the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Microsoft Exchange Server 2007

Version 1.1.0
July 2nd, 2010

http://cisecurity.org
feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Table of Contents 4
Introduction 7
Explanation of This Document 7
Intended Audience 7
Security Levels 8
Precursor Technical Information 8
1. General Exchange Guidance 10
1.1. General Guidance 10
1.2. Exchange Edge vs. Hub Transport 11
1.3. Edge Server Management 11
1.4. Roles 12
1.5. Features 13
2. Recommended Security Settings for Exchange Controls 15
3. Pre-Installation and Installation Recommendations 36
3.1. Installation Host is Not a Domain Controller 36
3.2. Patches and Updates 36
3.3. Security Configuration Wizard 36
3.4. Disable Unnecessary Exchange Services and Roles 37
4. All Roles 38
4.1. Audit Administrative Access to Exchange 38
4.2. Ensure Fatal Error Reporting is Disabled 38
5. Edge Transport Role 40
5.1. Restrict Accepted Domains 40
5.2. Mail Routing Options 40
5.3. Audit Send Connector Address Space 41
5.4. Enable TLS for Smart Host Basic Authentication 42
5.5. Specify Block List Service Provider 42
5.6. Specify Allow List Service Provider 43
5.7. Filter Recipients Who Are Not in Directory 44
5.8. Filter Recipients 45
5.9. Filter Senders 46
5.10. Filter Blank Senders 46
5.11. Filter Custom Words 47
5.12. Filter Attachment extensions 47
5.13. Configure Allowed IPs 48
5.14. Enable TLS for Basic Authentication 48
5.15. Restrict Mail Send Size 49
5.16. Restrict Mail Receive Size 50
5.17. Restrict Max Recipients 50
5.18. Restrict IP Range For Receive Connectors 51
5.19. Ensure Sender Reputation is Enabled 51
6. Mailbox Role 53
6.1. Restrict Email Deletion Retention 53

6.2. Restrict Mailbox Deletion Retention 53
6.3. Restrict Deletion of Mail or Mailboxes Until Archival 54
6.4. Mounting of Mailbox Database at Startup 55
6.5. Ensure Proper Permissions on Mail Database 55
6.6. Ensure Mailbox Database Cannot Be Overwritten 56
6.7. Verify Default Mailbox Storage Limits 56
6.8. Ensure Public Folder Database Cannot Be Overwritten 57
6.9. Verify Default Public Folder Storage Limits 58
6.10. Audit Public Folder Client Access 59
6.11. Audit Public Folder Administrative Access 59
6.12. Verify Proper Permissions on Public Folder Database 60
6.13. Mounting of Public Folder Database at Startup 60
6.14. Restrict Deletion of Mail or Mailboxes Until Archival 61
6.15. Restrict Mail Send Size 62
6.16. Restrict Mail Receive Size 62
6.17. Restrict Max Recipients 63
6.18. Audit Mailbox Spam Bypass Settings 63
6.19. AntiSpam Updates 64
6.20. Zero out Deleted Database pages 64
7. Hub Transport Role 66
7.1. Restrict Accepted Domains 66
7.2. Mail Routing Options 66
7.3. Audit DNS Lookup Servers 67
7.4. Enable TLS for Basic Authentication 68
7.5. Restrict Out of Office Responses 68
7.6. Restrict Mail Send Size 69
7.7. Restrict Mail Receive Size 69
7.8. Restrict Max Recipients 70
7.9. Restrict IP Range For Receive Connectors 70
8. Client Access Server Role 72
8.1. Require SSL for POP3 72
8.2. Limit number of POP3 connections 72
8.3. Enforce Pop3 Connection Timeouts 73
8.4. Require SSL for IMAP 73
8.5. Enable IMAP connection timeout 73
8.6. Restrict number of IMAP connections 74
8.7. Remove Legacy Web Applications 74
8.8. Restrict Web Authentication Methods 75
8.9. Require SSL for Web Applications 76
8.10. Disable Web Anonymous Access 77
8.11. Enable Logging for Default Website 77
8.12. Enable Policy for ActiveSync 78
8.13. Forbid ActiveSync NonProvisionable Devices 79
8.14. Forbid ActiveSync Simple Device Password 80
8.15. Disable ActiveSync WSS/UNC Access 81
8.16. Require ActiveSync Password 82

8.17. Require ActiveSync Alphanumeric Password 82
8.18. Require ActiveSync Minimum Password Length 83
8.19. Require ActiveSync Password Expiration 84
8.20. Require ActiveSync Password History 85
8.21. Require ActiveSync Encryption 85
8.22. Restrict ActiveSync Attachment Size 86
8.23. Require ActiveSync Policy Refresh 87
8.24. Restrict ActiveSync Maximum Password Attempts 87
8.25. Require ActiveSync Certificate Based Authentication 88
8.26. Require ActiveSync Inactivity Lockout Time 89
8.27. Disable Outlook Anywhere 90
9. Unified Messaging Role 91
9.1. Disable Faxing 91
9.2. Require PIN length 91
9.3. Require PIN complexity 92
9.4. Restrict Allowed In-Country/Region Groups 93
9.5. Restrict Allowed International Groups 93
9.6. VoIP IPSec 94
10. Post Installation 95
10.1. Configure Monitoring 95
10.2. Install Anti-Virus Software 96
10.3. Security Configuration Wizard 96
11. Appendix A: Change History 97

Introduction

Explanation of This Document

This document is a general guide for securing Microsoft Exchange Server 2007 (Exchange) hosted on the Windows Server 2003 platform. The first section pre-installation and installation prescribes general advice for installing Exchange. The document breaks down the (five) 5 roles Exchange 2007 can perform, and makes security recommendations for each. These sets of rules constitute a benchmark. This benchmark represents an industry consensus of "best practices" listing steps to be taken as well as rationale for their recommendation.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Adam Cecchetti, Leviathan Security Group

Contributors and Reviewers
Chris Ahlers
Susan Bradley
Gary Gapinski
Michael Nelte
Paul E. Robichaux
Miles Stevenson
Charles Schmidt
Nguyen Tuan Trung, *Tripwire, Inc.*

Intended Audience

This document is intended for system administrators, but can be read by anyone involved with or interested in installing and/or configuring Exchange. We assume that the reader is a knowledgeable "system administrator." In the context of this document, a knowledgeable system administrator is defined as someone who can create and manage accounts and groups, understands how operating systems perform access control, understands how to set account policies and user rights, is familiar with how to set up auditing and read audit logs, and can configure other similar system-related functionality.

Additionally, it is assumed that the reader is a competent Exchange administrator. Consequently, no tutorial-type information is provided regarding Exchange or electronic messaging in general. Many documents and books exist which provide this information, including Microsoft's web presence at http://www.microsoft.com. That site leads to an extensive array of Exchange-related material.

Practical Application

The best usage of this document is to review the internal security policy for an organization then to make adjustments as necessary. The benchmark can then properly help you gauge the how it should be used to assess the security state of an Exchange server.

Security Levels

Legacy - Settings in this level are designed for Exchange Servers that need to operate with older systems such as Exchange 2003, or in environments where older third party applications are required. The settings will not affect the function or performance of the operating system or of applications that are running on the system.

Enterprise - Settings in this level are designed for Exchange 2007 where legacy systems are not required. It assumes that all Exchange servers are 2007 or later, therefore able to use all possible security features available within those systems. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.

Specialized Security – Limited Functionality – Formerly "High Security," settings in this level are designed for Exchange servers in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Precursor Technical Information

Exchange 2007 Shell

To open the Exchange 2007 Shell

Goto Start->All Programs->Microsoft Exchange Server 2007-> Exchange Management Shell

This will be referred forth in this document as EMShell all commands required to be run in the shell will be prefixed with **EMShell >**

Exchange 2007 Management Console

To open the Exchange Management console

Start->All Programs->Microsoft Exchange Server 2007-> Exchange Management Console

This will be referred forth in this document as EMC all actions first requiring the console will be prefixed with **EMC->**

IIS 6.0 Management Console

To open the Internet Information Server Management Console

Start ->All Programs Administrative Tools -> Internet Information Server (IIS) Manager

This will be referred forth in this document as IIS all actions first requiring the console will be prefixed with **IIS>**

Command Shell

To open the command shell

Start-> Run
Enter *cmd*
Click Ok

This will be referred forth in this document as IIS all actions first requiring the console will be prefixed with **CMD>**

1. General Exchange Guidance

1.1. General Guidance

This chapter contains general security guidance for Exchange Server 2007. The following recommendations are provided to facilitate a more secure platform.

- Review all recommendations to ensure they comply with local policy.
- Do not install Exchange Server 2007 on a domain controller.
- Load the operating system and secure it before loading Exchange onto the platform. It is important to realize that the system cannot be considered to be secured until the operating system has first been secured. If the operating system is not secured, Exchange functionality might be secure but the platform as a whole will be vulnerable.
- Ensure that all relevant operating system security patches have been applied.
- Ensure that all relevant Exchange security patches have been applied.
- Exchange Administrator should require a User's network/domain username to be different than their email alias. If a malicious user has access to your email address, they would also have a valid network/domain username to conduct malicious activity.
- Subscribe to the Windows Security mailing list at: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- Visit and implement appropriate recommendations at the vendor's web site: http://technet.microsoft.com/en-us/library/aa996775.aspx
- Because the recommendations in this document yield a Specialized Security - Limited Functionality posture, it is essential that the administrator:
  - Carefully review the recommendations to ensure that they are not disabling functionality that is required by their enterprise.
  - Test the settings in a non-production environment before deployment.
- The recommended settings only increase security. It is essential to continually monitor the latest in best security practices.

