Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/72

16 Feb 2011

Version 1.0

Amendment Record

Version	Date	Description
0.1	11/02/2011	Internal release.
0.2	16/02/11	Extended review.
1.0	18/03/2011	Public release.

Executive Summary

1 Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit build 14.01.0218.015 (Exchange 2010) is a product that is designed to be an e-mail and collaboration server that provides secure access to personal and shared data for a variety of clients using various protocols. Exchange 2010 SP1 is the Target of Evaluation (TOE).

2 The TOE implements a number of security functions which were included in the scope of the evaluation:

- **Connection filtering** - Protects from unwanted spam or unsolicited commercial e-mail (UCE) by blocking messages from specified IP addresses.
- **Message filtering** - Filters potential spam messages based on administrator configured SMTP filters; including local and third party block/allow lists.
- **Attachment filtering** - Provides a mechanism to filter potentially harmful attachments.
- **Transport filtering** - Allows the administrator to define mail policies to prevent specific internal and/or external users from emailing each other.
- **Access control** - Protects mailboxes and public folders from unauthorized access.
- **Identification and authentication** - Provides identification and authentication mechanism for the Outlook Voice Access functionality in cases where Outlook Voice Access is not secured by the use of the TLS protocol.
- **Distribution group restriction** - Requires users sending mail to a distribution group to be successfully authenticated and to be authorised.
- **Remote device wipe** – An administrator can issue a command to wipe a managed Windows Mobile device in the event that the device may have been compromised.
- **Security management** – Provides a set of task based commands for use by an administrator to manage Microsoft Exchange.

3 This report describes the findings of the IT security evaluation of Microsoft's Exchange 2010 SP1, 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 relevant criteria and

the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed on the 3rd February 2011.

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

- The administrator should ensure that the KB2416471 patch has been applied to the environment. This will solve the .net oracle padding information disclosure vulnerability (CVE-2010-3332).

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

6 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

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

1.2 Purpose

8 The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE, Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit version 14.01.0218.015 against the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3 and
- provide a source of detailed security information about the TOE for any interested parties.

9 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

10 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 Exchange 2010 SP1 Enterprise (English) 64-bit
Software Version	14.01.0218.015
Security Target	Microsoft Exchange 2010 EAL4+ Security Target
Evaluation Level	EAL4 + ALC_FLR.3
Evaluation Technical Report	Evaluation Technical Report for Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit, Version 1.0, Released: 1 February 2011.
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. CCMB-2009-07-001, CCMB-2009-07-002, & CCMB-2009-07-003

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004.
Conformance	CC Part 2 conformant. CC Part 3 Augmented with flaw remediation ALC_FLR.3
Developer	Microsoft Corporation 1 Microsoft Way, Redmond WA 98052-8300, USA
Evaluation Facility	stratsec Suite 1/50 Geils Court, Deakin ACT 2600, Australia

Chapter 2 - Target of Evaluation

2.1 Overview

11 This chapter contains information about the 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

12 The TOE is the Exchange 2010 SP1 developed by Microsoft. This software is installed on a Windows server operating system and suitable underlying hardware. A typical installation of the TOE can be found in Figure 1 – TOE Roles below and identifies the various server roles and components of the Exchange 2010 server.

13 The underlying platform for the evaluated version of Exchange 2010 SP1 is the Windows Server 2008 R2 Enterprise Edition x64 Edition (English) operating system with patches as listed in the Exchange Server Guidance Addendum. This includes internet protocol support using the Internet Information Services (IIS) component in Windows and the Active Directory for directory services.

14 All roles, with the exception of the Edge Transport Server, can be installed on a single machine; however, for reasons of performance, in medium and large organisation installations, these roles may be installed on individual servers. The TOE roles communicate in the same way whether they are installed on one or many servers.

2.3 Security Policy

15 This evaluation was performed at EAL4 augmented with ALC_FLR.3. There is no security policy model required for the TOE.

