augmented (EAL4 + ALC_FLR.3)
Sponsor	Microsoft One Microsoft Way Redmond, WA 98052 USA
Developer	Microsoft One Microsoft Way Redmond, WA 98052 USA
Evaluation Facility	Stratsec lab - AISEF 1 / 50 Geils Crt Deakin ACT 2600 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 architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Microsoft Forefront Identity Manager 2010 developed by Microsoft.

12 Microsoft Forefront Identity Manager 2010 is an enterprise identity management solution. The TOE is designed to manage identities, credentials, and associated attributes across heterogeneous environments. The TOE provides centralised management of identities and security policies, and synchronisation across a range of products in a network environment. It can be configured to provide support for additional products via a set of APIs and a codeless identity provisioning system.

13 Note that Forefront Identity Manager 2010 includes a Certificate Management service, but that this is explicitly excluded from the TOE.

2.3 Security Policy

14 The TOE Security Policy (TSP) is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) REQUEST-SFP - This Security Functional Policy (SFP) defines the implementation of rules-based policies for the TOE. For users or requesters to access resources in the environment, the administrator will grant permission to perform operations on them under this policy.

b) INBOUND-SFP - This policy defines the rules for Inbound Synchronisation. Inbound synchronisation creates and updates the integrated view of the identity information from the connected data sources. Inbound synchronisation begins in the connector space and ends in the metaverse.

c) OUTBOUND-SFP - This policy defines the rules for Outbound Synchronisation. Outbound synchronisation distributes the integrated view of the identity information to all the connected data sources. Outbound synchronisation begins in the metaverse and ends in the connector space.

The Security Target (Ref [1]) additionally contains the following implied TSPs:

a) Authentication policy – when and how is a user authenticated; and

b) Secure management policy – rules governing the use of the management functions.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) **FIM Clients;**

b) **FIM Portal;**

c) **FIM Service;** and

d) **FIM Synchronisation Service.**

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

a) **FIM Clients.** The TOE provides a number of different client-side components called a FIM Add-in that can be used for supporting the password reset functions and also workflow activities. The Password Reset Add-in can be deployed and integrated with the Windows client operating system to modify the logon process to allow anonymous (unauthenticated) users to reset their password. The FIM Add-in for Outlook allows approval requests to be approved or rejected directly from Office Outlook experience.

b) **FIM Portal**. A web-based user interface designed to provide the administrator with the capability to perform user, group and policy management and general administrative operations. The FIM Password Reset Portal also provides general users with the interface for performing self-service functions including password reset and identity management.

c) **FIM Service.** A web service that provides the centralised request-based access control features to ensure that requested access to identity resources is controlled in a secure manner. This web service implements a request processing model that comprises three distinct workflow steps: authentication, authorisation, and action. Workflows (each of which contains one or more activities) can be attached to each of these steps and run in the context of executing a single request for access to protected identity resources.

d) **FIM Synchronisation Service.** A centralised service that stores and integrates information for organisations that have multiple sources

of identity information. The FIM Synchronisation Service provides a unified view of all connected identity sources that can relate to users, applications, and network resources. The service manages information by receiving identity information from the connected data sources via Managed Agents and storing the information in the connector space as connector space objects. The connector space objects are then mapped to entries in the metaverse, called metaverse objects.

17 The following components are considered outside the physical scope of the TOE, but are necessary software elements that support the TOE in delivering the security objectives:

a) **Management Agents (MAs).** Management agents link specific connected data sources to FIM 2010. A management agent is responsible for moving data from a connected data source to FIM. When data in FIM is modified, the management agent can also export the data out to the connected data source to keep the connected data source synchronised with the data in FIM.

b) **Microsoft SQL Server.** Both the FIM Service and FIM Synchronisation Service store their data in independent SQL databases.

c) **Identity Stores.** Also known as connected data sources are the systems that FIM manages through MAs. FIM 2010 includes several default MAs to manage a number of identity systems.