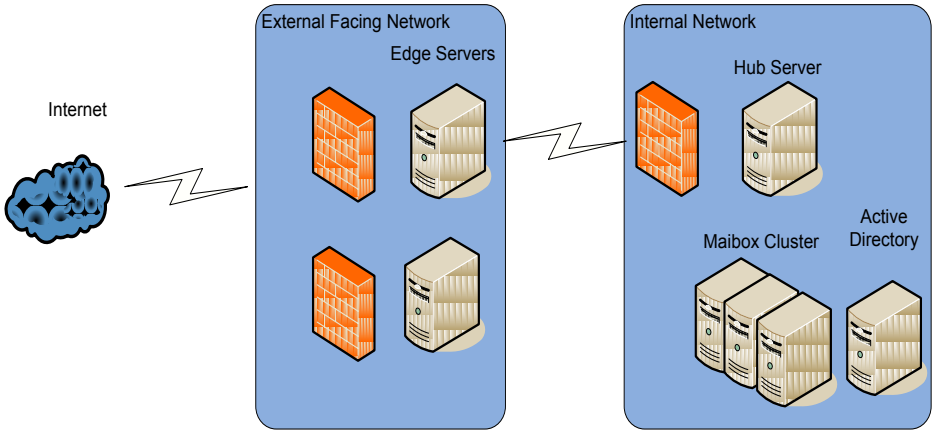
1.2. Exchange Edge vs. Hub Transport

Exchange 2007 supports Edge and Hub server architectures. The Edge server is a server running Exchange 2007 that does not host mailboxes or public folder stores.

The Edge server forwards client requests to the Hub server for processing. Mailboxes and/or public folder stores are hosted on the Hub server(s) that are running Exchange 2007. The advantages of using front-end/back-end server topology are as follows:

- A single namespace for each user.
- Offload processing.
- Strengthened security: Edge servers can be positioned as the single point of access and located after a firewall(s).
- Scalability: As an enterprise expands, adding additional role server can assist in the expansion as well as address load balancing issues.

Figure 1 depicts the recommended Exchange Edge and Hub server architecture. In a real world environment, it is critical to place a firewall in front of each Edge machine. This adds an additional layer of protection between the Internet and the Edge servers. The recommended deployment of Edge servers involves separating each server from the Domain and using ADAM (Active Directory Application



1.3. Edge Server Management

Edge servers are by nature internet facing devices, and thus privy to targeted attacks and possible compromise. A properly installed Edge server will only accept inbound SMTP (25 and 587), combining a proper Exchange configuration

with a firewalling and filtering solution will reduce the attack surface of the Edge server considerably.

In smaller environments Edge transport servers should be deployed as workgroup members. The servers they are hosed on are meant to be deployed in a DMZ separate from the corporate network. As standalone systems they rely on ADAM (Active Directory Application Mode) for configuration and mail routing information. When deployed correctly Edge servers are entirely separate from the Windows infrastructure and rely on no internal Windows services. Joining the Edge server to the internal domain would require trust relationships be established between hosts on the internal network and internal services to be forwarded to the DMZ. This would defeat the purpose of deploying the Edge Server in the DMZ and aid an attacker in taking over the internal network in the case of an Edge server compromise.

For medium and large enterprises Edge server installations manual management and ADAM syncing is simply not an option. In larger environments a separate domain or forest should be created for the Edge servers residing in the DMZ that is only used for the management of the Exchange Edge Cluster. The list of administrators and users that are able to access and administer this tree should be controlled and audited on a periodic basis.

1.4. Roles

Exchange 2007 Servers can be configured to function with a specific role. Roles include Hub Transport, Client Access, Edge Transport, Mailbox, Unified Messaging, or Management Tools Server. This paper provides security recommendations based on each of these roles. Table 1 identifies each role and their associated functions.

Table 1

Client Access	The Client Access role accepts connections from a various user clients. Mail clients such as Microsoft Outlook or Mozilla Thunderbird access mail via POP3 or IMAP4. Mobile devices use ActiveSync, POP3, or IMAP4 to communicate with the Exchange server.
Hub Transport	The Hub Transport role handles all mail flow inside the organization and delivers messages to mailboxes. Email that is sent to external address is relayed by the Hub Transport server to the Edge Transport. Mail that is received from the Internet is processed by the Edge server before being relayed to the Hub Transport.
Edge Transport	The Edge Transport role is deployed on the perimeter network as a stand-alone server. It is designed to minimize the attack surface and

	handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the Exchange organization.
Mailbox	The Mailbox role hosts mailbox databases and public folders.
Unified Messaging	The Unified Messaging role combines voice messaging, fax, and e-mail into one Inbox, which can be accessed from the telephone and the computer.

1.5. Features

Exchange Management Console: The Exchange Management Console is built on a set of snap-ins for the Microsoft Management Console. The EMC provides a graphic management Interface to Exchange Server 2007

Exchange Management Shell: The Exchange Management Shell provides administrators a command-line interface that they can use to administer Exchange 2007. Command line access makes management of Exchange easy with commandlets to manage nearly every aspect of Exchange 2007.

ActiveSync: ActiveSync is a service provided by Exchange Server 2007 that allows users to synchronize e-mail, calendaring, and contact information between the Exchange server and Windows supporting mobile devices, such as PDAs.

Outlook Web Access (OWA): OWA is a remote email client and a basic Exchange Server 2007 messaging service. OWA allows users to access mailboxes and folders using an Internet browser that is compliant with HTML 3.2 and JavaScript standards. The HTML standard provides drag and drop functionality, expandable folder hierarchies, HTML composition, toolbar tips and Kerberos authentication

Public Folders: Exchange Server 2007 supports public folders even though they have been de-emphasized. The purpose of public folders is to provide common access to messages and files. Files can be dragged and dropped into public folders for instant sharing. In addition, sorting rules can be applied to public folders to ensure items are arranged by name or date. Each server has one default public folder store (named the Public Folder Store) that supports the Public Folder tree. There can be up to five stores per storage group, and any number of the five stores may be public folders. Lastly, users can be granted access or denied access to specific public folders.

Public Folder Tree: Public Folder Trees are a group of public folders in a hierarchical structure. One tree can have multiple public folder stores. Each Exchange organization has one default public tree. Additional public folder trees can be created that users can access using Outlook Web Access.

Mailbox Stores: Mailbox Stores is a database for storing mailboxes in Exchange 2007. Mailbox stores hold data that is private to an individual and contain mailbox folders generated each time a new mailbox is created for an individual. Stores are located in storage groups. There can be up to five stores per storage group, and any number of the five stores may be mailbox stores. Each mailbox store has a set of transaction logs associated with it. These transaction logs provide detailed information of messages received and sent from a store in a storage group.

2. Recommended Security Settings for Exchange Controls

This chapter supplies control-specific Exchange guidance. (In this document, the term "control" refers to a specific parameter or setting through which the administrator configures the platform through the user-interface.)

Table 2 identifies the specific security recommendations. The information contained in the control table is the primary means by which the administrator can secure the Exchange platform. Several types of information are provided in the control table. The fundamental security-related information provided includes:

- The control name
- The recommended security setting for the control
- How the administrator can navigate through the user-interface or power shell to access that control

The following is an explanation of the column and row headings in the table.

Column Headings:

- **Reference—** ID/ Number and Title associated with specific control for referencing purposes.
- **Roles—** The role associated with the setting
- **Security Level (SL) —** The security level associated with the setting: Legacy, Enterprise, or Special Security
- **Scorable/Reportable/Manual (SR)—**Identifies whether a control is ("scorable"), or whether the control value could only reported by a tool and not included in the assessment ("reportable"). Lastly, items that are marked "manual", means a tool could neither score nor report on the item.
- **GUI/SH—**Navigation path through the Exchange MC to locate the control setting and the name of the control as it appears in the MS Exchange Management Console. If no MC path is available an Exchange Shell Command is given.
- **Default —** This list the out of the box default install setting in Exchange if any.
- **Suggested —**Suggested setting for the security benchmark.

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Installation Host is Not a Domain Controller	General	E	M	dsquery * "CN=hostname,DC=Domain Controller, DC=domain, DC=com"	N/A	N/A
Patches and updates	General	E	M	wupdmgr	N/A	N/A
Security Configuration Wizard	General	E	M	Start->All Programs->Administrative Tools->Security Configuration Wizard	N/A	N/A
Disable Unnecessary Exchange Services and Roles	General	E	R	*Get-Service* *Get-ExchangeServer | select identity, ServerRole*	N/A	N/A
Audit Administrative Access to Exchange	General	E	M	*Get-ExchangeAdministrator*	N/A	N/A
Ensure Fatal Error Reporting is Disabled	General	E	S	*Microsoft Exchange->Server Configuration-><Role Name>-><Server Name>* *Right click server name Select properties* *General Tab* *Automatically send fatal service error report to Microsoft*	Unchecked $false	Unchecked $false
Restrict Accepted Domains	Edge	E	M	*Microsoft Exchange->Edge Transport->Accepted Domains* *Right Click <name> Properties* *(Tab) General* *Authoritative Domain: Selected*	*Authoritative Domain*	*Authoritative Domain*
Mail Routing Options	Edge	E	S	*Microsoft Exchange->Edge Transport* *(Tab) Send Connectors* *Select <name>* *Right Click Properties* *(Tab) Network* *Select how to send mail with this connector*	DNS	Smart Host if available.