2.4 TOE Architecture

16 The TOE consists of five server roles as outlined below; those roles can be considered to be subsystems in terms of Common Criteria. The TOE exists within an enterprise operating environment and is supported through communications with a number of enterprise resources that are not within the scope of the TOE. The TOE does not include the underlying server operating system and hardware for the five Exchange 2010 server roles. The TOE is comprised of Exchange 2010 RTM with Exchange 2010 service pack 1 installed as a patch.

2.4.1 Edge Transport Server Role

17 The Edge Transport Server Role is a mail routing server that sits outside the perimeter of the network topology (typically in a DMZ) and routes mail into and out of the Exchange organisation. The Edge Transport server role handles two major tasks:

- **Mail Flow -** The Edge Transport server role accepts mail coming into the Exchange 2010 Organisation from remote SMTP servers in the Internet, and from trusted Exchange 2010 gateway servers in external organisations in some forest-to-forest scenarios, plus it routes all outbound messages to the internet. The Edge Transport server role uses Domain Name System (DNS) to locate servers outside the organisation to which outbound messages must be delivered.

- **SMTP Filtering** - The Edge Transport server role helps protect the Exchange Server 2010 organisation from unwanted messages by filtering inbound messages as they arrive.

18 The Edge Transport server role routes all accepted messages to a Hub Transport server role inside the organisation.

2.4.2 Hub Transport Server Role

19 This is the mail routing server that routes mail within the Exchange Organisation. The Hub Transport server role handles all mail flow inside the organisation, applies transport rules and journaling policies and delivers messages to a recipient's mailbox. Messages that are received from the Internet are processed by the Edge Transport server role (deployed in the perimeter network) before they are relayed to the Hub Transport server. Messages that are sent to the Internet are either: relayed by the Hub Transport server to the Edge Transport server role, which in turn relays the remote servers; or (if the Edge Transport Server role is unavailable) directly to the internet.

20 The Edge Transport servers cannot directly communicate with Active Directory, so the Hub Transport server role works as an intermediary between the Edge Transport server and Active Directory. Global Edge Server configurations are copied from the Active Directory and sent to the

Edge Transport server role's Active Directory Lightweight Directory Service (AD LDS) instance by the EdgeSync Process, which is a component of the Hub Transport server role.

2.4.3 Mailbox Server Role

21 The Mailbox server role hosts mailbox and public folder databases, as well as providing address list and offline address book generation RPC Clients (e.g. Outlook 2010) can connect directly to the Mailbox server role. The Mailbox server role, in conjunction with the environment, provides access control for users, mail, fax, and voice messages. The Mailbox server role communicates with other TOE components including the Hub Transport server role, the Unified Messaging server role and Client Access server role, as well as components external to the TOE including the Active Directory server and Outlook clients.

2.4.4 Unified Messaging Server Role

22 Unified Messaging combines voice messaging, fax, and e-mail services, making them accessible from a telephone or a computer. Exchange 2010 Unified Messaging integrates Exchange Server with an organisation's internal telephony networks and brings the Unified Messaging features to the core of Exchange Server.

23 The Unified Messaging Server Role provides users with the opportunity to access their mail and calendar information via telephone, as well as providing call answering functionality, and the capability to access voice messages via the Outlook client or via Outlook Web application. The Unified Messaging server role ensures that each user is authenticated prior to being granted access to user mail and calendar functions. Authentication (of a user connecting using a telephone) is performed through the correct input of the PIN by the user, or alternatively if mutual transport layer security (TLS) authentication is employed, no authentication is performed by the TOE.

24 The Unified Messaging server role provides an interface between the IP/PBX and the Exchange Organisation. This role receives faxes and unanswered voice calls and submits them to a user's mailbox, via the Hub Server.

25 The Exchange 2010 Unified Messaging server does not include built-in support for fax message creation (as was included in Exchange 2007), instead requiring the use of an externally provided Fax Partner server (external to the TOE) to be implemented to provide this functionality.

