EAL4+ Security Target

Common Criteria: EAL4 augmented with ALC_FLR.3

Version 1.0

21-DEC-10

Document management

Document identification

Document ID	E14_EAL4_ASE
Document title	Microsoft Exchange 2010 SP1 EAL4 Security Target
Release authority	Amy Blumenfield (amyblu)
Product version	Exchange 2010 SP1 Enterprise (English) 64-bit (Build: 14.01.0218.015)

Document history

Version	Date	Description
1.0	21-DEC-10	Initial release.

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Microsoft Exchange 2010 EAL4+ Security Target
ST Version	1.0, 21-DEC-10
TOE Reference	Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit Build 14.01.0218.015
Assurance Level	EAL4 augmented with ALC_FLR.3
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. International Standard – International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 15408:1999.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either TOE security functions or environmental controls.
- Section 4 defines the security objectives for the TOE and environment.
- Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 6 provides a summary of the TOE, identifying the IT security functions provided by the TOE and also the assurance measures designed to meet the assurance requirements.
- Section 7 provides a rationale to explicitly demonstrate that security objectives have been satisfied by the TOE.

1.3 TOE overview

1.3.1 TOE type and usage

The Target of Evaluation (TOE) is Microsoft Exchange 2010 SP1 Enterprise (English) 64-bit (Build 14.01.0218.015) and is referred to as both Exchange and Exchange 2010 in this document. The TOE is an e-mail and collaboration server that provides secure access to personal and shared data for a variety of clients using various protocols.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

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 function	Description
Security management	Provides a set of task based commands for use by an Administrator to manage Microsoft Exchange.

1.4 TOE description

1.4.1 Physical scope of the TOE

The TOE comprises the Exchange software and is installed on a Windows server operating system supported by suitable hardware. A typical installation of the TOE can be found in Figure 1 below and identifies the various server roles and components of the TOE.

The underlying platform for the evaluated version of Exchange 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.

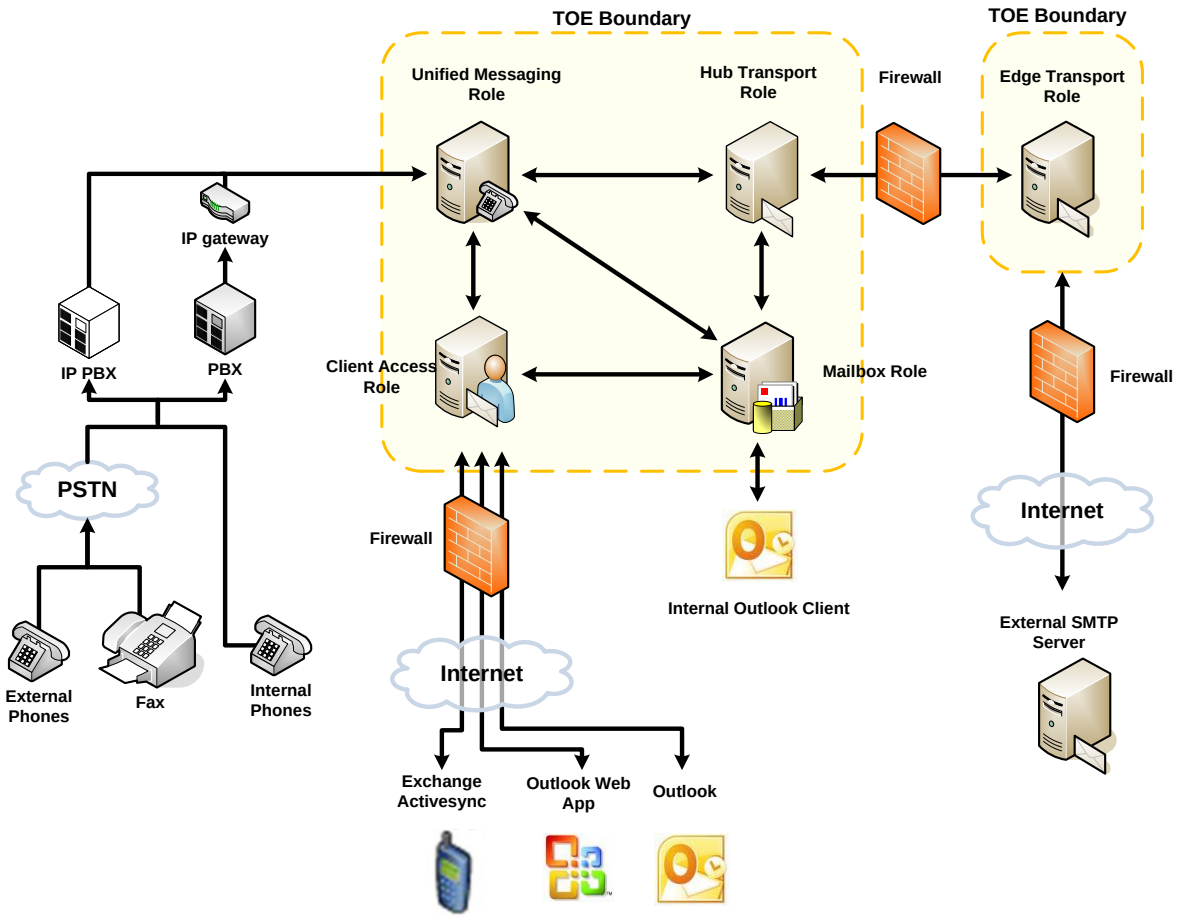

Figure 1 – Exchange 2010 SP1 architecture

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 organization installations, these roles may be installed on individual servers. The TOE roles communicate in the same way whether they are installed on one server or many servers. More information about the installation of the TOE is provided in the related guidance documents.

The following table describes each of the Exchange Server roles specified in Figure 1 above.

Server role	Description
Mailbox Server Role	The Mailbox server role hosts mailbox and public folder databases. The administrator manages mail Lifecycle folders and policies from a Mailbox server. The mailbox server role, in conjunction with the environment, provides access control for users, mail, fax, and voice messages.
Client Access Server Role	This is the server that hosts the client protocols. The Client Access Server also exposes a Web Services interface for application developers. The Client Access server role accepts connections to the Exchange server from a variety of different clients. See Section 1.5.1 for more details on client applications and protocols.
Unified Messaging Server Role	Unified Messaging combines voice messaging, fax, calendaring and e-mail, which are accessible from a telephone or a computer. The Exchange Unified Messaging server integrates Exchange Server with telephony networks and brings Unified Messaging features to the core of Exchange Server. Outlook Voice Access (OVA) is a feature of the Unified Messaging Role and lets users access their mailbox using telephone communication. OVA can optionally be secured by the Transport Layer Security Protocol (TLS).
Hub Transport Server Role	This is the mail routing server that routes mail within the Exchange organization. The Hub Transport server role handles all mail flow inside the organization, applies transport rules, applies journaling policies, and delivers messages to the recipient's mailbox. Messages that are sent to the Internet are relayed by the Hub Transport server to the Edge Transport server role that is deployed in the perimeter network.

Server role	Description
Edge Transport Server Role	This is the mail routing server that sits at the perimeter of the network topology and routes mail into and out of the Exchange organization. The Edge Transport server role handles the following scenarios: • **Mail Flow** - The Edge Transport server role accepts mail coming into the Exchange organization from the Internet and routes all outbound messages to the Internet. • **Filtering** - The Edge Transport server role helps protect the Exchange organization from spam by filtering inbound messages as they arrive and before they are delivered to the internal private network.

1.5 Logical scope of the TOE

1.5.1 Supported protocols and clients

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 tunneled over HTTP,
- Web Services Application Programming Interface (API) for in-house applications, and
- SIP/RTP for Outlook Voice Access (OVA).

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.

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.

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.

The Unified Messaging server role in Exchange 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.

1.5.2 Excluded features

The following components and features are considered outside the scope of the evaluation:

- 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 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, July 2009.

- Part 3 conformant, EAL4 augmented. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL4 augmented with ALC_FLR.3.

3 Security problem definition (ASE_SPD)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through assumptions about the security aspects of the environment and any threats to the assets that the TOE will be providing protection.