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Audit Send Connector Address Space	Edge	E	M	*Microsoft Exchange->Organization Configuration->Hub Transport* *(Tab) Send Connections* *Right Click <name> properties* *(Tab) Network* *Smart host authentication* *Click Change*	N/A	N/A
Enable TLS for Smart Host Basic Authentication	Edge	E	S	*Microsoft Exchange->Organization Configuration->Hub Transport* *(Tab) Send Connections* *Right Click <name> properties* *(Tab) Network* *Smart host authentication* *Click Change*	Unchecked	Checked
Specify Block List Service Provider	Edge	SS	M	*Microsoft Exchange-> Edge Transport->IP Block List Providers* *Right Click Properties* *Providers (Tab)*	None	Verified Black List Provider
Specify Allow List Service Provider	Edge	SS	M	*Microsoft Exchange-> Edge Transport->IP Block List Providers* *Right Click Properties* *Providers (Tab)*	None	Verified White List Provider
Filter Recipients Who Are Not in Directory	Edge	SS	S	*Edge Transport->Anti Spam -> Recipient Filtering ->* *Properties -> (Tab) Blocked Recipients* *Block messages sent to recipients not listed in Global Address List Checked*	Checked	UnChecked

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Filter Recipients	Edge	E	M	*Edge Transport -> Anti-Spam->Recipient Filter->Blocked Recipients -> Block the following Recipients*	None	Black Listed Recipients
Filter Senders	Edge	E	M	*Edge Transport -> Anti-Spam->Sender Filter->Blocked Senders -> Block the following Senders*	None	Black Listed Senders
Filter Blank Senders	Edge	E	S	*Microsoft Exchange-> Edge Transport -> Anti-Spam -> Sender Filter->Block Senders-> Block Messages from blank senders (check)*	Checked	Checked
Filter Custom Words	Edge	SS	M	*Microsoft Exchange->Edge Transport* *(Tab) Anti-spam* *Content Filtering* *Right Click Properties* *(Tab) Custom Words*	None	Custom
Filter Attachment extensions	Edge	SS	M	*Get-AttachmentFilterEntry | list* Add-AttachmentFilterEntry -Name <MIMEContentType> -Type ContentType	See List	Custom
Configure Allowed IPs	Edge	E	M	*Microsoft Exchange->Edge Transport-><Select server>* *(Tab) Anti-Spam* *Right-Click IP Allow List*	None	Custom
Enable TLS for Basic Authentication	Edge	E	S	*Microsoft Exchange->Edge Transport->Receive Connectors -><name>* *Right Click Properties* *(Tab) Authentication* *Offer Basic Authentication only after starting TLS*	Unchecked	Checked

Restrict Mail Send Size	Edge	E	S	*Get-TransportConfig	select identity, MaxSendSize* *Get-SendConnector	select identity, MaxMessageSize* *Set-TransportConfig –MaxSendSize 20Mb* *Set-SendConnector –MaxMessageSize 20Mb*	30Mb	20Mb

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict Mail Receive Size	Edge	E	S	*Get-TransportConfig | select identity, MaxReceiveSize* *Get-ReceiveConnector |select identity, MaxMessageSize* *Get-TransportServer | select identity, ExternalDsnMaxMessageAttachSize, InternalDsnMaxMessageAttachSize* *Set-TransportConfig -identity <name> -MaxReceiveSize 10MB* *Set-RecieveConnector -identity <name> -MaxMessageSize 10MB* *Set-TransportServer -identity <name> - ExternalDsnMaxMessageAttachSize 10mb* *Set-TransportServer -identity <name> - InternalDsnMaxMessageAttachSize 10mb*	30Mb, 10Mb, 10Mb, 10Mb	10Mb 10Mb 10Mb 10Mb
Restrict Max Recipients	Edge	E	S	*Get-ReceiveConnector | select identity, MaxRecipientsPerMessage* *Set-ReceiveConnector -identity <name> -MaxRecipientsPerMessage 100*	200	100
Restrict IP Range For Receive Connectors	Edge	E	M	*Microsoft Exchange->Server Configuration->Hub Transport (Tab) Receive Connectors Select Name Right Click Properties (Tab) Network*	None	Custom
Ensure Sender Reputation is Enabled	Edge	E	S	*Get-SenderReputationConfig*	Enabled	Enabled

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict Email Deletion Retention	Mailbox	E	S	*Server Configuration->Mailbox->Mailbox Database* *Right Click Properties* *Tab Limits* *Keep deleted items for (days)*	7	7
Restrict Mailbox Deletion Retention	Mailbox	E	S	*Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database* *Right Click Properties* *Tab Limits* *Keep deleted mailboxes for (days)*	30	30
Restrict Deletion of Mail or Mailboxes Until Archival	Mailbox	E	S	*Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database* *Right Click Properties* *Tab Limits* *Do not permanently delete items until the database has been backed up*	Unchecked	Checked
Mounting of Mailbox Database at Startup	Mailbox	E	S	*Microsoft Exchange->Sever Configuration->Mailbox Database Management* *Right Click Properties* *(Tab) General* *Do no mount this database at startup*	Unchecked	Unchecked
Ensure Proper Permissions on Mail Database	Mailbox	E	M	*See Description*	N/A	N/A
Ensure Mailbox Database Cannot Be Overwritten	Mailbox	E	S	*Microsoft Exchange->Server Configuration->Mailbox->Database Managements* *Mailbox Database* *Right Click Properties* *(Tab) General* *This Database can be over written by a Restore*	Checked	Unchecked

Verify Default Mailbox Storage Limits	Mailbox	E	S	*Server Configuration->Mailbox->Mailbox Database* *Right Click Properties* *(Tab) Limits* *Issue warning at (KB) : value* *Prohibit send at (KB) : value* *Prohibit send and receive at (KB) : value*	Custom	Custom

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Ensure Public Folder Database Cannot Be Overwritten	Mailbox	E	S	*Microsoft Exchange->Server Configuration->Mailbox->Database Management* *Public Folder Database* *Right Click Properties* *(Tab) General* *This Database can be over written by a Restore*	Checked	Unchecked
Verify Default Public Folder Storage Limits	Mailbox	E	S	*Microsoft Exchange* **->** *Server Configuration->Mailbox->Public Folder Database* *Right Click Properties* *(Tab) Limits* *Issue warning at (KB) : value* *Prohibit send at (KB) : value* *Prohibit send and receive at (KB) : value*	Custom	Custom
Audit Public Folder Client Access	Mailbox	E	S	*Get-PublicFolderClientPermission -identity "\foldername"*	Custom	Custom
Audit Public Folder Administrative Access	Mailbox	E	S	*Get-PublicFolderAdmistrativePermission -identity "\foldername"*	Custom	Custom
Verify Proper Permissions on Public Folder Database	Mailbox	E	M	Custom	Custom	Custom
Mounting of Public Folder Database at Startup	Mailbox	E	S	*Microsoft Exchange->Sever Configuration->Mailbox* *Public Folder Database Management* *Right Click Properties* *(Tab) General* *Do no mount this database at startup*	Unchecked	Unchecked
Restrict Deletion of Mail or Mailboxes Until Archival	Mailbox	E	S	*Microsoft Exchange-> Server Configuration->Mailbox ->PublicFolder* *Right Click Properties* *Tab Limits* *Do not permanently delete items until the database has been backed up*	Unchecked	Checked

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict Mail Send Size	Mailbox	E	S	*Get-Mailbox | select identity, MaxSendSize* *Get-MailContact | Select identity, MaxSendSize* *Get-DistributionGroup | Select identity, MaxSendSize* *Set-Mailbox -identity <name> -MaxSendSize 10Mb* *Set-MailContact -identity <name> -MaxSendSize 10Mb* *-DistributionGroup -identity <name> -MaxSendSize 10mb*		10Mb 10Mb 10Mb
Restrict Mail Receive Size	Mailbox	E	S	*Get-Mailbox | select identity,MaxReceiveSize* *Get-MailContact | select -identity, MaxReceiveSize* *Get-DistributionGroup | Select identity, MaxReceiveSize* *Set-Mailbox -identity <name> -MaxReceiveSize 10Mb* *Set-MailContact -identity <name> -MaxReceiveSize 10Mb* *Set-DistributionGroup -identity <name> -MaxReceiveSize 10Mb*		10Mb 10Mb 10Mb
Restrict Max Recipients	Mailbox	E	S	*Get-Mailbox | select identity, RecipientLimits* *Set-Mailbox -RecipientLimits 2000*	5000	2000
Audit Mailbox Spam Bypass Settings	Mailbox	E	M	*Get-Mailbox | select identity, AntispamBypassEnabled* *Set-Mailbox -identity <name> -AntispamBypassEnabled $false*	False	False
AntiSpam Updates	Mailbox	E	S	*Get-AntiSpameUpdates* *Enable-AntispamUpdates -SpamSignatureUpdatesEnabled $true -UpdateMode Automatic*	Disabled	See Description

Zero out Deleted Database pages	Mailbox	E	S	*Get-StorageGroup | select Identity, ZeroDatabasePages* *Set-StorageGroup -Identity <name> -ZeroDatabasePages $true*	False	True

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict Accepted Domains	Hub	E	S	*Microsoft Exchange->Edge Transport->Accepted Domains Right Click <name> Properties (Tab) General Authoritative Domain: Selected*	*Authoritative Domain*	*Authoritative Domain*
Mail Routing Options	Hub	E	S	*Microsoft Exchange->Edge Transport (Tab) Send Connectors Select <name> Right Click Properties (Tab) Network Select how to send mail with this connector*	*DNS*	*Smart Host (if available)*
Audit DNS Lookup Servers	Hub	E	M	*Microsoft Exchange->Server Configuration->Hub Transport-> (Tab) Receive Connectors Right Click Properties External DNS Lookups or Internal DNS Lookups*	*None*	*Custom*
Enable TLS for Basic Authentication	Hub	E	S	*Microsoft Exchange->Edge Transport->Receive Connectors -><name> Right Click Properties (Tab) Authentication Offer Basic Authentication only after starting TLS*	*Unchecked*	*Checked*
Restrict Out of Office Responses	Hub	E	S	*Microsoft Exchange->Organization Configuration->Hub Transport-> Remote Domains->General Tab*		*None*
Restrict Mail Send Size	Hub	E	S	*Get-TransportConfig | select identity, MaxSendSize Get-SendConnector | select identity, MaxMessageSize Set-TransportConfig –MaxSendSize 10Mb Set-SendConnector –MaxMessageSize 10Mb*	*30mb 30mb*	*10mb 10mb*