2.4.5 Client Access Server Role

26 The Client Access server role in Exchange 2010 lets users access voice mail, e-mail, fax messages, and calendar information located in their Exchange 2010 mailbox from an e-mail client such as Microsoft Outlook (via Outlook Anywhere) or Outlook Web Access, from a mobile device

that has Microsoft Exchange ActiveSync enabled, such as a Windows Mobile® powered SmartPhone or personal digital assistant (PDA).

27 This is the server that hosts the client protocols, such as Post Office Protocol 3 (POP3), Internet Message Access Protocol 4 (IMAP4), Secure Hypertext Transfer Protocol (HTTPS), Outlook Web Access, and Outlook Anywhere. POP3 and IMAP4 are deactivated in the evaluated version as described in the guidance. The Client Access server also exposes a web services interface for application developers and supports internal web services used by Exchange, as well as external web services such as auto discover and the availability service.

28 Outlook clients usually access their mailboxes directly on the Mailbox server, but rely on the Client Access server for "auto discover" and other web services.

29 This server role implements the remote wipe functionality allowing an administrator to send a remote wipe command (sent from the Client Access server) to a mobile device to request a reset of the mobile device back to factory default settings erasing all data and configurations set on the mobile device.

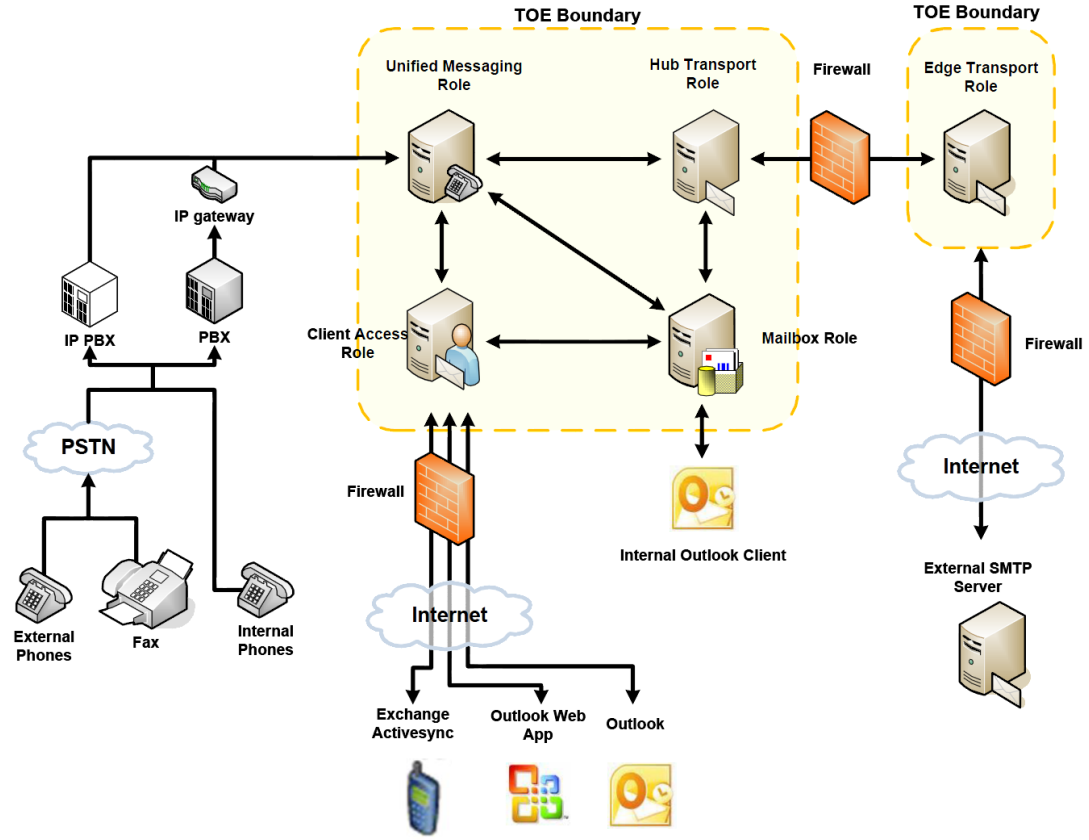

Figure 1 – TOE Roles

2.5 Clarification of Scope

30 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). The scope of the evaluation only includes the five roles (see Figure 1) provided by the Microsoft Exchange 2010 with SP1 software (Hub, Client Access, Edge, Mailbox and Unified Messaging) deployed according to the evaluated configuration. It does not include external VOIP servers or other Mail servers that Exchange may interface with. It does not also include any clients that are used to access TOE functionality.