3.2 Assumptions

Identifier	Assumption statement
A.COM_PROT	It is assumed that the communication channels between all server roles are appropriately secured against eavesdropping and manipulation by physical protection of the wire or by using encryption. Any internet connection to a server role is assumed to be appropriately secured by a firewall. Finally, it is assumed that the connection between the TOE and the user (connecting to the Unified Messaging role, the Mailbox Role, the Hub role, or the Client Access Server role) is appropriately secured by a physical protection of the wire or by using encryption to avoid eavesdropping or manipulation of the communication.
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.
A.PLATFORM	The platform upon which the TOE resides is Windows Server 2008 R2 Enterprise Edition x64 (English). 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 administrators authorized to perform these functions. • 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 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 the access to TSF data where necessary. Other than the software necessary for the management and operation of the

Identifier	Assumption statement
	TOE (e.g. management tools) it is assumed that no untrusted software is installed on the machines the TOE is installed on. It is assumed that the administrator ensures that the machines the TOE is installed on support the secure operation of the TOE.
A.BLOCKLIST	Block/allow lists from third parties which are used to evaluate email messages have to be of sufficient quality and trustworthy. Therefore it is assumed that only third party block/allow lists from trustworthy sources will be used and that the download of these block/allow lists is appropriately secured with respect to the integrity and authenticity of the block/allow lists
A.NO_EVIL_ADM	There will be one or more competent administrator(s) assigned to manage the TOE, its platform and the security of the information both of them contain. The administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
A.PHYS_PROTECT	The TOE and its platform will be located within facilities providing controlled access to prevent unauthorized physical access.

3.3 Threats

Identifier	Threat statement
T.UNAUTH_DAC	An unauthenticated user may attempt to read, create, modify or delete information contained in private stores (i.e. mailboxes) or public stores (i.e., public folders), which are managed by the TOE. An attacker may try to get access to mailboxes or public folders although he has no account information and is not authenticated.
T.AUTH_DAC	A user who has been authenticated may attempt to read, delete or modify information contained in another user's private store for which this user has not been authorized. For example: A user could use his account information to authenticate against Windows (the TOE relies on identification and authentication of the operating system). Once authenticated he could try to get unauthorized access to mailboxes belonging to other users of the TOE.

T.UNAUTHUSE	An authenticated user may attempt to read, delete or modify information contained in a public folder (e.g. shared folders and documents) that belongs to a group the user is not a member of or is not authorized to use. This scenario is similar to the scenario described in T.AUTH_DAC but in this case the authenticated user tries to get unauthorized access to a public folder instead of a private store, although he is not a member of a group that is allowed to access the folder or is not authorized to use.
T.SPAM	An attacker could send Unsolicited Commercial email (UCE or spam) through the TOE, and have it delivered to mailboxes controlled by the TOE. The threat is an external entity that may send unsolicited messages to TOE users consuming TOE resources or delivering unwanted information to TOE users. For example, this unwanted information may result in an attempt to obtain financial information from the end-user (a “phishing” attack)
T.DL_MISUSE	An unauthenticated user or an authenticated but unauthorized user may send messages that consume TOE resources by delivering inappropriate email, such as UCE to a distribution group. A distribution group may be restricted in a way that only authenticated and authorized users shall be allowed to send messages to a distribution group. An attacker may attempt to send mail for such a distribution group although he is not allowed to deliver email to this distribution group.

3.4 Organizational security policies

Identifier	Organizational security policy statements
OSP.MAIL_FLOW	Administrators shall be able to control email flow within their organization. The administrator shall be able to prevent email flow between specific senders and recipients based on the flowing characteristics of an email: sender, recipients, subject, classification, header, attachment name, attachment size, attachment MIME type, importance, and keywords contained in the subject or body. The Administrators should also be able to prevent specific attachments from being sent to, from or around the organization.
OSP.WIPE	Administrators shall be able to send wipe commands to supported mobile device platforms.

4 Security objectives (ASE_OBJ)

4.1 Overview

The security objectives are concise statements of the TOE's response to the security problem. Some objectives are to be achieved through the security functionality of the TOE and some elements of the problem will be addressed through the establishment of a secure environment in which the TOE must operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.DAC	The TOE shall prevent unauthorized access to objects maintained in the Exchange Store (i.e. mailboxes, public folders) based on the identity of the user. Therefore the TOE shall provide discretionary access controls to private mailboxes and public folders so that only authorized users can read, modify or delete messages and documents.
O.CONBLK	To keep the level of spam as low as possible, the TOE shall provide the ability to reject an SMTP connection based on the IP address or hostname of the remote SMTP sender using accept and block/allow lists configurable by the administrator. The TOE shall further be able to calculate a reputation level for SMTP servers that express how likely this server is used for SPAM. The TOE shall be able to block messages based on the sending server's reputation level.
O.RESTDIST	The TOE shall allow Administrators to restrict mail routing to distribution groups[1] by only allowing mail to be delivered to the distribution group from authenticated and authorized users. Also, Administrators can specify which users can or cannot send mail to specific distribution groups.
O.REDUCE_SPAM	The TOE shall allow Administrators to reduce unwanted or unsolicited mail (UCE or spam) by providing a filter mechanism based on the sender and receiver information of an email.
O.MAIL_FLOW	The TOE shall allow Administrators to control email flow within their organization. The TOE will provide the administrator with filters to prevent

[1] A distribution group may be either a statically defined group in the Active Directory or created dynamically based on a LDAP query.

Identifier	Objective statements
	email flow between specific senders and receivers based on the following characteristics of an email: sender, recipients (including copied recipients), subject, classification, header, attachment name, attachment size, importance and also keywords contained in the subject or body. Also, the TOE will allow Administrators to prevent specific types of attachments (characterized by the extension or the MIME type of the attachment) from being sent to, from or around the organization.
O.I&A	The TOE shall provide an identification and authentication mechanism for users using Outlook Voice Access in cases the access is not secured by TLS[2]. The resulting information about the identity of the user is then used by other policies of the TOE.
O.WIPE	The TOE shall be able to send remote wipe commands to compatible mobile device platforms. Note: The action of the device on receipt of the command is dependent on the platform and configuration and considered out of scope.

4.3 Security objectives for the IT environment

Identifier	Objective statements
OE.PLATFORM	The platform upon which the TOE resides shall be Windows Server 2008R2 Enterprise Edition x64 (English).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.

[2] In case of a connection that is secured via a mutually authenticated TLS channel, the environment will be responsible for the identification and authentication of the user.

4.4 Security objectives for the non-IT environment

Identifier	Objective statements
OE.COM_PROT	The administrator of the TOE shall ensure that the communication channels between all server roles are appropriately secured against eavesdropping and manipulation by physical protection of the wire or by using encryption. Any internet connection to a server role shall be appropriately secured by a firewall. The administrator shall ensure that the connection between the TOE and the user is appropriately secured by a physical protection of the wire or by using encryption to avoid eavesdropping or manipulation of the communication.
OE.INSTALL	The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures and only by trustworthy staff. The administrator must ensure that the TOE is delivered, installed, configured, managed and operated in a manner that is consistent with IT security. Beside the software necessary for the management and operation of the TOE (e.g. management tools) no untrusted software shall be installed on the machines the TOE is installed on. The administrator(s) shall ensure – during TOE installation and operation - that the platform the TOE is running on allows the secure operation of the TOE.
OE.BLOCKLIST	Block/allow lists from third parties - which are used to evaluate email messages - have to be of sufficient quality and trustworthy. Therefore, the administrator shall ensure that only third party block/allow lists from trustworthy sources will be used and that the download of these block/allow lists is appropriately secured with respect to the integrity and authenticity of the block/allow lists
OE.PHYSICAL	The administrators shall ensure that those parts of the TOE and its platform that are critical to security policy are protected from any physical attack.

5 Security requirements (ASE_REQ)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.3 Security functional requirements

5.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.2 and summarized in the table below.