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict Mail Receive Size	Hub	E	S	*Get-TransportConfig | select identity, MaxReceiveSize* *Get-ReceiveConnector |select identity, MaxMessageSize* *Get-TransportServer | select identity, ExternalDsnMaxMessageAttachSize, InternalDsnMaxMessageAttachSize* *Set-TransportConfig -identity <name> -MaxReceiveSize 10MB* *Set-RecieveConnector -identity <name> -MaxMessageSize 10MB* *Set-TransportServer -identity <name> -ExternalDsnMaxMessageAttachSize 10mb* *Set-TransportServer -identity <name> -InternalDsnMaxMessageAttachSize 10mb*	30Mb 30Mb 10Mb 10Mb	10Mb 10Mb 10Mb 10Mb
Restrict Max Recipients	Hub	E	S	*Get-ReceiveConnector | select identity, MaxRecipientsPerMessage* *Set-ReceiveConnector - -MaxRecipientsPerMessage 2000*	5000	2000
Restrict IP Range For Receive Connectors	Hub	SS	M	*Microsoft Exchange->Server Configuration->Hub Transport* *(Tab) Receive Connectors* *Select Name* *Right Click Properties* *(Tab) Network*	None	Custom
Require SSL for POP3	Client Access	E	S	*Get-Popsettings | select identity, LoginType*	SecureLogin	SecureLogin
Limit number of POP3 connections	Client Access	E	S	*Get-Popsettings | select identity, MaxConnections* *Set-Popsettings -identity <name> -MaxConnections 500*	500	500
Enforce Pop3 Connection Timeouts	Client Access	E	S	*Get-PopSettings | select identity, AuthenticatedConnectionTimeout,*	00:30:00 00:01:00	00:20:00 00:01:00

				PreAuthenticatedConnectionTimeout *Set-PopSettings -identity <name> -* *AuthenticatedConnectionTimeout 00:20:00* *-PreAuthenticatedConnectionTimeout* *00:01:00*		

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Require SSL for IMAP	Client Access	E	S	*Get-ImapSettings | select identity, LoginType* *Set-ImapSettings –identity <name> -LoginType SecureLogin*	SecureLogin	SecureLogin
Enable IMAP connection timeout	Client Access	E	S	*Get-ImapSettings | select identity, AuthenticatedConnectionTimeout, PreAuthenticatedConnectionTimeout* *Set-ImapSettings –identity <name> -AuthenticatedConnectionTimeout 00:20:00 –PreAuthenticatedConnectionTimeout 00:01:00*	00:30:00 00:01:00	00:20:00 00:01:00
Restrict number of IMAP connections	Client Access	E	S	*Get-ImapSettings | select identity, MaxConnections* *Set-ImapSettings –identity <name> -MaxConnections 500*	500	500
Remove Legacy Web Applications	Client Access	SS	S	<server name>-> Web Sites->Default Web Site-> {Exchange, Exchweb, Exadmin, Public} *Get-OwaVirtualDirectory* *See Description for Remediation*	Installed	Removed
Restrict Web Authentication Methods	Client Access	E	S	*<Server Name>->Web Sites-><Site Name>* *Right Click Properties* *Tab Directory Security* *Authentication and access control*	See Description	See Description
Require SSL for Web Applications	Client Access	E	S	*<Server Name>->Web Sites->Default Web Site* *Right Click Properties* *Tab Directory Security* *Secure Communications* *Click Edit* *Require Secure Channel SSL* *128-bit encryption*	Checked Unchecked	Checked Checked
Disable Web Anonymous Access	Client Access	E	S	*<Server Name>->Web Sites-><Site Name>* *Right Click Properties* *Tab Directory Security* *Authentication and access control* *Click Edit*	Unchecked	Unchecked

				Enable anonymous access		
Enable Logging for Default Website	Client Access	E	S	*<Server Name>->Web Sites->Default Web Site* *Right Click Properties* *Tab Website* *Enable Logging*	Checked	Checked

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Enable Policy for ActiveSync	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*	None	See Discussion
Forbid ActiveSync NonProvisionable Devices	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Allow NonProvisionable Devices*	Checked	Unchecked
Forbid ActiveSync Simple Device Password	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Allow simple password*	Checked	UnChecked
Disable ActiveSync WSS/UNC Access	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *General Tab* *WSS/UNC Access* *Windows File Shares* *Windows Sharepoint Services*	Checked Checked	Unchecked Unchecked
Require ActiveSync Password	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Require Password*	Unchecked	Checked

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Require ActiveSync Alphanumeric Password	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Require alphanumeric password*	Unchecked	Checked
Require ActiveSync Minimum Password Length	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Minimum password length*	Checked, 4	Checked, 8
Require ActiveSync Password Expiration	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Password Expiration*	Unchecked	60
Require ActiveSync Password History	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Enforce password history*	0	5
Require ActiveSync Encryption	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*	Unchecked	Checked

				Right Click on Policy, Select properties *Password Tab* *Require encryption on device*		

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Restrict ActiveSync Attachment Size	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *General Tab* *Maximum Attachment Size*	Unchecked	Unchecked 3mb
Require ActiveSync Policy Refresh	Client Access	E	S	*Get-ActiveSyncMailboxPolicy | Select identity, DevicePolicyRefreshInterval*	None	*24.00:00:00*
Restrict ActiveSync Maximum Password Attempts	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Number of attempts allowed*	8	8
Require ActiveSync Certificate Based Authentication	Client Access	SS	S	*Server Configuration->Client Access Exchange Active Sync Microsoft-Server-ActiveSync* *Right Click Select Properties* *Authentication (tab)* *Select*	Ignore Client Certs	Require Client Certs
Require ActiveSync Inactivity Lockout Time	Client Access	E	S	*Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies* *Right Click on Policy, Select properties* *Password Tab* *Time without user input before password must be re-entered*	Checked, 15	Checked, 15
Disable Outlook Anywhere	Client Access	SS	S	*Microsoft Exchange->Server Configuration->Client Access-> <Name> Outlook Anywhere Enabled*	Enabled	Disabled

Reference	Role	SL	SR	GUI/SH	Default	Suggested
Disable Faxing	Uni Msg	SS	S	*Microsoft Exchange->Unified Messaging (Tab) UM Dial Plan Right Click <name> Properties (Tab) General Allow users to receive faxes*	Checked	Unchecked
Require PIN length	Uni Msg	E	S	*Microsoft Exchange->Unified Messaging (Tab) UM Mailbox Policies Right Click <name> Properties (Tab) PIN Policies Minimum PIN length*	6	6
Require PIN complexity	Uni Msg	E	S	*Microsoft Exchange->Unified Messaging (Tab) UM Mailbox Policies Right Click <name> Properties (Tab) PIN Policies Allow common patterns in PIN*	Unchecked	Unchecked
Restrict Allowed In-Country/Region Groups	Uni Msg	E	M	*Microsoft Exchange->Organization Configuration->Unified Messaging (Tab) UM Dial Plan Right Click <name> Properties (Tab) Dialing Rule Groups In-Country/Region Rule Groups*	None	Custom
Restrict Allowed International Groups	Uni Msg	E	M	*Microsoft Exchange->Organization Configuration->Unified Messaging (Tab) UM Dial Plan Right Click <name> Properties (Tab) Dialing Rule Groups International Rule Groups*	None	Custom
VoIP IPSec	Uni Msg	E	M	*See Description*	None	Custom
Configure Monitoring	Gen	E	M	*See Description*	None	Custom
Install Anti-Virus Software	Gen	E	M	*See Description*	None	Custom
Security Configuration Wizard	Gen	E	M	*See Description*	None	Custom

3.Pre-Installation and Installation Recommendations

3.1. Installation Host is Not a Domain Controller

Description: Installation of Exchange should never be performed on the same host as a domain controller.

Rationale: Installation of Exchange should be on a standalone server to reduce the attack surface and minimize possible damage done by a system compromise.

Recommendation Level: Enterprise

Audit: dsquery * "CN=hostname, DC=Domain Controller, DC=domain, DC=com"

Remediation: Select a different host for the installation of Exchange.

Scoring Status: Manual

3.2. Patches and Updates

Description: Install all relevant patches and updates before installing Exchange 2007.

Rationale: Ensuring the integrity of the host and its services is integral to performing a secure Exchange installation and deployment. Make sure the Windows 2003 Server is fully up to date before installing Exchange 2007.

Recommendation Level: Enterprise

Audit:
Remediation: Start->Run
wupdmgr

Scoring Status: Manual

3.3. Security Configuration Wizard

Description: Run the Microsoft Security Configuration Wizard to lock down the server Exchange is being installed on. The security configuration wizard should also be run **post installation**.

Rationale: The Security Configuration Wizard will create a security policy and reduce the attack surface of the Windows server.

Recommendation Level: Enterprise

Remediation:
Start->Control Panel->Add Remove Programs
Click Add/Remove Windows Components
Select Security Configuration Wizard
Click next
Click Finish

Start->All Programs->Administrative Tools->Security Configuration Wizard

Scoring Status: Manual

Additional Resources: http://technet.microsoft.com/en-us/library/aa998208.aspx

3.4. Disable Unnecessary Exchange Services and Roles

Description: Remove all services and roles that the individual Exchange server does not require.

Rationale: Reducing the service list to only necessary services simplifies the administration complexity and reduces the attack surface of the Exchange server.

Recommendation Level: Enterprise

Audit:

EMShell > `Get-Service`
EMShell > `Get-ExchangeServer | select identity, ServerRole`

Remediation:

EMShell > `Set-Service -name <name> -startupType Disabled`
CMD > *Setup.com /mode:uninstall /role:<server roles to remove>*

Role Names: HubTransport, ClientAccess, EdgeTransport, Mailbox, UnifiedMessaging, ManagementTools

Scoring Status: Reportable

Additional Resources: http://technet.microsoft.com/en-us/library/bb124115.aspx

4. All Roles

4.1. Audit Administrative Access to Exchange

Description: Restrict administrative access to Exchange to only necessary administrators.

Rationale: Allowing too many administrators or unrestricted administrative access to Exchange can result in a system instability or security compromise. Audit the Exchange administrator list to ensure that the least privileges required are assigned to each admin. This audit will be manual and different for each organization.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ExchangeAdministrator*

Remediation:

EMShell *> Remove-ExchangeAdministrator -identity <name>*

Scoring Status: Manual
Additional Resources: http://technet.microsoft.com/en-us/library/36cc2315-2d5c-4c55-9b7c-e6058c9ad83e.aspx

4.2. Ensure Fatal Error Reporting is Disabled

Description: Restrict sending error reports to Microsoft in the case of a fatal error.