2.5 Clarification of Scope

18 The scope of the evaluation was limited to those claims made in the Security Target.

2.5.1 Evaluated Functionality

19 The TOE provides the following evaluated security functionality:

a) Request-based access control policy.

b) Synchronisation information flow policy.

c) Identification and authentication associated with password reset and accessing the FIM Portal.

d) General identity management activities that relate to policy, user and group management.

2.5.2 Non-evaluated Functionality and Services.

20 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).

21 It should be noted that this evaluation did not cover:

a) Cryptographic protection of data in transit between the distributed components of the TOE;

b) Protection of identity information in the various external identity stores;

c) The implementation of custom add-ins or extensions;

d) Management agents. Management agents link specific connected data sources to FIM 2010. A management agent is responsible for moving data from a connected data source to FIM. When data in FIM is modified, the management agent can also export the data out to the connected data source to keep the connected data source synchronised with the data in FIM; and

e) Certificate Management. FIM provides credential management features to both Windows Server and 3rd party certification authorities (CAs) by acting as an administrative proxy. Once installed within an organisation, all digital certificate and smartcard management functions pass through FIM.

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 this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that configuration 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) FIM 2010 Service (Build 4.0.3547.2);

b) FIM 2010 Synchronisation Service (Build 4.0.3547.2); and

c) FIM 2010 Portal (Build 4.0.3547.2).

24 The TOE relies on the following hardware:

a) General server grade hardware.

25 The TOE is a software product that runs on the Windows Server 2008 operating system. As such, the following security objectives must be considered when deploying the TOE in an evaluated configuration:

a) **Firewall protection**. There is a wide range of guidance available for the deployment of the various components of FIM 2010. There is no specific network architecture that is considered approved or used as the basis of the evaluated configuration, the only requirement is that there is appropriate network and application layer firewalling of the servers from untrusted networks.

b) **Installed in accordance with provided procedures**. It is important that the administrator(s) of FIM 2010 ensure that the product is delivered, installed and then configured securely. It is important that all guidance is followed by the administrators in these initial steps of deployment to ensure that the product is initiated securely.

c) **Logical access control**. The underlying server operating system must provide adequate access control protection for the executable and configuration files of the FIM 2010 product and the components that support it. It is important the Windows Server 2008 is installed and configured appropriately to provide this system-level production of FIM 2010.

d) **Identification and authentication**. The underlying server operating system must provide the ability to enforce identification and authentication of the underlying platform that the FIM 2010 components are installed on. This ensures that the administrators must be successfully authenticated prior to performing any maintenance or administration of the FIM servers or components.

e) **Data storage**. The IT environment must provide the capability to store data on behalf of the FIM 2010. There is significant guidance on the establishment of the necessary SQL databases that are required to support the operation of FIM 2010. It is important that the IT environment also provide adequate protection for these servers and the data that they contain.

f) **Servers updated and hardened**. There underlying server operating systems and the database servers are updated with all the latest hotfixes and security patches available and hardened to support a secure deployment of FIM 2010.

g) **Malware protection**. It is expected that the administrators will implement capabilities on the servers to ensure that they are suitably protected from malware.

h) **Competent and capable administration**. It is also expected that there will be one or more competent administrators assigned to

manage FIM 2010, the underlying servers and platforms and the security of the information both of them contain. There is a need to ensure that the administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.

i) **Physical access control**. There is an expectation that the operational environment will provide a suitable set of physical access controls for the actual servers that host the FIM 2010 components.

26 In particular, Secure Sockets Layer (SSL) should be implemented on the server hosting the FIM Portal. The procedure to configure this is included in the FIM 2010 Installation Guide.

27 The evaluated configuration is based on default installation of the TOE. Microsoft provides guidance to assist their customers understand the deployment and usage of the TOE, as referenced in the installation guidance.