Identifier	Title
FDP_ACC.1a	Subset access control (Folder)
FDP_ACC.1b	Subset access control (Group)
FDP_ACF.1a	Security attribute based access control (Folder)
FDP_ACF.1b	Security attribute based access control (Group)
FDP_IFC.1a	Subset information flow control (Connect)
FDP_IFC.1b	Subset information flow control (SRL)
FDP_IFC.1c	Subset information flow control (Message)
FDP_IFC.1d	Subset information flow control (AttachmentFilter)
FDP_IFC.1e	Subset information flow control (Transport)
FDP_IFF.1a	Simple security attributes (Connect)
FDP_IFF.1b	Simple security attributes (SRL)
FDP_IFF.1c	Simple security attributes (Message)
FDP_IFF.1d	Simple security attributes (AttachmentFilter)
FDP_IFF.1e	Simple security attributes (Transport)
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behavior (Remote Wipe)

Identifier	Title
FMT_SMF.1	Specification of Management Functions
FMT_MSA.1	Management of security attributes
FMT_MSA.3a	Static attribute initialization (Folder)
FMT_MSA.3b	Static attribute initialization (Group)
FMT_MSA.3c	Static attribute initialization (Connect)
FMT_MSA.3d	Static attribute initialization (SRL)
FMT_MSA.3e	Static attribute initialization (Message)
FMT_MSA.3f	Static attribute initialization (AttachmentFilter)
FMT_MSA.3g	Static attribute initialization (Transport)

5.3.2 FDP_ACC.1a Subset access control (Folder)

Hierarchical to:	No other components.
FDP_ACC.1a.1	The TSF shall enforce the [**Discretionary Access Control SFP**] on [**Subjects:** **a) processes acting on behalf of users** **Objects:** **a) Mailbox, public folder items[3] and (sub)folders** **Mailbox operations:** **a) List folder** **b) Create subfolder** **c) Create item** **d) Read item** **e) Edit item** **f) Delete item** **g) Modify folder permissions** **h) Send item** **Public folder operations:** **a) List Folder** **b) Create subfolder** **c) Create item** **d) Read item** **e) Edit item** **f) Delete item** **g) Modify folder permissions**].
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	None.

[3] Mailbox and public folder items include all objects that are stored in a mailbox or public folder (e.g. emails, contacts or certificates)

5.3.3 FDP_ACC.1b Subset access control (Group)

Hierarchical to:	No other components.
FDP_ACC.1b.1	The TSF shall enforce the [**Distribution Group Restriction SFP**] on [**Subjects:** **a) users sending e-mail** **objects:** **a) distribution groups** **operation:** **a) use, i.e. send messages to a distribution group**].
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	None.

5.3.4 FDP_ACF.1a Security attribute based access control (Folder)

Hierarchical to:	No other components.
FDP_ACF.1a.1	The TSF shall enforce the [**Discretionary Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID[4] of the user and its corresponding role** **Object attributes:** **a) Object name** **b) Owner of the folder**].
FDP_ACF.1a.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed if the ID of the user is linked[5] to a role permitted to perform the request operation on the object.**].
FDP_ACF.1a.3	The TSF shall explicitly authorize access of subjects to objects based on the

[4]The ID of the current user is provided by the Windows Operating System or by the authentication policy as expressed in FIA_UAU.2 (only when the user is connected via non-TLS secured Outlook Voice Access).

[5]The link from a user ID to a role may not be direct. A user may be linked to a role assignment which is then linked to an end-user role.

	following additional rules: [**None**].
FDP_ACF.1a.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.3.5 FDP_ACF.1b Security attribute based access control (Group)

Hierarchical to:	No other components.
FDP_ACF.1b.1	The TSF shall enforce the [**Distribution Group Restriction SFP**] to objects based on the following: [**Object attributes (distribution groups):** **a) Message Delivery Restrictions** **1. "Require that all senders are authenticated" restriction** **2. "Accept messages from a specific list of senders" list** **3. "Reject messages from a specific list of senders" list].** **Subject attribute:** **a) ID of the user and its corresponding role** **b) Authentication status within exchange**].
FDP_ACF.1b.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) the "require that all senders are authenticated" is set to false; or** **b) the "require that all senders are authenticated" is set to true and the subject is authenticated (i.e. the corresponding ID is available),** **and** **a) the ID of the sending user is in the "Accept messages from a specific list of senders" list and not the "Reject messages from a specific list of senders" list**].
FDP_ACF.1b.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1b.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.3.6 FDP_IFC.1a Subset information flow control (Connect)

Hierarchical to:	No other components.
FDP_IFC.1a.1	The TSF shall enforce the [**Connection Filtering SFP**] on [**Subjects:** **a) External SMTP Servers** **b) Edge Transport Server Role** **Information:** **a) email messages** **Operations:** **a) email transfer**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.7 FDP_IFC.1b Subset information flow control (SRL)

Hierarchical to:	No other components.
FDP_IFC.1b.1	The TSF shall enforce the [**Sender Reputation SFP**] on [**Subjects:** **a) External SMTP Servers** **b) Edge Transport Server Role** **Information:** **a) email messages** **Operations:** **a) email transfer**].

Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.8 FDP_IFC.1c Subset information flow control (Message)

Hierarchical to:	No other components.
FDP_IFC.1c.1	The TSF shall enforce the [**Message Filtering SFP**] on [**Subjects:** **a) External SMTP Servers** **b) Edge Transport Server Role** **Information:** **a) email messages** **Operations:** **a) email transfer**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.9 FDP_IFC.1d Subset information flow control (AttachmentFilter)

Hierarchical to:	No other components.
FDP_IFC.1d.1	The TSF shall enforce the [**Attachment SFP**] on [**Subjects:** **a) External SMTP Servers** **b) Edge Transport Server Role** **Information:** **a) email messages** **Operations:** **a) email transfer**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.10 FDP_IFC.1e Subset information flow control (Transport)

Hierarchical to:	No other components.
FDP_IFC.1e.1	The TSF shall enforce the [**Hub Transport SFP**] on [**Subjects:** **a) Hub Transport Server Role** **Information:** **a) email messages** **Operations:** **a) email transfer**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.11 FDP_IFF.1aSimple security attributes (Connect)

Hierarchical to:	No other components.
FDP_IFF.1a.1	The TSF shall enforce the [**Connection Filtering SFP**] based on the following types of subject and information security attributes: [**Subject attributes:** **a) IP address of the external SMTP server** **b) allow/block lists of the Edge Transport Server Role** **c) list of exceptional recipients[6] of the Edge Transport Server Role** **Information attributes:** **a) recipients of the e-mail**].
FDP_IFF.1a.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**None**].
FDP_IFF.1a.3	The TSF shall enforce the **additional ordered rules** [**a) If the IP address of the sending external SMTP server is listed on a local allow list, the message will be accepted**

[6] 'Exceptional Recipients' are recipients within the Exchange Organization which are permitted to receive e-mails from senders on the block lists. Exceptional recipients must be explicitly added as 'exceptions' to block lists,

	b) If the IP address of the sending external SMTP server is listed on a local block list, the message will be rejected **c) If the IP address of the sending external SMTP server is listed on a remote allow list, the message will be accepted** **d) If one of the recipients of the e-mail is on the local list of exceptional recipients the message will be accepted** **e) If the IP address of the sending external SMTP server is listed on a remote block list, the message will be rejected** **f) Else the message will be accepted**].
FDP_IFF.1a.4	The TSF shall explicitly authorize an information flow based on the following rules: [**None**].
FDP_IFF.1a.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	This functionality utilizes the following kinds of allow and block lists: a) Local allow and block lists maintained by Administrators b) Remote allow and block lists retrieved from external service providers (so called “block list service providers”) c) A local list of exceptional recipients. The remote lists are not considered to be Security Attributes in the context of this policy as they are not stored locally.

5.3.12 FDP_IFF.1b Simple security attributes (SRL)

Hierarchical to:	No other components.
FDP_IFF.1b.1	The TSF shall enforce the [**Sender Reputation SFP**] based on the following types of subject and information security attributes: [**Subject attributes** **a) Sender Reputation Level (SRL) of the external SMTP server (calculated by the TOE)** **b) SRL Threshold** **c) local list of SRL values from the Edge Transport Server Role** **Information attributes:** **a) None**].

FDP_IFF.1b.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**None**].
FDP_IFF.1b.3	The TSF shall enforce the [**additional rules** **If:** **a) the local list of SRL values contains an entry for the external SMTP server with a SRL value greater than or equal to the SRL threshold; or** **b) The SRL value (calculated by the TOE) for the external SMTP server is greater than or equals the SRL Threshold;** **the server will be added to the local block list of FDP_IFF.1a (Connect) for an Authorized Administrator configurable period of time**].
FDP_IFF.1b.4	The TSF shall explicitly authorize an information flow based on the following rules: [**None**].
FDP_IFF.1b.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.3.13 FDP_IFF.1c Simple security attributes (Message)

Hierarchical to:	No other components.
FDP_IFF.1c.1	The TSF shall enforce the [**Message Filtering SFP**] based on the following types of subject and information security attributes: [**Subject attributes:** **a) sender and recipient filtering lists from the Edge Transport Server Role** **b) local address book[7] from the Edge Transport Server Role** **Information attributes:** **a) MAIL FROM: field of the RFC 2821 envelope** **b) RFC 2822 header** **c) RCPT TO: field of the RFC 2821 envelope**].