Rationale: This feature controls whether debugging messages are sent to Microsoft whenever a system error is detected. While no sensitive information is sent in the debugging report, the act of sending the report can provide system stability information to attackers. It is disabled by default and should be left as such. If a reoccurring problem occurs that requires Microsoft support enable this feature long enough to collect the report and disable it after.

Recommendation Level: Enterprise

Audit:

EMC >*Microsoft Exchange->Server Configuration-><Role Name>-><Server Name>*
Right click server name Select properties
General Tab
Automatically send fatal service error report to Microsoft

Remediation:

EMC *> Microsoft Exchange->Server Configuration-><Role Name>-><Server Name>*
Right click server name Select properties
General Tab
Automatically send fatal service error report to Microsoft : unchecked

Scoring Status: Scorable

5.Edge Transport Role

5.1. Restrict Accepted Domains

Description: Accepted domains for which this Exchange will route and or relay email for.

Rationale: Exchange should only route mail for which it is both the authoritative domain and the users/mailboxes are present in the organization. Allowing external mail routing on an Edge Transport role opens the Exchange server to both spam abuse and malicious activity. Authoritative Domain is selected by default and should be kept in this configuration. For more information on alternative configurations see the Additional Resources section.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Edge Transport->Accepted Domains*
Right Click <name> Properties
(Tab) General
Authoritative Domain: Selected

Remediation:

EMC-> *Microsoft Exchange->Edge Transport->Accepted Domains*
Right Click <name> Properties
(Tab) General
Authoritative Domain: Selected

Scoring Status: Manual
Additional Resources: http://technet.microsoft.com/en-us/library/bb124423.aspx

5.2. Mail Routing Options

Description: This controls whether the SMTP connector routes its messages through simple DNS lookups (forming outbound connections to whichever host its routing table prefers) or whether it should use a Smart host

Rationale: Selecting "Smart host" means that all outbound messages through this connector will pass through a single server. This allows hardening to be applied to this single point rather than at multiple locations throughout your network. As such, the Smart host provides many of the advantages of a proxy server (and, indeed, could be the same machine). The only exception to this recommendation is when one is

configuring the external SMTP server. Since such a host would have no more outward facing computer to forward its messages to, it cannot be configured to use a Smart host, it should simply use DNS. Smart hosts may be chained together, but care must be taken that the chain is not cyclic or outbound mail will never travel beyond the Smart hosts.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Send Connectors
Select <name>
Right Click Properties
(Tab) Network
Select how to send mail with this connector

Remediation:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Send Connectors
Select <name>
Right Click Properties
(Tab) Network
Select hot to send mail with this connector
Select Route mail though the following smart hosts
Click Add
Add Smart hosts as necessary.

Scoring Status: Scorable

5.3. Audit Send Connector Address Space

Description: The send connector will only route email for a specific approved list of domains and sub-domains.

Rationale: A send connector will route mail for various sub domains allowing too general a list or other domains can result in server or relaying abuse. Manually check to ensure the send connector is only routing for approved address spaces.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Organization Configuration->Hub Transport*
(Tab) Send Connections
Right Click <name> properties
(Tab) Network
Smart host authentication
Click Change

Remediation:

EMC-> *Microsoft Exchange->Edge Transport*

Scoring Status: Manual

5.4. Enable TLS for Smart Host Basic Authentication

Description: If basic authentication must be used with smart host authentication require that TLS be enabled for the transport of the credentials. Whenever it is possible Smart host authentication should be done via Exchange Authentication or IPSec.

Rationale: Basic authentication passes credentials encoded and not encrypted across the network an attacker can trivially intercept the credentials and decode them. Requiring TLS ensures the security of the credential is maintained in transit.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange->Organization Configuration->Hub Transport*
(Tab) Send Connections
Right Click <name> properties
(Tab) Network
Smart host authentication
Click Change

Remediation:

EMC-> *Microsoft Exchange->Organization Configuration->Hub Transport*
(Tab) Send Connections
Right Click <name> properties
(Tab) Network
Smart host authentication
Click Change
Select Basic Authentication over TLS

Scoring Status: Scorable
Additional Resources: http://technet.microsoft.com/en-us/library/bb124423.aspx

5.5. Specify Block List Service Provider

Description: Configure a block list service provider to automatically update IP block lists.

Rationale: Block list providers update lists of known compromised or malicious email servers. Filtering known hostile email providers helps protect the Exchange infrastructure and users from viruses, spam, phishing, and other email based attacks

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange-> Edge Transport->IP Block List Providers*
Right Click Properties
Providers (Tab)

EMShell > *Get-IPBlockListProvidersConfig*

Remediation:

EMC-> *Microsoft Exchange-> Edge Transport-> Providers (Tab)-> Add*
Fill in Provider Name, Lookup Domain, Custom Error message
Click Ok

EMShell > *Add-IPBlockListProvider –Name <name> –LookupDomain Example.com -Enabled $true -RejectionResponse "Example response"*

Scoring Status: Manual

5.6. Specify Allow List Service Provider

Description: The allow list will white list which servers are able to communicate with the edge transport domain. This list will bypass the blacklist routing the email to its proper destination.

Rationale: Allowing specific servers as exceptions to the block rules can help performance and mail flow. However, this can also be dangerous configuring a white list provider should only be used when the integrity of the list is verified or the list is run internally. Examples of server to be white listed are other internal email servers, a branch corporate offices and/or partner. This will be organizational dependent and filters may not exist or be needed in some cases.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange-> Edge Transport->IP Block List Providers*
Right Click Properties
Providers (Tab)

EMShell > *Get-IPAllowListProvidersConfig*

Remediation:

EMC-> *Microsoft Exchange-> Edge Transport-> Providers (Tab)-> Add*
Fill in Provider Name, Lookup Domain

EMShell > *Add-IPAllowListProvider –Name <name> –LookupDomain Example.com -Enabled $true*

Scoring Status: Manual

5.7. Filter Recipients Who Are Not in Directory

Description: Filter email that is sent to a recipient that does not exist in the Exchange directory.

Rationale Exchange 2007 has a built in tar pitting functionality for recipient connections. The default tar pitting combined with other built in defense mechanisms Connection Filtering and Sender Reputation slow down account harvesting.

It should be noted that this feature can be used by external entities to determine whether a particular user exists in the Active Directory domain. By monitoring whether or not messages are filtered, an external entity could build a list of known accounts on the system. To prevent this disclosure of information, it is recommended that this feature not be employed.

Consequently, disabling this setting also disables the default Exchange 2007 tar pitting of invalid recipients allowing an attacker to send more requests to the server generating Non Delivery Reports. The NDRs allow an attacker to harvest accounts by looking at the intersection of NDRs vs. requests sent.

If this setting is disabled other actions in the Recipient Filtering should be taken to slow down or restrict the number of emails an external mailer can send to the Exchange server. For more information see the Technical resources section.

This option is considered a special security setting.

Recommendation Level: Special Security

Audit:

EMC-> *Edge Transport->Anti Spam -> Recipient Filtering ->*
Properties -> (Tab) Blocked Recipients
Block messages sent to recipients not listed in Global Address List

EMShell > *Get-RecipientFilterConfig | select identity,*

RecipientValidationEnabled

Remediation:

EMC-> *Edge Transport->Anti Spam -> Recipient Filtering -> Properties -> (Tab) Blocked Recipients*
Uncheck Block messages sent to recipients not listed in Global Address List

EMShell > *Set-RecipientFilterConfig -identity <name> -RecipientValidationEnabled 0*

Scoring Status: Manual
Technical Resources:

http://technet.microsoft.com/en-us/library/aa998898.aspx
http://technet.microsoft.com/en-us/library/bb123891.aspx

5.8. Filter Recipients

Description: Filter any email sent to the recipients on the filter list.

Rationale: If this filter is enabled, any messages sent to a filtered recipient will be dropped early in the transmission process. This filter will be organizational dependent and filters may not exist or be needed in some cases.

Recommendation Level: Enterprise

Audit:

EMC-> *Edge Transport -> Anti-Spam->Recipient Filter->Blocked Recipients -> Block the following Recipients*

EMShell > *Get-RecipientFilterConfig | select BlockedRecipients*

Remediation:

EMC-> *Edge Transport -> Anti-Spam->Recipient Filter->Blocked Recipients -> Block the following Recipients*
Add Recipients that should be filtered.

EMShell > *Set-RecipientFilterConfig -BlockedRecipients {email@domain1.com, email2@domain2.com}*

Scoring Status: Manual

5.9. Filter Senders

Description: Filter any email sent by the following addresses.

Rationale: If this filter is enabled, any messages sent by a filtered sender will be dropped early in the transmission process. This filter will be organizational dependent and filters may not exist or be needed in some cases.

Recommendation Level: Enterprise

Audit:

EMC-> *Edge Transport -> Anti-Spam->Sender Filter->Blocked Senders -> Block the following Senders*

EMShell > *Get-SenderFilterConfig | select BlockedSenders*

Remediation:

EMC-> *Edge Transport -> Anti-Spam->Senders Filter->Blocked Recipients -> Block the following Senders*
Add Senders that should be filtered.

EMShell > *Set-SenderFilterConfig -BlockedSenders {email@domain1.com, email2@domain2.com}*

Scoring Status: Manual

5.10. Filter Blank Senders

Description: Block message with a blank sender.

Rationale: Email with a blank senders is commonly spam or malicious. These emails should be dropped early in the transmission process.

Recommendation Level: Enterprise

Audit:

EMC-> *Edge Transport -> Anti-Spam -> Sender Filter->Block Senders-> Block Messages from blank senders (check)*

EMShell > *Get-SenderFilterConfig | select identity, BlankSenderBlockingEnabled*

Remediation:

EMC-> *Edge Transport -> Anti-Spam -> Sender Filter->Block Senders Check Block Messages from blank senders*

EMShell > *Set-SenderFilterConfig - BlankSenderBlockingEnabled 1*

Scoring Status: Scroable

5.11. Filter Custom Words

Description: Enable content filtering based on keywords.