2.6.2 Delivery procedures

28 The TOE is downloaded from the Microsoft website.

2.6.3 Determining the Evaluated Configuration

29 To verify the FIM Package is downloaded from the trusted source, perform the following steps:

a) Download the package from Microsoft website. The download link is obtained from Microsoft sales at the time of purchase;

b) Locate the “Forefront Identity Manager VL.exe” file, right-click and select Properties. This will bring up the Properties dialog box;

c) At the top, click the Digital Signatures tab;

d) Click on Details. Look for Signer Information and note the value. It should be Microsoft Corporation;

e) Click the View Certificate;

f) At the top, click the Details tab;

g) Look for Issuer and note the value. It should be Microsoft Code Signing PCA; and

h) Close the Properties dialog box.

30 To verify the build numbers of the FIM Services perform the following steps:

a) Navigate to the following directory: c:\Program Files\Microsoft Forefront Identity Manager\2010\Service;

b) Locate the Microsoft ResourceManagement.Service.exe file, right-click and select Properties. This will bring up the Properties dialog box;

c) At the top, click the Details tab;

d) Look for Product Version and note the value. It should be 4.0.3547.2. Click Cancel;

e) Navigate to the following directory: c:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronisation Service\Bin;

f) Locate the miiserver.exe file, right-click and select Properties. This will bring up the Properties dialog box;

g) At the top, click the Details tab; and

h) Look for Product Version and note the value. It should be 4.0.3547.2. Click Cancel.

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 upon request from the developer:

a) Guidance Documentation and associated references (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:

Identifier	Assumption statement
A.FIREWALL	Any internet connection to a server role is assumed to be appropriately secured by a firewall.
A.INSTALL	It is assumed that the TOE will be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures. It is assumed that the administrator ensures that the machines the TOE is installed on support the secure operation of the TOE.

Identifier	Assumption statement
A.PLATFORM	It is assumed that the underlying server operating systems will provide the following: a) Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases only to the administrators authorised to perform these functions. b) Functionality for supporting and enforcing Identification and Authentication of users. It is assumed that the platform ensures the identification and authentication of users except for the case that they are performing the self-service function of the TOE. c) Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict the access to TSF data where necessary.
A.UNTRUSTED	It is assumed that no untrusted software is installed on the machines the TOE is installed on.
A.NO_EVIL	It is assumed that there will be one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain. It is also assumed that the administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
A.PROTECT	It is assumed that the TOE and its platform will be located within facilities providing controlled access to prevent unauthorised physical access.
A.PATH	It is assumed that the IT environment will provide a trusted communication path between itself and remote users for: a) use of the FIM clients transfer authentication data; b) access to the self-service portal by users; and c) access to the administrative interface by administrators.

Chapter 3 - Evaluation

3.1 Overview

34 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

35 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

36 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.

37 The evaluator test environment was equivalent to the developer test environment. The same hardware was used, which was made available by the developers. The evaluators configured an equivalent test environment, based on the Forefront Identity Manager 2010 Test Lab documented in the Microsoft TechNet Forefront Identity Manager 2010 Test Lab Guide. The evaluators chose to repeat approximately 85% of the developer tests that they were supplied.

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 The evaluators' penetration tests are based on an independent vulnerability analysis of the TOE using the guidance documentation, functional

specification, TOE design, security architecture description, implementation representation as well as available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

Chapter 4 - Certification

4.1 Overview

40 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

41 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 Forefront Identity Manager 2010 performed by the Australasian Information Security Evaluation Facility, stratsec.

42 stratsec has found that Forefront Identity Manager 2010 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.3.

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

4.3 Assurance Level Information

44 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.

45 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.

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

47 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

48 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.

49 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) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved; and
b) Test and verify Management agents as trusted prior to installation.

Annex A - References and Abbreviations

A.1 References

[1] Microsoft Forefront Identity Manager 2010 Security Target v1.0, 24 March 2012.

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

[3] Forefront Identity Manager 2010, Guidance documentation, Version 0.2, 08-JUL-2011.

[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 Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, 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 Microsoft Forefront Identity Manager (FIM) 2010 23 April 2012.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
API	Application Program Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIM	Forefront Identity Manager
GCSB	Government Communications Security Bureau
MAs	Management Agents
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