[7] The local address book is a list of local SMTP addresses.

FDP_IFF.1c.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**The e-mail will be accepted unless:** **a) the sender listed in the MAIL FROM: field of the (RFC 2821) message envelope is on the sender filtering list or** **b) the sender in the FROM header of the message (RFC 2822) is on the sender filtering list or** **c) the MAIL FROM: field of the RFC 2821 message envelope is blank[8] and the FROM header of the message (RFC 2822) does not contain a valid e-mail address[9] or** **d) the recipient listed in the RCPT TO: field of the RFC 2821 message envelope is on the recipient filtering list or** **e) the recipient does not exist in the local address book**].
FDP_IFF.1c.3	The TSF shall enforce the [**None**].
FDP_IFF.1c.4	The TSF shall explicitly authorize an information flow based on the following rules: [**None**].
FDP_IFF.1c.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	None.

5.3.14 FDP_IFF.1d Simple security attributes (AttachmentFilter)

Hierarchical to:	No other components.
FDP_IFF.1d.1	The TSF shall enforce the [**Attachment SFP**] based on the following types of subject and information security attributes: [**Subject attributes:** **a) Attachment Policy of the Edge Transport Server Role** **Information attributes:**

[8] As this field can never be completely empty, the term “blank” refers to a so called null address which is a MAIL FROM field that contains the characters "<>"

[9] A valid email address in this context means a string in the structure of [recipient]@[domain].[top level domain]

	a) MIME Type **b) extension of the attachment**].
FDP_IFF.1d.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**The information flow is permitted if not explicitly prohibited by the Attachment policy**].
FDP_IFF.1d.3	The TSF shall enforce the [**additional rule:** **Attachments will be stripped or emails containing attachments will be blocked in accordance with the Attachment policy**].
FDP_IFF.1d.4	The TSF shall explicitly authorize an information flow based on the following rules: [**None**].
FDP_IFF.1d.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	The attachment policy as defined in FDP_IFF.1d (AttachmentFilter) comprises a set of ordered rules that are defined by the administrator of the TOE. These rules are evaluated in order to determine how an e-mail attachment shall be handled. The MIME type and Attachment extension information attributes are used by these rules to define whether a rule shall be applied to an attachment. Each rule is comprised of: a) A set of criteria that defines the attachments to which the rule shall apply (based on MIME type and Attachment extension). b) A set of exceptions to which the rule shall not be applied. c) An action to perform when an attachment meets the rule criteria.

5.3.15 FDP_IFF.1e Simple security attributes (Transport)

Hierarchical to:	No other components.
FDP_IFF.1e.1	The TSF shall enforce the [**Hub Transport SFP**] based on the following types of subject and information security attributes: [**subject attributes:** **a) Hub Transport Policy of the Hub Transport Server Role** **Information attributes:** **a) Sender**

	b) Recipients **c) CC:** **d) Subject** **e) Classification** **f) Header** **g) Attachment Name** **h) Attachment Size** **i) Attachment extension** **j) Importance** **k) Key words in Subject or email body**].
FDP_IFF.1e.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**None**].
FDP_IFF.1e.3	The TSF shall enforce the [**following additional rule:** **For each email the Hub Transport policy shall be evaluated and each rule that fits to the email shall be applied**].
FDP_IFF.1e.4	The TSF shall explicitly authorize an information flow based on the following rules: [**None**].
FDP_IFF.1e.5	The TSF shall explicitly deny an information flow based on the following rules: [**None**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	The Hub transport policy as defined in FDP_IFF.1e (Transport) comprises a set of ordered rules that are defined by the administrator of the TOE. The rules are evaluated in order to determine how an e-mail message shall be handled. Each rule is comprised of: a) A set of criteria that define the mails to which the rule shall be applied (based on the information attributes). b) A set of exceptions to which the rule shall not be applied. c) An action to perform when a mail meets the rule criteria.

5.3.16 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**Outlook Voice Access PIN quality metrics as defined by the administrator including an Outlook Voice Access PIN of at least 8 digits**].
Dependencies:	No dependencies.
Notes:	The Outlook Voice Access PINs are the only secrets maintained by the TOE in the context of this requirement.

5.3.17 FIA_UAU.2User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user **connecting via non TLS-secured Outlook Voice Access** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	The environment is responsible for user authentication prior to any action for users connecting via RPC, SMTP, HTTP, RPC over HTTP, Web Services, TLS-secured OVA.

5.3.18 FIA_UID.2User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user **connecting via non TLS-secured Outlook Voice Access** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	The environment is responsible for user identification prior to any action for users connecting via RPC, SMTP, HTTP, RPC over HTTP, Web Services, TLS-secured OVA.

5.3.19 FIA_USB.1User-subject binding

Hierarchical to:	No other components.
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**a) ID (user's identity)** **b) Group Memberships**].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**None**].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**None**].
Dependencies:	FIA_ATD.1 User attribute definition
Notes:	None.

5.3.20 FMT_MOF.1 Management of security functions behavior (Remote Wipe)

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***modify the behavior of***] the functions [**a) Issue the remote wipe command.**] to [**Authorized Administrators**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.21 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) Management of security attributes for the Discretionary Access Control SFP (FDP_ACC.1a (Folder))** **b) Management of security attributes for the Distribution Group**

	Restriction SFP (FDP_ACC.1b (Group)) **c) Management of security attributes for the Message Filtering SFP (FDP_IFF.1c (Message))** **d) Management of security attributes for the Connection Filtering SFP(FDP_IFF.1a (Connect))** **e) Management of security attributes for the Sender Reputation SFP (FDP_IFF.1b (SRL))** **f) Management of security attributes for the Attachment SFP (FDP_IFF.1d (AttachmentFilter))** **g) Management of security attributes for the Hub Transport SFP (FDP_IFF.1e (Transport))** **h) Management of attributes for authentication via Outlook Voice Access (FIA_UAU.2)** **i) Management of quality metric for user PINs (FIA_SOS.1)** **j) Issue a remote wipe command to a Windows Mobile Device (FMT_MOF.1)**].
Dependencies:	No dependencies.
Notes:	None.

5.3.22 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce ~~the~~ [***All access control and information flow control SFPs***] to restrict the ability to [***query, modify, delete, change default***] the security attributes [**RBAC Roles**] to [**Authorized Administrators and Users with the appropriate role assignment**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.23 FMT_MSA.3a Static attribute initialization (Folder)

Hierarchical to:	No other components.
FMT_MSA.3a.1	The TSF shall enforce the [**Discretionary Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3a.2	The TSF shall allow ~~the~~ [**nobody**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	Every user with an Exchange mailbox, including administrators, is given a role assignment policy by default. Administrators can decide which role assignment policy should be assigned by default, choose what the default role assignment policy should include, override the default for certain mailboxes, or not assign role assignment policies by default at all.

5.3.24 FMT_MSA.3b Static attribute initialization (Group)

Hierarchical to:	No other components.
FMT_MSA.3b.1	The TSF shall enforce the [**Distribution Group Restriction SFP**] to provide [***administratively defined***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3b.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.3.25 FMT_MSA.3c Static attribute initialization (Connect)

Hierarchical to:	No other components.
FMT_MSA.3c.1	The TSF shall enforce the [**Connection Filtering SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3c.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.3.26 FMT_MSA.3d Static attribute initialization (SRL)

Hierarchical to:	No other components.
FMT_MSA.3d.1	The TSF shall enforce the [**Sender Reputation SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3d.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	Here “permissive” means an SRL threshold of “7”.

5.3.27 FMT_MSA.3e Static attribute initialization (Message)

Hierarchical to:	No other components.
FMT_MSA.3e.1	The TSF shall enforce the [**Message Filtering SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3e.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes

	FMT_SMR.1 Security roles
Notes:	None.