31 The TOE does not counter the threat of information disclosure by authorised users. Users are explicitly trusted to use the TOE in a secure manner and ensure that the TOE is in the evaluated configuration.

32 The TOE offers its services for users via a variety of protocols including:

- RPC for applications like Microsoft Office Outlook ,
- SMTP for generic clients and servers sending e-mail to the TOE,
- HTTP for Web Browsers (using Outlook Web Access) and for ActiveSync clients,
- RPC tunnelled over HTTP,
- Web Services Application Programming Interface (API) for in-house applications, and
- SIP/RTP for Outlook Voice Access (OVA).

33 Outlook Voice Access (OVA) can optionally be secured by enabling the TLS protocol with mutual authentication for SIP/RTP. In this case, the identification and authentication of OVA users is not performed by the TOE but is the sole responsibility of the TLS authenticated application which is part of the IT environment.

34 These protocols can be used to connect to the TOE via different clients. Clients can be categorized into the following groups:

- **Generic Client (also known as Internet Client):** A client of this type could be any mail client that uses SMTP to connect to the TOE or a web browser that uses HTTP or Web Services to connect to the TOE.
- **Outlook client:** In contrast to the generic clients, an Outlook client uses RPC (or RPC over http) to connect to the TOE.

35 In addition to the above clients, the TOE allows users to connect using a standard or IP telephone via Outlook Voice Access. To use standard telephones, a PBX must be connected to the TOE. A PBX may also forward IP calls.

36 The Unified Messaging server role in Exchange 2010 lets users access voice mail, e-mail, fax messages, and calendar information located in their Exchange mailbox from an e-mail client such as Microsoft Outlook or Outlook Web Access, from a mobile device that has Microsoft Exchange ActiveSync enabled, such as a Windows Mobile® powered smartphone or a personal digital assistant (PDA), or from a telephone. Further, the SMTP protocol can be used by a SMTP server to connect to the TOE. The scope of the TOE ends at the interfaces where it provides its services and does not include any functionality of any client.

2.5.1 Evaluated Functionality

37 The TOE provides the security functionality described in the table below:

Table 1 – Functional Overview

Security Function	Description
Connection filtering	Protects from unwanted spam or Unsolicited Commercial E-mail (UCE) by blocking messages from specified IP addresses.
Message filtering	Filters potential spam messages based on administrator configured SMTP filters, including local and third party block/allow lists.
Attachment filtering	Provides a mechanism to filter potentially harmful attachments.
Transport filtering	Allows the administrator to define mail policies to prevent specific internal and/or external users from emailing each other.
Access control	Protects mailboxes and public folders from unauthorized access.
Identification and authentication	Provides identification and authentication mechanism for the Outlook Voice Access functionality in cases where Outlook Voice Access is not secured by the use of the TLS protocol.
Distribution group restriction	Requires users sending mail to a distribution group to be successfully authenticated and to be authorized.
Remote device wipe	An administrator can issue a command to wipe a managed Windows Mobile device in the event that the device may have been compromised.
Security management	Provides a set of task based commands for use by an administrator to manage Microsoft Exchange.

2.5.2 Non-evaluated Functionality

38 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 ICT 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).

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

- the IMAP4 and POP3 protocols
- all clients that can be used to connect to the TOE, and
- all externally compiled lists that the TOE relies on for filtering of email messages

2.6 Usage

2.6.1 Evaluated Configuration

40 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluated configuration is based on default installation of the TOE with the additional configuration stated below. 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.