Rationale: If this filter is enabled, any message containing a keyword from the list will be filtered from transit. This can help catch common words and terms in spam and malicious email or help keep sensitive information from leaving your network. This list of custom words will be organizational dependent and filters may not exist or be needed in some cases.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Anti-spam
Content Filtering
Right Click Properties
(Tab) Custom Words

EMShell > *Get-ContentFilterPhrase*

Remediation:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Anti-spam
Content Filtering
Right Click Properties
(Tab) Custom Words
Click Add
Input Filtered Words

Scoring Status: Manual

5.12. Filter Attachment extensions

Description: Enable email attachment filtering based on extensions.

Rationale: If this filter is enabled, any message containing an attachment of a particular extension will be dropped. This can help catch common viruses, trojans, or other malicious software but should not be considered a replacement for a robust

virus scanning solution. This list will be organizational dependent and additional attachment filters may not exist or be needed in some cases.

Recommendation Level: Special Security

Audit:

EMShell > *Get-AttachmentFilterEntry | list*

Remediation:

EMShell> `Add-AttachmentFilterEntry -Name <MIMEContentType> -Type ContentType`

Scoring Status: Manual
Additional Resources: http://technet.microsoft.com/en-us/library/aa997139.aspx

5.13. Configure Allowed IPs

Description: White list specific IPs for mail delivery.

Rationale: Allowing specific servers as exceptions to the block rules can help performance and mail flow. Examples of servers to be white listed are other internal email servers, a branch corporate office, or partner. This list of custom IPs will be organizational dependent and may not exist or be needed in some cases

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Edge Transport-><Select server>*
(Tab) Anti-Spam
Right-Click IP Allow List

Remediation:

EMC-> *Microsoft Exchange->Edge Transport-><Select server>*
(Tab) Anti-Spam
Right-Click IP Allow List
Add IPs as needed

Scoring Status: Manual

5.14. Enable TLS for Basic Authentication

Description: If basic authentication must be used ensure that the credentials are protected by TLS.

Rationale: Basic authentication sends user credentials across the network encoded. It is trivial to intercept these credentials and decode them revealing the users password. TLS ensures that both that the identity of the end server are known to the user and that their credentials are protected. If possible it is preferable to use TLS Mutual authentication or IPSEC

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Edge Transport->Receive Connectors -><name>*
Right Click Properties
(Tab) Authentication
Offer Basic Authentication only after starting TLS

EMShell > *Get-RecieveConnector | select identity, AuthMechanism*

Remediation:

EMC-> *Microsoft Exchange->Edge Transport->Receive Connectors -><name>*
Right Click Properties
(Tab) Authentication
Offer Basic Authentication only after starting TLS

EMShell > *Set-RecieveConnector -identity <name> -AuthMechanism BasicAuth, BasicAuthRequireTLS*

Scoring Status: Scorable

5.15. Restrict Mail Send Size

Description: Restrict the size of email that can be sent via Exchange.

Rationale: Sending email of too large a size can cause network congestion, needlessly fill disk space, and cause denial of service issues or continuous rejection for mail servers and users. Restricting the size of email sent will help ensure that mail services are not over burdened by large messages or attachments.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-TransportConfig | select identity, MaxSendSize*
EMShell > *Get-SendConnector | select identity, MaxMessageSize*

Remediation:

EMShell > *Set-TransportConfig –MaxSendSize 20Mb*
EMShell > *Set-SendConnector –MaxMessageSize 20Mb*

Scoring Status: Scorable

5.16. Restrict Mail Receive Size

Description: Restrict the size of email that can be received via Exchange.

Rationale: Receiving email of too large a size can cause local denial of service issues or continuous rejection for external mail. Restricting the size of email received will help ensure that mail services are not over burdened by large messages or attachments.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-TransportConfig | select identity, MaxReceiveSize*
EMShell > *Get-ReceiveConnector |select identity, MaxMessageSize*
EMShell > *Get-TransportServer | select identity, ExternalDsnMaxMessageAttachSize, InternalDsnMaxMessageAttachSize*

Remediation:

EMShell > *Set-TransportConfig –identity <name> –MaxReceiveSize 10MB*

EMShell > *Set-RecieveConnector –identity <name> –MaxMessageSize 10MB*

EMShell *> Set-TransportServer –identity <name> –ExternalDsnMaxMessageAttachSize 10mb*

EMShell *> Set-TransportServer –identity <name> –InternalDsnMaxMessageAttachSize 10mb*

Scoring Status: Scorable

5.17. Restrict Max Recipients

Description: Restrict the maximum number or recipients per email.

Rationale: Allowing an unlimited number of recipients can lead to a denial of services to users or system instability. It should be limited to a reasonable number.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ReceiveConnector | select identity, MaxRecipientsPerMessage*

Remediation:

EMShell > *Set-ReceiveConnector –identity <name> –MaxRecipientsPerMessage 100*

Scoring Status: Scorable

5.18. Restrict IP Range For Receive Connectors

Description: Restrict the IP ranges that can connect to a receive connector.

Rationale: Restricting the host IPs or ranges of IPs that can connect to an Edge Receive Connector adds another layer of defense to your Exchange Server. These settings will be organizational dependent and strict IP ranges may not be practical in larger environments.

Recommendation Level: Special Security

Audit:

EMC -> *Microsoft Exchange->Server Configuration->Hub Transport*
(Tab) Receive Connectors
Select Name
Right Click Properties
(Tab) Network

Remediation:

EMC -> *Microsoft Exchange->Server Configuration->Hub Transport*
(Tab) Receive Connectors
Select Name
Right Click Properties
(Tab) Network
Add Restrictions

Scoring Status: Manual

5.19. Ensure Sender Reputation is Enabled

Description: Ensure that the sender reputation setting is enabled for anti spam scoring. .

Rationale: Sender Reputation is anti-spam functionality that is enabled by default on Exchange servers disabling the sender reputation functionality can lead to excessive spam or denial of services.

Recommendation Level: Special Security

Audit:

EMShell -> `Get-SenderReputationConfig`

Remediation:

EMShell -> `Set-SenderReputationConfig -Enabled $true`

Scoring Status: Scorable

6.Mailbox Role

6.1. Restrict Email Deletion Retention

Description: Restrict deletion of email before being archived.

Rationale: It is recommended that deleted messages be retained for 7 days before being purged. This strikes a balance between the desires to be able to recover deleted messages within a reasonable amount of time without resorting to backups, while at the same time reducing the amount of storage being consumed by deleted messages.

Recommendation Level: Enterprise

Audit:

EMC-> *Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Keep deleted items for (days)

Remediation:

EMC-> *Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Keep deleted items for (days) : 7

Scoring Status: Scorable

6.2. Restrict Mailbox Deletion Retention

Description: Restrict deletion of mailboxes before being archived.

Rationale: It is recommended that deleted mailboxes be retained for 30 days before being purged. This strikes a balance between the desires to be able to recover deleted mailboxes within a reasonable amount of time without resorting to backups, while at the same time reducing the amount of storage being consumed by deleted mailboxes

Recommendation Level: Enterprise

Audit:

EMC->*Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Keep deleted mailboxes for (days)

Remediation:

EMC-> *Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Keep deleted mailboxes for (days): 30

Scoring Status: Scorable

6.3. Restrict Deletion of Mail or Mailboxes Until Archival

Description: Disable general deletion of mail and mailboxes before they have been properly archived.

Rationale: It is recommended that items are not permanently deleted until the database is backed up. This ensures the ability to recover deleted information from backups, while at the same time reducing the amount of storage being consumed by deleted items.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Do not permanently delete items until the database has been backed up

EMShell> *Get-MailboxDatabase | select identity, RetainDeletedItemsUntilBackup*

Remediation:

EMC-> *Microsoft Exchange-> Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
Tab Limits
Do not permanently delete items until the database has been backed up: Checked

EMShell> *Set-MailboxDatabase -identity <name> -RetainDeletedItemsUntilBackup $true*

Scoring Status: Scorable

6.4. Mounting of Mailbox Database at Startup

Description: Enable the mounting of the mail database

Rationale: This control should be cleared for general use. Doing this ensures that the store is mounted when Exchanges starts and thus is accessible to users. If, however, conditions require that the store be un-mounted (for example, maintenance), then this checkbox should be selected so that, should Exchange restart before maintenance is completed, it will not be inadvertently mounted in a bad state.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Sever Configuration->Mailbox Database Management*
Right Click Properties
(Tab) General
Do no mount this database at startup

EMShell > *Get-MailboxDatabase | select identity, MountAtStartup*

Remediation:

EMC-> *Microsoft Exchange->Sever Configuration->Mailbox Database Management*
Right Click Properties
(Tab) General
Do no mount this database at startup : UcChecked

EMShell > *Set-MailboxDatabase -identity <name> -MountAtStartup $true*

Scoring Status: Scorable

6.5. Ensure Proper Permissions on Mail Database

Description: Ensure proper restrictive administrative access to database is configured.

Rationale: This ACL controls the various rights to this mailbox store. Various rights include viewing the status of the store as well as changing its settings. Note that the "Full Access" right will appear to be granted to most users and groups including the "SYSTEM" group. This right is required by Exchange, does not represent a security risk, and should not be changed.

Recommendation Level: Enterprise

Scoring Status: Manual

6.6. Ensure Mailbox Database Cannot Be Overwritten

Description: Ensure the database cannot be overwritten by a system restore.

Rationale: Disabling this feature prevents the accidental loss of data due to a backup restore. To perform a database restore enable the over write feature immediately before, conduct the restore, and then disable it immediately afterwards.
.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Server Configuration->Mailbox->Database Managements*
Mailbox Database
Right Click Properties
(Tab) General
This Database can be over written by a Restore

EMShell > *Get-MailboxDatabase | select identity, AllowFileRestore*

Remediation:

EMC-> *Microsoft Exchange->Server Configuration->Mailbox->Database Managements*
Mailbox Database
Right Click Properties
(Tab) General
This Database can be over written by a Restore: Unchecked

EMShell > *Set-MailboxDatabase -identity <name> -AllowFileRestore $false*

Scoring Status: Scorable

6.7. Verify Default Mailbox Storage Limits

Description: Check that default Exchange storage limits are reasonable.