5.3.28 FMT_MSA.3f Static attribute initialization (AttachmentFilter)

Hierarchical to:	No other components.
FMT_MSA.3f.1	The TSF shall enforce the [**Attachment SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3f.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.3.29 FMT_MSA.3g Static attribute initialization (Transport)

Hierarchical to:	No other components.
FMT_MSA.3g.1	The TSF shall enforce the [**Hub Transport SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3g.2	The TSF shall allow ~~the~~ [**Authorized Administrator and users with the appropriate role**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	In the context of this ST, the functionality required by FMT_MSA.3.2 shall be seen in the way that the TOE does not provide any functionality to change the default values rather than restricting the access to such functionality.

5.4 TOE security assurance requirements

The assurance package for the evaluation of Exchange 2010 is Evaluation Assurance Level 4 (EAL4), augmented by the life cycle support component that provides systematic flaw remediation (ALC_FLR.3).

EAL4 assurance requirements provide confidence in the security functionality of the TOE by analysis using a functional and interface specification, guidance documentation and the high-level design of the TOE to understand the security behavior.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

EAL4 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

The table below provides a summary of the TOE security assurance requirements for this evaluation. Complete details of all assurance components are located in part 3 of the Common Criteria.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic Modular Design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance class	Assurance components
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6 TOE summary specification (ASE_TSS)

6.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- **Connection Filtering.** The TOE 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 from external networks.
- **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 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. As security management pertains to the configuration and management of the remaining security functions, details are included within the description of each of these security functions. .

6.2 Connection Filtering

Exchange will reject SMTP connections based on IP address of the connecting external SMTP server[10]. To do so, Exchange references allow lists, block lists and a list of exceptional recipients. These lists which may contain IP addresses or IP address ranges. The TOE references local and remote allow and block lists. Local lists are defined by an authorized Administrator while remote allow and block lists are retrieved from external service providers (so called block list service providers).

When an SMTP connection is established, Exchange enforces the following ordered rules, according to the IP address of the external SMTP server:

- If the IP address of the sending SMTP server is listed on a local allow list, the message will be accepted;
- If the IP address of the sending SMTP server is listed on a local block list, the message will be rejected;
- If the IP address of the sending SMTP server is listed on a remote allow list, the message will be accepted;
- If one of the recipients of the e-mail is on the local list of exception recipients, the message will be accepted;
- If the IP address of the sending SMTP server is listed on a remote block list, the message will be rejected;
- Else the message will be accepted.

By default, the local allow and block lists that are used in this Security Function are empty.

The TOE also calculates the Sender Reputation Level (SRL) of a remote SMTP server after at least 20 mails have been received from this server. This SRL is a numeric value between 0 and 9 that serves as an indicator of how likely the sending server is a spammer.

Further, the environment of the TOE maintains a local list of SRL values for known SMTP servers. This list is updated on a regular basis.

[10] An external SMTP server is an SMTP server logically outside the Exchange organization that connects to an Edge Server.

If the local SRL for a sending SMTP server or the calculated SRL has reached or exceeded an administrator configurable value (the SRL Threshold which is 7 by default), the SMTP server will be added to the local block list for an administrator defined period of time.

Functional Requirements Satisfied: FDP_IFC.1a (Connect), FDP_IFC.1b (SRL), FDP_IFF.1a (Connect), FDP_IFF.1b (SRL),FMT_MSA.3c (Connect) and FMT_MSA.3d (SRL).

Security Management for Connection Filtering: The TOE will provide functionality to:

- manage local allow and block lists,
- manage the list of exceptional recipients,
- manage the use of remote block and allow lists,
- manage the use of the list of local SRL values, and
- configure SRL threshold settings and the period of time for which servers exceeding the threshold will be added to the block list.

6.3 Message filtering

Exchange allows the administrators to configure the TOE to reduce spam received by an organization. The Message Filter will accept or reject messages based on the rules of the following policies. By default, messages will be accepted by this policy.

Messages will be rejected if:

- the sender listed in the MAIL FROM: field of the RFC 2821 message envelope is on the sender filtering list, or
- the sender in the FROM header of the message (RFC 2822) is on the sender filtering list, or
- the MAIL FROM: field of the RFC 2821 message envelope is blank[11] and the FROM header of the message (RFC 2822) does not contain a valid email address, or
- the recipient listed in the RCPT TO: field of the RFC 2821 message envelope is on the recipient filtering list, or

[11] As this field can never be completely empty the term blank refers to a so called null address which is a MAIL FROM field that contains only the characters "<>"

- the recipient does not exist in the local address book

Finally, the TOE evaluates the SPF record for the sending domain and stamps the result on the message. This SPF record is published by domain servers in addition to their standard DNS information and identifies the machines that are allowed to send emails on behalf of the domain. In this way, the SPF record can help to identify forged addresses.

By default, the sender and recipient filtering list for this Security Function are empty.

Functional Requirements Satisfied: FDP_IFC.1c (Message), FDP_IFF.1c (Message), and FMT_MSA.3e (Message).

Security Management for Message Filtering: The TOE will provide functionality to manage sender and recipient filtering lists.

6.4 Attachment Filtering

The TOE applies an attachment filter to incoming mail based on the e-mail attachments.

The TOE provides the administrator the ability to specify that messages that contain a specified attachment or attachment type be subject to a predefined action. The Administrator can choose to block the whole message while optionally advising the sender that the message was not delivered, or remove the attachment and deliver the message. This policy is defined by the Administrator based on the Attachment MIME Type or the Attachment extension.

The default policy is to remove all attachments of the following MIME types and extensions:

- **MIME Type:** application/x-msdownload, message/partial, text/scriptlet, application/prg, application/msaccess, text/javascript, application/x-javascript, application/javascript, x-internet-signup, application/hta

- **Extensions:** *.xnk, *.wsh, *.wsf, *.wsc, *.vbs, *.vbe, *.vb, *.url, *.shs, *.shb, *.sct, *.scr, *.scf, *.reg, *.prg, *.prf, *.pif, *.pcd, *.ops, *.mst, *.msp, *.msi, *.psc2, *.psc1, *.ps2xml, *.ps2, *.ps11xml, *.ps11, *.ps1xml, *.ps1, *.msc, *.mdz, *.mdw, *.mdt, *.mde, *.mdb, *.mda, *.lnk, *.ksh, *.jse, *.js, *.isp, *.ins, *.inf, *.hta, *.hlp, *.fxp, *.exe, *.csh, *.crt, *.cpl, *.com, *.cmd, *.chm, *.bat, *.bas, *.asx, *.app, *.adp, *.ade.

Functional Requirements Satisfied: FDP_IFC.1d (AttachmentFilter), FDP_IFF.1d (AttachmentFilter), and FMT_MSA.3f (AttachmentFilter).

Security Management for Attachment Filtering: The TOE will provide functionality to manage the Attachment Filtering Policy. This functionality will allow authorized Administrators to add or delete rules to the Attachment Filtering Policy.

6.5 Transport Filtering

The TOE allows an administrator to configure a set of ordered rules that can be applied to all messages passing through the Hub Transport server role. The Hub server will evaluate all the rules in order and execute any rules that apply. By default, no rules exist for this policy initially.

The administrator can define rules for messages based on the following attributes of an email:

- Sender,
- Recipients,
- CC:,
- Subject,
- Classification,
- Header,
- Attachment name,
- Attachment size,
- Attachment extension,
- Importance, and
- Key words in Subject or email body.

Functional Requirements Satisfied: FDP_IFC.1e (Transport), FDP_IFF.1e (Transport), and FMT_MSA.3g (Transport).

Security Management for Transport Filtering: The TOE will provide functionality to manage the Hub Transport Policy. This functionality will allow authorized Administrators to add or delete rules to the Hub Transport Policy.

6.6 Access Control

The TOE uses Role Based Access Control (RBAC) permissions for the Mailbox, Hub Transport, Unified Messaging, and Client Access server roles. RBAC has two primary ways of assigning permissions to users in the organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions to control access to all functions and data within the TOE.

Permissions available for the mailbox and public folders include:

Mailbox permissions: The AccessRights parameter specifies the rights needed to perform the operation. Valid values include:

- FullAccess
- SendAs
- ExternalAccount
- DeleteItem
- ReadPermission
- ChangePermission
- ChangeOwner

Public folders: The AccessRights parameter specifies the rights being added. This parameter accepts the following values:

- **ReadItems** - The user has the right to read items within the specified public folder.
- **CreateItems** - The user has the right to create items within the specified public folder.
- **EditOwnedItems** - The user has the right to edit the items that the user owns in the specified public folder.
- **DeleteOwnedItems** - The user has the right to delete items that the user owns in the specified public folder.
- **EditAllItems** - The user has the right to edit all items in the specified public folder.