2.6.2 Installation prerequisites

2.6.2.1 Hardware prerequisites

41 The following are the recommended minimum hardware requirements for Microsoft Exchange 2010 SP1 Enterprise servers (English) 64-bit:

- Any of the following processors:
  - x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) ; or
  - x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform.
- At least 1.2 GB of available disk space on the drive on which you install Exchange. 200 MB of available disk space on the system drive. An additional 500 MB of available disk space is needed for each Unified Messaging (UM) language pack that you plan to install. Disk partitions must be formatted as NTFS file systems. This requirement applies to the following partitions:
  - System partition;
  - Partitions that store Exchange 2010 binary files;

- Partitions containing storage group files, including transaction log files;
- Partitions containing database files; and
- Partitions containing other Exchange 2010 files.

- DVD-ROM drive, local or network accessible.
- Screen resolution set to 800 x 600 pixels or higher.
- At least the following amounts of memory:
  - For servers hosting a single Exchange 2010 role: 4 gigabytes (GB) of RAM;
  - For servers hosting both the Client Access and Hub Transport roles: 8 GB RAM; and

a) For servers hosting multiple roles (Hub Transport, Client Access, and Mailbox server roles): 10GB RAM.

42 For additional guidance regarding the minimum memory requirements for servers hosting Exchange 2010 roles, please see the "Understanding Memory Configurations and Exchange Performance" and "Understanding Multiple Server Role Configurations in Capacity Planning" sections of Microsoft Exchange 2010 help [3].

43 Additional memory requirements exist for the server hosting the Mailbox server role based on the number of mailbox databases that exist. For minimum memory required, based on the number of mailbox databases, see the following table or the "Understanding the mailbox database cache" section of Microsoft Exchange 2010 help.

Database count	Minimum required physical RAM
1–10	2 GB
11-20	4 GB
21-30	6 GB
31-40	8 GB
41-50	10 GB
51-60	12 GB
61-70	14 GB
71-80	16 GB
81-90	18 GB
91-100	20 GB

44 The recommended minimum and maximum paging file size for Exchange 2010 servers is the amount of physical RAM plus 10MB.

45 Notes: The paging file size recommendation accounts for the amount of memory needed to collect information if the operating system fails. By

default, if the operating system fails, it will copy everything in memory to a .dmp file. That file can be examined later to determine the cause of the failure. To be able to copy everything that is stored in memory, you must have a paging file size that can hold everything in memory, plus some additional space to gather the data.

46 Intel Itanium IA64 processors are not supported.

2.6.3 Software prerequisites

47 Before the installation of the TOE, the operating system has to be installed on the machine.

48 The supported operating system is Windows Server 2008 R2 Standard and Enterprise Edition. The following software must also be installed on all Exchange 2010 servers:

- Microsoft .NET Framework Version 4. http://www.microsoft.com/downloads/details.aspx?FamilyID=9cfb2d51-5ff4-4491-b0e5-b386f32c0992&displaylang=en
- Microsoft Windows PowerShell v2.0 and Windows Remote Management (WinRM) 2.0. For download information, see Microsoft Knowledge Base article 968929, Windows Management Framework (Windows PowerShell 2.0, WinRM 2.0, and BITS 4.0)1.
- Microsoft Windows Installer 4.5 (or above) http://go.microsoft.com/fwlink/?LinkId=151819
- Security update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 (http://support.microsoft.com/kb/2416471).

49 Exchange 2010 requires that you do not have the Network News Transfer Protocol (NNTP) service or the Simple Mail Transfer Protocol (SMTP) service installed.

50 The servers hosting Exchange 2010 must be configured to meet the prerequisites as defined in the “Exchange 2010 prerequisites” section of Microsoft Exchange 2010 Help [3].

2.7 Delivery procedures

51 This section outlines the delivery process required for secure acceptance of the TOE. The end user or administrator should check the TOE version and the package integrity in accordance with the guidance provided by the developer [4].