Rationale: Exchange sets default mailbox database storage limits. Ensure they are reasonable for your storage solution and expectations. The acceptable limits will differ from environment to environment the Exchange team has provided a

requirements calculator to help Exchange Administrators make these decisions. See the Technical Resources of this section for details.

Recommendation Level: Enterprise

Audit:

EMC-> *Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
(Tab) Limits
Issue warning at (KB): value
Prohibit send at (KB): value
Prohibit send and receive at (KB): value

EMShell> *Get-MailboxDatabase | select identity,*
IssueWarningQuota, ProhibitSendQuota, ProhibitSendReceiveQuota,

Remediation:

EMC-> *Server Configuration->Mailbox->Mailbox Database*
Right Click Properties
(Tab) Limits
Issue warning at (KB): new value
Prohibit send at (KB): new value
Prohibit send and receive at (KB): new value

EMShell> *Set-MailboxDatabase -identity <name> -IssueWarningQuota <value> -ProhibitSendQuota<value> -ProhibitSendReceiveQuota <value>*

Scoring Status: Not Scorable
Technical Resources:

Mailbox Server Role Storage Requirements Calculator

http://msexchangeteam.com/archive/2007/07/05/445802.aspx

6.8. Ensure Public Folder Database Cannot Be Overwritten

Description: Ensure the database cannot be overwritten by a system restore.

Rationale: Disabling this feature prevents the accidental loss of data due to a backup restore. To perform a database restore enable the over write feature immediately before, conduct the restore, and then disable it immediately afterwards.
.
Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Server Configuration->Mailbox->Database Management*
Public Folder Database
Right Click Properties
(Tab) General
This Database can be over written by a Restore

EMShell > *Get-PublicFolderDatabase | select identity, AllowFileRestore*

Remediation:

EMC-> *Microsoft Exchange->Server Configuration->Mailbox->Database Management*
Mailbox Database
Right Click Properties
(Tab) General
This Database can be over written by a Restore : Unchecked

EMShell > Public Folder Database *-identity <name> -AllowFileRestore $false*

Scoring Status: Scorable

6.9. Verify Default Public Folder Storage Limits

Description: Check that default Exchange storage limits are reasonable.

Rationale: Exchange sets default mailbox database storage limits. Ensure they are reasonable for your storage solution and expectations.

Recommendation Level: Enterprise

Audit:

EMC-> *Server Configuration->Mailbox->Public Folder Database*
Right Click Properties
(Tab) Limits
Issue warning at (KB): value
Prohibit send at (KB): value
Prohibit send and receive at (KB): value

EMShell> *Get-PublicFolderDatabase | select identity, IssueWarningQuota, ProhibitPostQuota, MaxItemSize*

Remediation:

EMC-> *Server Configuration->Mailbox-> Public Folder Database*
Right Click Properties
(Tab) Limits
Issue warning at (KB): new value

```
Prohibit send at (KB): new value
Prohibit send and receive at (KB): new value
```

EMShell> *Set-PublicFolderDatabase -identity <name> -IssueWarningQuota <value> -ProhibitPostQuote <value> -MaxItemSize <value>*

Scoring Status: Not Scorable

6.10. Audit Public Folder Client Access

Description: Audit administrative access to public folders.

Rationale: Carefully scrutinize the permissions associated with each public folder and only include the most restrictive set of permissions needed to administer the folder. Due to the wide variety of uses of public folders, no single recommendation for these settings can be given. Administrators must identify and grant required permissions on a folder-by-folder basis

Audit:

EMShell> *Get-PublicFolderClientPermission -identity "\foldername"*

Remediation:

EMShell > *Remove-PublicFolderClientPermission –identity*

Scoring Status: Not Scorable
Additional Resources: http://technet.microsoft.com/en-us/library/bb310789.aspx

6.11. Audit Public Folder Administrative Access

Description: Audit administrative access to public folders.

Rationale: Carefully scrutinize the permissions associated with each public folder and only include the most restrictive set of permissions needed to administer the folder. Due to the wide variety of uses of public folders, no single recommendation for these settings can be given. Administrators must identify and grant required permissions on a folder-by-folder basis

Audit:

EMShell> *Get-PublicFolderAdmistrativePermission -identity "\foldername"*

Remediation:

EMShell > *Remove-PublicFolderAdministrativePermission –identity*

Scoring Status: Not Scorable
Additional Resources: http://technet.microsoft.com/en-us/library/bb310789.aspx

6.12. Verify Proper Permissions on Public Folder Database

Description: Ensure proper restrictive administrative access to database is configured.

Rationale: This ACL controls the various rights to the mailbox store. Various rights include viewing the status of the store as well as changing its settings. Note that the "Full Access" right will appear to be granted to most users and groups including the "SYSTEM" group. This right is required by Exchange, does not represent a security risk, and should not be changed.

Recommendation Level: Enterprise

Scoring Status: Manual
Additional Resources: http://technet.microsoft.com/en-us/library/bb310789.aspx

6.13. Mounting of Public Folder Database at Startup

Description: Enable the mounting of the mail database

Rationale: This control should be cleared for general use. Doing this ensures that the store is mounted when Exchanges starts and thus is accessible to users. If, however, conditions require that the store be un-mounted (for example, maintenance), then this checkbox should be selected so that, should Exchange restart before maintenance is completed, it will not be inadvertently mounted in a bad state

Recommendation Level: Enterprise

Audit:

EMC *-> Microsoft Exchange->Sever Configuration->Mailbox*
Public Folder Database Management
Right Click Properties
(Tab) General
Do no mount this database at startup

EMShell > *Get-PublicFolderDatabase | select identity, MountAtStartup*

Remediation:

EMC-> *Microsoft Exchange->Sever Configuration->Mailbox*
Public Folder Database

Right Click Properties
(Tab) General
Do no mount this database at startup: UnChecked

EMShell > *Set-PublicFolderDatabase -identity <name> -MountAtStartup $true*

Scoring Status: Scorable

6.14. Restrict Deletion of Mail or Mailboxes Until Archival

Description: Restrict items from being permanently deleted from Public Folders until they are backed up.

Rationale: It is recommended that items are not permanently deleted until the database is backed up. This strikes a balance between the desires to be able to recover deleted messages within a reasonable amount of time without resorting to backups, while at the same time reducing the amount of storage being consumed by deleted messages

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Server Configuration->Mailbox ->PublicFolder*
Right Click Properties
Tab Limits
Do not permanently delete items until the database has been backed up

EMShell> *Get-PublicFolder| select identity, RetainDeletedItemsUntilBackup*

Remediation:

EMC*-> Microsoft Exchange-> Server Configuration->Mailbox->PublicFolder*
Right Click Properties
Tab Limits
Do not permanently delete items until the database has been backed up : Checked

EMShell> *Set-PublicFolderxDatabase -identity <name> -RetainDeletedItemsUntilBackup $true*

Scoring Status: Scorable

6.15. Restrict Mail Send Size

Description: Restrict the size of email that can be sent via Exchange per mailbox, contact or group.

Rationale: Sending email of too large a size can cause local denial of service issues or continuous rejection for external mail servers. The list of mailboxes, contacts, and groups which have been given exceptions to the higher level transport and hug restrictions should be audited and corrected where necessary.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-Mailbox | select identity, MaxSendSize*
EMShell > *Get-MailContact | Select identity, MaxSendSize*
EMShell > *Get-DistributionGroup | Select identity, MaxSendSize*

Remediation:

EMShell > *Set-Mailbox -identity <name> -MaxSendSize 10Mb*
EMShell > *Set-MailContact -identity <name> -MaxSendSize 10Mb*
EMShell > *Set-DistributionGroup -identity <name> -MaxSendSize 10mb*

Scoring Status: Scorable

6.16. Restrict Mail Receive Size

Description: Restrict the size of email that can be received via Exchange.

Rationale: Receiving email of too large a size can cause local denial of service issues or continuous rejection for external mail servers. The list of mailboxes, contacts, and groups which have been given exceptions to the higher level transport and hug restrictions should be audited and corrected where necessary.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-Mailbox | select identity,MaxReceiveSize*
EMShell > *Get-MailContact | select -identity, MaxReceiveSize*
EMShell > *Get-DistributionGroup | Select identity, MaxReceiveSize*

Remediation:

EMShell > *Set-Mailbox –identity <name> -MaxReceiveSize 10Mb*
EMShell > *Set-MailContact –identity <name> -MaxReceiveSize 10Mb*
EMShell > *Set-DistributionGroup -identity <name> -MaxReceiveSize 10Mb*

Scoring Status: Scorable

6.17. Restrict Max Recipients

Description: Restrict the maximum number or recipients per email.

Rationale: Allowing an unlimited number of recipients can lead to a denial of services to users or system instability. It should be limited to a reasonable number.

Recommendation Level: Enterprise

Audit:
EMShell > *Get-Mailbox | select identity, RecipientLimits*

Remediation:
EMShell > *Set-Mailbox -RecipientLimits 2000*

Scoring Status: Scorable

6.18. Audit Mailbox Spam Bypass Settings

Description: Audit mailboxes that have opted to bypass spam filtering.

Rationale: When a mailbox has the AntispamBypassEnabled option set to false all spam filtering is skipped for that mailbox. This can cause inbound spam to go unchecked which can lead to the possible denial or services or user experience problems. It may be necessary in some cases to accept all spam for a particular mailbox for instance a catchall address; however this option is disabled by default and should be left as such.

Recommendation Level: Enterprise

Audit:
EMShell > *Get-Mailbox | select identity, AntispamBypassEnabled*

Remediation:

EMShell > *Set-Mailbox -identity <name> -AntispamBypassEnabled $false*

Scoring Status: Manual

6.19. AntiSpam Updates

Description: Automatic downloading of anti spam content filter updates.