- **DeleteAllItems** - The user has the right to delete all items in the specified public folder.
- **CreateSubfolders** - The user has the right to create subfolders in the specified public folder.
- **FolderOwner** - The user is the owner of the specified public folder. The user has the right to view and move the public folder and create subfolders. The user can't read items, edit items, delete items, or create items.
- **FolderContact** - The user is the contact for the specified public folder.
- **FolderVisible** - The user can view the specified public folder, but can't read or edit items within the specified public folder.

In addition to access rights, an Administrator can create rights based upon roles, which includes multiple access rights. This parameter accepts the following values for roles:

- **None** - FolderVisible
- **Owner** - CreateItems, ReadItems, CreateSubfolders, FolderOwner, FolderContact, FolderVisible, EditOwnedItems, EditAllItems, DeleteOwnedItems, DeleteAllItems
- **PublishingEditor** - CreateItems, ReadItems, CreateSubfolders, FolderVisible, EditOwnedItems, EditAllItems, DeleteOwnedItems, DeleteAllItems
- **Editor** - CreateItems, ReadItems, FolderVisible, EditOwnedItems, EditAllItems, DeleteOwnedItems, DeleteAllItems
- **PublishingAuthor** - CreateItems, ReadItems, CreateSubfolders, FolderVisible, EditOwnedItems, DeleteOwnedItems
- **Author** - CreateItems, ReadItems, FolderVisible, EditOwnedItems, DeleteOwnedItems
- **NonEditingAuthor** - CreateItems, ReadItems, FolderVisible
- **Reviewer** - ReadItems, FolderVisible
- **Contributor** - CreateItems, FolderVisible

Functional Requirements Satisfied: FDP_ACC.1 (Folder), FDP_ACF.1 (Folder), FMT_MSA.1, FMT_MSA.3 (Folder).

Security Management for Access Control: The RBAC permission model has removed the administrative task of modifying and managing access control lists (ACLs), present in versions of Exchange prior to Exchange Server 2010.

RBAC allows administrators to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables administrators to more closely align the roles assigned to users and administrators to the actual roles they hold within the organization. In Exchange 2010, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups; implemented through role groups and role assignment policies.

Both role groups and role assignment policies associate users with the permissions they need to perform their jobs. In addition to these methods, a third and more advanced method, direct user role assignment, can also be used.

Role groups:

- One or more Administrators can be members of a role group. They can also be members of more than one role group.
- The role group is assigned one or more role assignments. These link the role group with one or more administrative roles that define what tasks can be performed.
- The role assignments can contain management scopes that define where the users of the role group can perform actions. The scopes determine where the users of the role group can modify configuration.

Role assignment policies:

- One or more users can be associated with a role assignment policy.
- The role assignment policy is assigned one or more role assignments. These link the role assignment policy with one or more end-user roles. The end-user roles define what the user can configure on his or her mailbox.
- The role assignments between role assignment policies and roles have built-in scopes that restrict the scope of assignments to the user's own mailbox or distribution groups.

Direct role assignment (advanced):

- A role assignment can be created directly between a user or Universal Security Group (USG) and one or more roles. The role defines what tasks the user or USG can perform.

- The role assignments can contain management scopes that define where the user or USG can perform actions. The scopes determine where the user or USG can modify configuration.

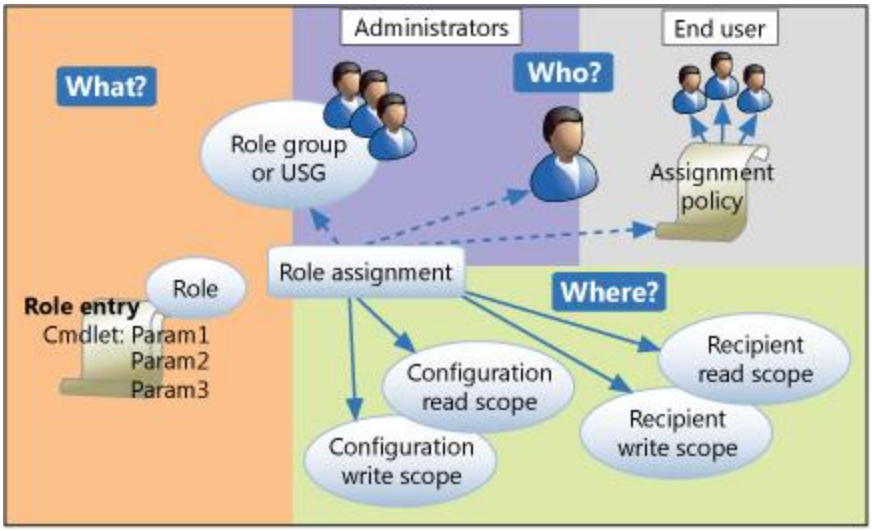

Figure 2 – RBAC Overview

Functional Requirements Satisfied: FDP_ACC.1a (Folder), FDP_ACC.1b (Group), FDP_ACF.1a (Folder), FDP_ACF.1b (Group), FMT_MSA.3a (Folder) FMT_MSA.3b (Group) and FMT_MSA.1.

6.7 Identification and Authentication

The TOE will identify and authenticate all users connecting to the TOE via Outlook Voice Access utilizing a SIP/RTP connection, with the exception of users who connect utilizing a mutually authenticated TLS connection.

The identity of the user in the context of this Security Function is represented by the user's mailbox number or a telephone number that is transmitted from the PBX to the TOE (caller ID). When a user initiates a phone call to OVA, the TOE references the associated Caller Id that is transmitted from the PBX as an additional mechanism to identify the user. If the Caller Id matches a user, the user does not have to enter their mailbox number, but still must enter their PIN prior to gaining access to any TOE resources[12]. If the Caller ID is not transmitted or the transmitted number has not been assigned to a mailbox, the user is asked to enter their mailbox number. After this identification, the user is asked to

[12] Please note that the caller ID and the mailbox number are only mechanisms for the TOE to map the calling user to their corresponding ID.

enter their PIN for authentication. After successful authentication, the TOE associates the calling user with their corresponding Windows user account and the corresponding roles.

In the event that a PBX establishes a connection utilizing the TLS protocol with mutual authentication for SIP/RTP, the identification and authentication of the user is not performed by the TOE, but is the responsibility of the TLS authenticated application which is part of the IT environment.

Further, the TOE will ensure that PINs generated by administrators, the user or the TOE itself meet a quality metric as defined by the administrator based on:

- the number of digits of the PIN,
- the history of the last PINs, and
- common patterns.

The TOE specifically ensures that a PIN has at least a length of 8 digits.

After the user has been successfully authenticated, the user's identity is used to control the user's access to data to ensure that one user cannot access other user's data via this interface.

Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.2, FIA_UID.2, and FIA_USB.1.

Security Management for Identification and Authentication: The TOE will provide functionality to manage the attributes of users for Outlook Voice Access. Specifically this will allow Authorized Administrators to manage the quality metric for Outlook Voice Access PINs.

6.8 Distribution Group Restriction

Exchange can place restrictions on how messages are delivered to individual recipients. Message delivery restrictions apply to all recipient types and are used for controlling access to specific recipients.

An administrator can configure the following message delivery restrictions for a distribution group:

- Accept messages from a specific list of sender**s** - Specify a list of senders from which to accept messages, the recipient will receive messages only from those senders. By default, all recipients are configured to accept messages from all senders.
- Reject messages from a specific list of senders - Specify a list of senders from which to reject messages, the recipient will reject messages from those senders. By default, all recipients are configured not to reject messages from any senders (this list has priority over the accept list).

- Require that all senders are authenticated – Setting that requires that all senders are authenticated; any messages from senders that don't have valid logon credentials will be rejected.

Functional Requirements Satisfied: FDP_ACC.1b (Group), FDP_ACF.1b (Group), FMT_MSA.3b (Group).

Security Management for Distribution Group Restriction: The TOE will provide functionality to:

- create and delete distribution groups, and
- configure message delivery restrictions.

6.9 Remote Device Wipe

Microsoft Exchange enables administrators to send a command to a mobile phone that will perform a wipe of that phone. This process, known as a remote device wipe, clears all Exchange information that's stored on the mobile phone.

The Remote Wipe function is implemented through the Exchange ActiveSync protocol, which utilizes a HTTP connection established between the managed mobile device (which initiates the connection) and the listening server.