2.7.1 Integrity of the Package

52 Exchange 2010 and subsequent SP1 package download can be verified by checking that the binaries are signed with the Microsoft certificate as follows.

53 The files contained on the installation media as well as the service pack 1 installation file should have their digital signatures checked. This is performed through the completion of the following steps for each file:

- Right-click on the file and select “properties”.
- Click on the “digital signatures” tab.
- Click on the “details” button.
- Verify that the name of the signer is “Microsoft Corporation” and click on “details”.
- Check that the digital signature information identifies the signature as ok.

2.7.2 Version Numbers for the TOE

54 The next section describes versioning in general for Exchange 2010. This section describes versioning for Exchange 2010 in detail and explains how to identify the correct version number.

2.7.3 General introduction into versioning of Exchange 2010

55 The Target of Evaluation (TOE) is “Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit Build 14.01.0218.015”.

56 Note that there is a product version number and for each executable there is a file version number. When the product is shipped, these version numbers will be the same, though they will be in a different format and the same number may be displayed in different formats. During development, some files may be revised and therefore have a different file version number as that number includes the rev or revision number.

57 Note also that leading and trailing zeroes in the product version number are sometimes displayed (e.g. 14.01.0218.015) and sometimes not displayed (e.g. 14.1.218.15).

58 There are two methods to examine the version of an instance of Exchange 2010, from the properties of the executable file and from the Exchange 2010 administrative console. Either can be used to determine the version number of an instance of Exchange Server. Note that a version number in the format “14.x.y.z” can also be read as “Version 14.x (build y.z)”. Both versions are equivalent.

59 The File version number or the product version number 14.x.y.z verifies that the instance corresponds to the evaluated version named in the ST "Exchange Server 2010 SP1". The numbers "14.x" in the file version number and the product version number both indicate Exchange Server 2010.

60 The version numbering scheme of the executable parts of the TOE is defined as following: Exchange Server is labelled 14.x.y.z.

61 The "x" indicates the minor version number. The "y" is the build number. For every new version, that number is incremented. The "z" is the number of rebuilds of the same build. On a few occasions, late in the development process if ever, the "z" represents builds when another group needs to hard code an Exchange Server build number before the final build. Technically, there is no difference between a build and a rebuild. A rebuild is done in situations when the build number of the product should not be changed due to another build process, e.g. if minor changes to the code happen after a certain build of the product has been shipped.

62 For example, the 2nd rebuild of the 685th build of Exchange 2010 would be 14.0.685.2. The next rebuild would be 14.0.685.3 and the next build would be 14.0.686.0.

2.7.4 Getting the version number for the TOE

63 To see the Exchange 2010 version, from the Exchange Management shell, enter the Cmdlet "get-ExchangeServer | fl" and check "AdminDisplayVersion" for the version number of Exchange Server 2010 and "Edition" for the product version.

64 When "AdminDisplayVersion" equals "Version 14.0 (build 639.21)" and "Edition" equals "Enterprise" the correct version of the TOE has been installed.

65 **Note:** It is important that all installed roles (Mailbox-, Unified Messaging-, Client Access-, Hub-, Edge-Role) are verified separately.

2.7.5 Exchange 2010 Build - Versioning

66 The final RTM build of Exchange 2010 is build 639.21. When you view the version information in the Exchange Management Console or examine the value of the AdminDisplayVersion property for Exchange servers in the Exchange Management shell, it shows the version as 639.21.

2.7.6 Exchange 2010 SP1 Build (Evaluated Configuration) - Versioning

67 Once service pack 1 has been applied to Exchange 2010, the build will be 14.01.0218.015. When you view the version information in the Exchange Management console or examine the value of the AdminDisplayVersion

property for Exchange servers in the Exchange Management shell, it shows the version as 14.01.0218.015.

2.7.7 Documentation

68 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. The documents can be downloaded from the secure website: https://www.stratsec.net/Microsoft-Exchange2010-CC-Certification.aspx

a) Microsoft Exchange 2010 Help ([3]); and

b) E14_EAL4_AGD_Guidance_Documentation (Ref [4]),

69 User documentation is hosted on a website with communication protected by https. If a user is concerned about the authenticity of the documents, they can verify the certificate on the server hosting the website. The certificate should be issued to "www.stratsec.net".

2.7.8 Secure Usage

70 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.

71 The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures (as described in this document and in the Microsoft Exchange 2010 Help), and only by trustworthy staff.

72 The administrator must ensure that the TOE is delivered, installed, configured, managed and operated in a manner that is consistent with IT security by doing the appropriate integrity checks.

73 No untrusted software shall be installed on the machines the TOE is installed on.

74 The administrator(s) shall ensure that during TOE installation and operation that the platform the TOE is running on allows the secure operation of the TOE.

75 The administrator should ensure that the KB2416471 patch has been applied to the environment. This will solve the .net oracle padding information disclosure vulnerability (CVE-2010-3332).

76 The platform upon which the TOE resides shall be Windows Server 2008 Enterprise Edition x64 Edition R2. The platform provides:

- Access Control to restrict modification to TOE executables, the platform itself, configuration files and databases (mailboxes and public folders) only to the authorized administrators.

- Functionality for supporting and enforcing identification and authentication of users. The platform shall ensure the identification and authentication of users except for the case that they connect via a non TLS encrypted Outlook Voice Access connection.

- Methods to store and manage TSF data for the TOE. Further, the platform will provide a role concept for administrative roles and restrict access to TSF data where necessary.

Chapter 3 - Evaluation

3.1 Overview

77 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

78 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [5], [6], [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [8]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9] & [12]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.3 Functional Testing

79 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. The evaluators chose to repeat all developer tests, ensuring that all SFR's were tested and allowing the evaluator to focus independent testing on new features from the previous version for greater assurance in the changes made to the TOE.

3.4 Penetration Testing

80 The developer performed penetration tests on 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. The evaluators performed these tests to determine if 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;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

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

81 The developers search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables.

Chapter 4 - Certification

4.1 Overview

82 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

83 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of Exchange 2010 SP1 performed by the Australasian Information Security Evaluation Facility, stratsec.

84 stratsec has found that Exchange 2010 SP1 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.

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

4.3 Assurance Level Information

86 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained though an informal model of the TOE security policy.

87 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

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

89 ALC_FLR.3 is a class that is used to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions and the distribution of corrective action information to users. Additionally, this sub-activity determines whether the developer's procedures provide for the corrections of the security flaws, for the receipt of flaw reports from TOE users, for

assurance that the corrections introduce no new security flaw, for the establishment of a point of contact for each TOE user and for the timely issue of corrective actions to TOE users. The evaluators examined the flaw remediation procedures and determined that the product complies with the ALC_FLR.3

4.4 Recommendations

90 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.

91 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) Ensure that the KB2416471 patch has been applied to the environment. This will solve the .net oracle padding information disclosure vulnerability (CVE-2010-3332)

Annex A - References and Abbreviations

A.1 References

[1] Exchange 2010 SP1 EAL4 Security Target Version 1.0 (E14_EAL4_ASE_1.0.docx) 21 Dec 10.

[2] Australian Government Information Security Manual (ISM), November 2010, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Microsoft Exchange 2010 Help, 4th October 2010, Exch2010Help.chm.

[4] Exchange 2010 SP1 Guidance Documentation Version 1.0 (E14_EAL4_AGD_1.0.docx).

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

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

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

[10] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

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

[14] Evaluation Technical Report for Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit, Version 1.0, Released: 1 February 2011, (Identifier: EFS-T024 ETR).

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DNS	Domain Name System
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EM64T	Extended Memory 64 Technology
GCSB	Government Communications Security Bureau
IMAP4	Internet Message Access Protocol Version 4
ISM	Information Security Manual
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
TSP	TOE Security Policy
UM	Unified Messaging