In order for the Remote Wipe function to work, a device must support the Provision command introduced in version 2.5 of the Exchange Active Sync protocol. For devices that do not support Provision or the claimed ability to support policies, a remote wipe command essentially blocks the device from syncing with Exchange Server.

Initiating remote wipe sets the following information in the device's sync state that resides in the user's mailbox:

- WipeRequestTime: Current date/time
- WipeSendTime: Null
- WipeAckTime: Null
- LastDeviceWipeRequestor: SMTP address of cmdlet executor
- WipeConfirmationAddresses: SMTP Addresses specified in -NotificationEmailAddresses parameter or Null if not present

Remote wipe initiation also causes any “hanging” command to complete by artificially deleting a custom folder within the user’s mailbox thereby immediately returning a response to the device.

Any subsequent commands by a provisionable device will result in a response from the server with the unique HTTP status code 449 telling the device to send up a Provision request. The server will respond to this request with a status telling the device to remote wipe. At this time, WipeSendTime will be set to the current data/time in the device’s sync state that resides in the user’s mailbox.

A non-provisionable device, if allowed to sync by policy, will receive an HTTP status code of 403 (Forbidden) for all subsequent requests.

In order for a remote wipe request to be actioned, the device must first connect to the Exchange server and establish an ActiveSync session. Once connected, the device will be issued with the remote wipe request for the Exchange server. Upon receiving the status to remote wipe from the server, the device should send up its acknowledgement Provision request with a remote wipe status value of 1 then promptly clear its memory. When the server receives this acknowledgement request, it sets the WipeAckTime to the current data/time in the device’s sync state that resides in the user’s mailbox.

Device wipe can be cancelled by an Administrator with the Clear-ActiveSyncDevice –Cancel cmdlet/parameter combination. The command is only valid if the server has not sent a Provision response asking the device to wipe. This state is indicated by a valid WipeRequestTime date/time stamp but a null value for WipeSendTIme in the device’s sync stat e that resides in the user’s mailbox.

Functional Requirements Satisfied: FMT_MOF.1 (Remote Wipe).

Security Management for Mobile Device Wipe: Through either the Exchange Management Console (EMC) or Exchange Management Shell administrators can issue remote wipe commands.

7 Rationale

7.1 Overview

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- **Security objectives rationale.** Provides coverage for the security objectives for the TOE and the environment, ensuring that all threats and assumptions are effectively addressed.
- **Security requirements rationale.** Provides justification for TOE assurance requirements, evidence that all dependencies have been addressed, specification of strength of function for all probabilistic mechanisms and demonstration that the IT requirements address the TOE and environment objectives.
- **TOE summary specification rationale.** Provides evidence that the IT security functions and assurance measures are adequate to implement the security functional and assurance requirements.

7.2 Security objectives rationale

7.2.1 Security objectives for the TOE

Threats	Objective	Justification
T.UNAUTH_DAC	O.DAC O.I&A OE.PLATFORM	The O.DAC, O.I&A and OE.PLATFORM objectives collectively address the threat (T.UNAUTH_DAC) of an unauthenticated and unauthorized user gaining access to information contained in private or public stores that are controlled by the TOE. O.DAC provides discretionary access controls on these public and private information stores which limit access to only authorized users. O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook

Threats	Objective	Justification
		Voice Access connection. The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user for access control; utilized by O.DAC to grant or deny access.
T.AUTH_DAC	O.DAC O.I&A OE.PLATFORM	The O.DAC, O.I&A and OE.PLATFORM objectives collectively address the threat (T.AUTH_DAC) of an authenticated user gaining access to information contained in private stores that are controlled by the TOE, to which the user is not authorized to access. O.DAC provides discretionary access controls on these private stores which limit access to only authorized users. O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection. The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user for access control; utilized by O.DAC to grant or deny access.
T.UNAUTHUSE	O.DAC O.I&A OE.PLATFORM	The O.DAC, O.I&A and OE.PLATFORM objectives collectively address the threat (T.AUTH_DAC) of an authenticated user gaining access to information contained in a public store (public folder) that is controlled by the TOE, to which the user is not authorized to access. O.DAC provides discretionary access controls on these public information stores which limit access to only authorized users. O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection.

Threats	Objective	Justification
		The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user for access control; utilized by O.DAC to grant or deny access.
T.SPAM	O.CONBLK	O.CONBLK (blocking of SMTP connections from IP addresses of suspected spammers) directly traces back to T.SPAM. Blocking connections from suspected UCE SMTP hosts helps reduce the amount of UCE because the TOE is able to filter SMTP connections. Therefore T.SPAM is partly countered by O.CONBLK (the other aspect of T.SPAM about known senders of UCE is countered by O.REDUCE_SPAM. See below).
	O.REDUCE_SPAM	Blocking messages with suspected UCE sender addresses helps reduce the amount of UCE because the TOE is able to filter the messages. Therefore, T.SPAM is partly countered by O.REDUCE_SPAM (the other aspect of T.SPAM about known IP addresses of UCE origin is countered by O.CONBLK. See above).
T.DL_MISUSE	O.RESTDIST O.I&A OE.PLATFORM	O.RESTDIST (access control for distribution groups) directly addresses T.DL_MISUSE. T.DL_MISUSE defines misuse of distribution groups as a threat. O.RESTDIST counters this threat by allowing the administrator to restrict the use of a distribution group to only those users that have been authenticated and/or – optionally – identify users who are explicitly authorized to use a distribution group. O.I&A provides the mechanism for Identification and Authentication for the cases where users connect via non TLS-secured OVA. OE.PLATFORM provides the mechanism for Identification and Authentication except for the case that users connect via a non TLS encrypted Outlook Voice Access connection. The combination of O.I&A and OE.PLATFORM ensures that all users are authenticated and that the TOE can rely on the identity of the user to enforce the policy as defined in O.RESTDIST.
OSP.MAIL_FLOW	O.MAIL_FLOW	The OSP.MAIL_FLOW is directly and completely addressed by the Security Objective O.MAIL_FLOW. The

Threats	Objective	Justification
		OSP as well as the Objective define that an administrator shall be able to control email flow within their organization and use the same set of email characteristics for this functionality.
OSP.WIPE	O.WIPE	The OSP.WIPE is directly and completely addressed by the Security Objective O.WIPE. The OSP as well as the Objective define that administrators shall be able to send wipe commands.

7.3 Security objectives for the IT and non-IT environment

Assumptions	Objectives	Justification
A.COM_PROT	OE.COM_PROT	This objective for the IT environment upholds the assumption that the environment will provide secure communication channels between all server roles, users and the TOE, and will implement a firewall between the TOE and the Internet (if Internet connectivity exists).
A.INSTALL	OE.INSTALL	This objective for the IT environment upholds the assumption that the TOE will be delivered, installed, configured and set up in accordance with delivery documentation.
A.PLATFORM	OE.PLATFORM OE.INSTALL	These objectives for the IT environment uphold the assumption that the environment will provide access control, user identification and authentication (except when connecting using a non-TLS secured connection using the Outlook Voice Access function), and methods to store, manage and limit access to TSF data. Additionally, these objectives uphold that no untrusted software is installed on the machines supporting the TOE, and that the Administrator ensures that the TOE is operating on the correct operating system platform.
A.BLOCKLIST	OE.BLOCKLIST	This objective for the IT environment upholds the assumption that only third party block and/or allow lists from trustworthy sources are used, and that the integrity of the block lists are maintained.

Assumptions	Objectives	Justification
A.NO_EVIL_ADMIN	OE.INSTALL	This objective for the IT environment upholds the assumption that the TOE is delivered, installed, configured and set up by trustworthy staff, and operated in a manner that is consistent with IT security.
A.PHYS_PROTECT	OE.PHYSICAL	This objective for the IT environment upholds the assumption that the environment will provide physical protection of the TOE.

7.4 Security requirements rationale

7.4.1 Dependency analysis

SFR	Dependency	Inclusion
FDP_ACC.1a	FDP_ACF.1 Security attribute based access control	FDP_ACF.1a
FDP_ACC.1b	FDP_ACF.1 Security attribute based access control	FDP_ACF.1b
FDP_ACF.1a	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1a, FMT_MSA.3a
FDP_ACF.1b	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1b, FMT_MSA.3b
FDP_IFC.1a	FDP_IFF.1 Simple security attributes	FDP_IFF.1a
FDP_IFC.1b	FDP_IFF.1 Simple security attributes	FDP_IFF.1b
FDP_IFC.1c	FDP_IFF.1 Simple security attributes	FDP_IFF.1c
FDP_IFC.1d	FDP_IFF.1 Simple security attributes	FDP_IFF.1d
FDP_IFC.1e	FDP_IFF.1 Simple security attributes	FDP_IFF.1e
FDP_IFF.1a	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.1a, FMT_MSA.3c
FDP_IFF.1b	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.1b, FMT_MSA.3d

SFR	Dependency	Inclusion
FDP_IFF.1c	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.1c, FMT_MSA.3e
FDP_IFF.1d	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.1d, FMT_MSA.3f
FDP_IFF.1e	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_IFC.1e, FMT_MSA.3g
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1 not included – see rationale below
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1 not included – see rationale below
FMT_SMF.1	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1a, FDP_ACF.1a, FMT_SMF.1 FMT_SMR.1 not included – see rationale below

SFR	Dependency	Inclusion
FMT_MSA.3a	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3b	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3c	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3d	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3e	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3f	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below
FMT_MSA.3g	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1 not included – see rationale below

7.4.2 Rationale for not addressing all dependencies

FIA_ATD.1 and FMT_SMR.1 have not been included as SFRs as the environment is responsible for performing the required functionality as specified in OE.PLATFORM.

7.4.3 TOE IT requirements correspondence

Objective	SFRs	Demonstration
O.DAC	FDP_ACC.1a FDP_ACF.1a FMT_MSA.1 FMT_MSA.3a FMT_SMF.1	Discretionary access control for user access to mailboxes and public folders is directly supported by access control components FDP_ACC.1a and FDP_ACF.1a. FMT_MSA.1 ensures that access control are also provided for the attributes that are utilized for this policy. FMT_MSA.3a ensures that appropriate default values are used for all attributes of this policy. Eventually, FMT_SMF.1 ensures that the TOE provides management functionality to query and modify the attributes of the access control policy.
O.CONBLK	FDP_IFC.1a FDP_IFF.1a FDP_IFC.1b FDP_IFF.1b FMT_MSA.3c FMT_MSA.3d FMT_SMF.1	O.CONBLK is represented by the SFRs FDP_IFC.1a and FDP_IFF.1a, which build an information flow policy for connection blocking based on allow and block lists and FDP_IFC.1b and FDP_IFF.1b, which build an information flow policy based on the “Sender Reputation Level” that determines the likelihood of a sender being a spammer. Support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3c resp. FMT_MSA.3d to ensure appropriate default values for the policies.
O.RESTDIST	FDP_ACC.1b FDP_ACF.1b FMT_MSA.3b	O.RESTDIST is represented by the SFRs FDP_ACC.1b and FDP_ACF.1b, which form an access control policy for distribution groups to restrict the ability of users to send emails to Distribution Groups.

Objective	SFRs	Demonstration
	FMT_SMF.1	FMT_MSA.3b ensures that appropriate default values are used for all attributes of this policy. Eventually, FMT_SMF.1 ensures that the TOE provides management functionality to query and modify the attributes of the policy.
O.REDUCE_SPAM	FDP_IFC.1c FDP_IFF.1c FMT_MSA.3e FMT_SMF.1	O.REDUCE_SPAM is represented by the SFRs FDP_IFC.1c and FDP_IFF.1c, which form an information flow policy to filter e-mail based on the RCPT TO: and MAILFROM fields of the RFC 2821 envelope and the RFC 2822 header of the email. Indirect support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3e to ensure that appropriate default values are provided.
O.MAIL_FLOW	FDP_IFC.1d FDP_IFF.1d FDP_IFC.1e FDP_IFF.1e FMT_MSA.3f FMT_MSA.3g FMT_SMF.1	O.MAIL_FLOW is represented by a combination of two information flow policies. FDP_IFC.1d and FDP_IFF.1d allow e-mail attachment filtering already on the Edge Transport Server Role of the TOE while FPP_IFC.1e and FDP_IFF.1e allow the administrator to specify rules for e-mail transport on the hub server role based on characteristics of the e-mail. Support is provided by FMT_SMF.1 to enable management of the security attributes used by this policy and by FMT_MSA.3f resp. FMT_MSA.3g to ensure that appropriate default values are provided.
O.I&A	FIA_UAU.2 FIA_UID.2 FIA_USB.1 FIA_SOS.1 FMT_SMF.1	O.I&A requires the identification and authentication of users that connect to the TOE via a non TLS OVA session (for the rest of the cases the environment is responsible for identification and authentication). This identification and authentication mechanism for non TLS-secured Outlook Voice Access is defined in FIA_UID.2 and FIA_UAU.2. FIA_USB.1 defines the security attributes for subjects that are used to bind subjects to their users. Finally, FIA_SOS.1 ensures that the PINs for Outlook Voice Access follow a quality metric to reduce the likelihood that an attacker can guess the PIN of a user.

Objective	SFRs	Demonstration
		Indirect support is provided by FMT_SMF.1 components from the FMT class to enable management of the security attributes used by this policy.
O.WIPE	FMT_MOF.1 FMT_SMF.1	O.WIPE specifies that the TOE shall be able to send remote wipe commands to compatible platforms. This management capability is specified in FMT_MOF.1 and listed as a management function in FMT_SMF.1.

7.4.4 TOE assurance requirements

This ST contains the assurance requirements from the CC EAL4 assurance package augmented with ALC_FLR.3. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures. This ST is based on good rigorous commercial development practices and has been developed for a general environment for a TOE that is readily available and does not require modification to meet the security needs of the environment specified in this ST.

The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. Specifically, that the TOE will not process information that requires protection from attackers possessing a Basic or Enhanced-Basic attack potential, and that protection from obvious vulnerabilities is required.

7.5 TOE summary specification rationale

7.5.1 Security functions

The security functions rationale has been provided as part of Section 6.

7.5.2 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_ARC.1 Security architecture description	Development	The development assurance measure provides all the necessary design documentation to support the effective detailed analysis of the TOE for an evaluation at EAL4. The security architecture description provides a detailed description of the TSF security architecture. The functional specification provides a detailed description of the security functions of the TOE. The design documentation provides a complete definition of the TSF, allowing for sufficient analysis to be performed.
ADV_FSP.4 Complete functional specification		
ADV_IMP.1 Implementation representation of the TSF		
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will use the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.4 Production support, acceptance procedures and automation	Life cycle support	The life cycle support measures provide the assurance that the TOE is developed and subsequently managed using a well defined and controlled approach. Configuration management measures provide the assurance that configured

Assurance requirement	Assurance measures	Demonstration
ALC_CMS.4 Problem tracking configuration management		items are managed and maintained in a controlled manner, through the demonstration of well defined processes, procedures and requirements. By placing the TOE and its components into this configuration management list provides assurance that the TOE components are only modified in a controlled manner with proper authorization. Employing sufficient security measures in the delivery process of the TOE to consumers ensures that the TOE is not tampered with prior to its receipt. Procedural, personnel and physical security related documentation is used to ensure that the confidentiality and integrity of the TOE and its design are maintained throughout the development life cycle. The life cycle support assurance measures provides a set of procedures aimed at the identifying, reporting and addressing security flaws or bugs that may appear in the TOE. An established development lifecycle methodology is employed to guide the development of the TOE. A set of well established development tools exist and are employed in the development of the TOE.
ALC_DEL.1 Delivery procedures		
ALC_DVS.1 Identification of security measures		
ALC_FLR.3 Systematic flaw remediation		
ALC_LCD.1 Developer defined life-cycle model		
ALC_TAT.1 Well-defined development tools		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL4 (augmented with ALC_FLR.3) can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.2 Security objectives		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.2 Derived security Requirements		
ASE_SPD.1 Security problem definition		
ASE_TSS.1 TOE summary specification		
ATE_COV.2 Analysis of coverage	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
ATE_DPT.1 Testing: basic design		
ATE_FUN.1 Functional testing		
ATE_IND.2 Independent testing – sample		
AVA_VAN.3 Focused vulnerability analysis	Vulnerability assessment	The vulnerability assessment assurance measure provides confidence that the TOE and its environment have been assessed for obvious vulnerabilities or exposures. A claim is also provided for the strength of function related to probabilistic mechanisms that are non-cryptographic.