Rationale: Microsoft provides biweekly anti spam content filter updates via the Microsoft Update service. It is recommended to evaluate the IT environment that Exchange is deployed before enabling automatic updates. If different policies, practices or management frameworks are currently in place then this setting can be left as default.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-AntiSpameUpdates*

Remediation:

EMShell > *Enable-AntispamUpdates -SpamSignatureUpdatesEnabled $true -UpdateMode Automatic*

Scoring Status: Scorable

6.20. Zero out Deleted Database pages

Description: Zero out old database pages on deletion or restoration from a backup.

Rationale: This feature controls how deleted memory is handled. If this feature is not enabled, when a mail message or public folder posting is deleted (this is to say, all references to it are removed and the management program actually deletes the message) the operating system simply marks the memory that was previously used to store the message as available for use. Eventually, this memory may be utilized to store additional information. However, until this time, the message will still be present on the disk and certain utilities will be able to recover some or the message.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-StorageGroup | select Identity, ZeroDatabasePages*

Remediation:

EMShell > *Set-StorageGroup -Identity <name> -ZeroDatabasePages $true*

Scoring Status: Scorable

7. Hub Transport Role

7.1. Restrict Accepted Domains

Description: Restrict the list of accepted domains for which this transport will route email.

Rationale: Exchange should only route mail for which it is the authoritative domain and the users/mailboxes are present in the organization. Allowing external mail routing on an Edge Transport role opens the Exchange server to both spam abuse and malicious activity. Authoritative Domain is selected by default and should be kept in this configuration unless absolutely necessary to configure for a specific edge case. For more information on alternative configurations see the Additional Resources section.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Edge Transport->Accepted Domains*
Right Click <name> Properties
(Tab) General
Authoritative Domain: Selected

Remediation:

EMC *Microsoft Exchange->Edge Transport->Accepted Domains*
Right Click <name> Properties
(Tab) General
Authoritative Domain: Selected

Scoring Status: Scorable
Additional Resources: http://technet.microsoft.com/en-us/library/bb124423.aspx

7.2. Mail Routing Options

Description: This controls whether the connector routes its messages through simple DNS lookups (forming outbound connections to whichever host its routing table prefers) or whether it should use a Smart host

Rationale: Selecting "Smart host" means that all outbound messages through this connector will pass through a single server. This allows hardening to be applied to this single point rather than at multiple locations throughout your network. As such, the Smart host provides many of the advantages of a proxy server (and, indeed, could be the same machine). If you organization has smart hosts deployed select smart host.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Send Connectors
Select <name>
Right Click Properties
(Tab) Network
Select how to send mail with this connector

Remediation:

EMC-> *Microsoft Exchange->Edge Transport*
(Tab) Send Connectors
Select <name>
Right Click Properties
(Tab) Network
Select hot to send mail with this connector
Select Route mail though the following smart hosts
Click Add
Add Smart hosts as necessary.

Scoring Status: Not Scorable

7.3. Audit DNS Lookup Servers

Description: Restrict the DNS servers the receive connector will use to make routing decisions.

Rationale: Domain name servers are often high value targets to attackers. Ensure that the DNS server list used to route mail is a trusted and known list of internal DNS hosts.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Server Configuration->Hub Transport->*
(Tab) Receive Connectors
Right Click Properties
External DNS Lookups or Internal DNS Lookups

Remediation:

EMC->
Microsoft Exchange->Server Configuration->Hub Transport->
(Tab) Receive Connectors
Right Click Properties
External DNS Lookups or Internal DNS Lookups
Select Use these DNS servers

Add specific DNS servers

Scoring Status: Manual

7.4. Enable TLS for Basic Authentication

Description: If basic authentication must be used ensure that the credentials are protected by TLS.

Rationale: Basic authentication sends user credentials across the network encoded. It is trivial to intercept these credentials and decode them revealing the users password. TLS ensures that both that the identity of the end server are known to the user and that their credentials are protected. If possible it is preferable to use TLS Mutual authentication or IPSEC

Recommendation Level: Enterprise

Audit:

EMC-> Microsoft Exchange->Edge Transport->Receive Connectors -><name>
Right Click Properties
(Tab) Authentication
Offer Basic Authentication only after starting TLS

EMShell > *Get-RecieveConnector | select identity, AuthMechanism*

Remediation:

EMC-> *Microsoft Exchange->Edge Transport->Receive Connectors -><name>*
Right Click Properties
(Tab) Authentication
Offer Basic Authentication only after starting TLS

EMShell > *Set-RecieveConnector -identity <name> -AuthMechanism BasicAuth, BasicAuthRequireTLS*

Scoring Status:

7.5. Restrict Out of Office Responses

Description: Disable out of office responses to internal users only.
Rationale: Out of office auto responders can leak sensitive information such as internal numbers, schedules, project names or organization trees. They should be limited to internal users only except on absolutely necessary.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Organization Configuration->Hub Transport-> Remote Domains->General Tab*

Heading Out-of-office message types delivered to this remote domain

EMShell > *Get-remotedomain | select identity, AllowedOOFType*

Remediation:

EMC->*Microsoft Exchange -> Organization Configuration -> Hub Transport -> Remote Domains -> General Tab*

Heading Out-of-office message types delivered to this remote domain. Select Allow None.

EMShell > *Set-remoteDomain -Identity default -AllowedOOFType None*

Scoring Status: Scorable

7.6. Restrict Mail Send Size

Description: Restrict the size of email that can be sent via Exchange.

Rationale: Sending email of too large a size can cause local denial of service issues or continuous rejection for external mail servers.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-TransportConfig | select identity, MaxSendSize*
EMShell > *Get-SendConnector | select identity, MaxMessageSize*

Remediation:

EMShell > *Set-TransportConfig -MaxSendSize 10Mb*
EMShell > *Set-SendConnector -MaxMessageSize 10Mb*

Scoring Status: Scorable

7.7. Restrict Mail Receive Size

Description: Restrict the size of email that can be received via Exchange.

Rationale: Receiving email of too large a size can cause local denial of service issues or continuous rejection for external mail servers.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-TransportConfig | select identity, MaxReceiveSize*
EMShell > *Get-ReceiveConnector |select identity, MaxMessageSize*
EMShell > *Get-TransportServer | select identity, ExternalDsnMaxMessageAttachSize, InternalDsnMaxMessageAttachSize*

Remediation:

EMShell > *Set-TransportConfig –identity <name> –MaxReceiveSize 10MB*

EMShell > *Set-RecieveConnector –identity <name> –MaxMessageSize 10MB*

EMShell *> Set-TransportServer –identity <name> -ExternalDsnMaxMessageAttachSize 10mb*

EMShell *> Set-TransportServer –identity <name> -InternalDsnMaxMessageAttachSize 10mb*

Scoring Status: Scorable

7.8. Restrict Max Recipients

Description: Restrict the maximum number or recipients per email.

Rationale: Allowing an unlimited number of recipients can lead to a denial of services to users or system instability. It should be limited to a reasonable number.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ReceiveConnector | select identity, MaxRecipientsPerMessage*

Remediation:

EMShell > *Set-ReceiveConnector - –MaxRecipientsPerMessage 2000*

Scoring Status: Scorable

7.9. Restrict IP Range For Receive Connectors

Description: Restrict the IP ranges that can connect to a receive connector.

Rationale: Restricting the host IPs or ranges of IPs that can connect to a Hub Receive Connector adds another layer of defense to your Exchange Server. This will be organizational dependent and strict IP ranges may not be particle in larger environments.

Recommendation Level: Special Security

Audit:

EMC -> *Microsoft Exchange -> Server Configuration -> Hub Transport*
(Tab) Receive Connectors
Select Name
Right Click Properties
(Tab) Network

Remediation:

EMC -> *Microsoft Exchange -> Server Configuration -> Hub Transport*
(Tab) Receive Connectors
Select Name
Right Click Properties
(Tab) Network
Add Restrictions

Scoring Status: Manual

8. Client Access Server Role

8.1. Require SSL for POP3

Description: If POP3 cannot be disabled require SSL be used for authentication and access.

Rationale: POP3 transmits credentials and sensitive information unencrypted across the network. Enabling SSL adds a layer of encryption to protect the information and allow the client to verify the server's address.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-Popsettings | select identity, LoginType*

Remediation:

EMShell > *Set-Popsettings –identity <name> -LoginType SecureLogin*

Scoring Status: Scorable

8.2. Limit number of POP3 connections

Description: If POP3 cannot be disabled require SSL be used for authentication and access.

Rationale: Failure to limit the number of IMAP connections, or setting a limit that is too high may result in excessive network congestion and prevent users from accessing Exchange's services.

.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-Popsettings | select identity, MaxConnections*

Remediation:

EMShell > *Set-Popsettings –identity <name> -MaxConnections 500*

Scoring Status: Scorable

8.3. Enforce Pop3 Connection Timeouts

Description: Drop Pop3 connection after set timeout duration.

Rationale: This controls the number of minutes an idle connection will be maintained by the server before it is dropped. This can be used to help limit the number of simultaneous connections the serve must support.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-PopSettings | select identity, AuthenticatedConnectionTimeout, PreAuthenticatedConnectionTimeout*

Remediation:

EMShell > *Set-PopSettings –identity <name> - AuthenticatedConnectionTimeout 00:20:00 – PreAuthenticatedConnectionTimeout 00:01:00*

Scoring Status: Scorable

8.4. Require SSL for IMAP

Description: If IMAP cannot be disabled require SSL be used for authentication and access.

Rationale: IMAP transmits credentials and sensitive information unencrypted across the network. Enabling SSL adds a layer of encryption to protect the information and allow the client to verify the server's address.

.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ImapSettings | select identity, LoginType*

Remediation:

EMShell *> Set-ImapSettings –identity <name> –LoginType SecureLogin*

Scoring Status: Scorable

8.5. Enable IMAP connection timeout

Description: Drop IMAP connection after set timeout duration.

Rationale: This controls the number of minutes an idle connection will be maintained by the server before it is dropped. This can be used to help limit the number of simultaneous connections the serve must support.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ImapSettings | select identity, AuthenticatedConnectionTimeout, PreAuthenticatedConnectionTimeout*

Remediation:

EMShell > *Set-ImapSettings –identity <name> -AuthenticatedConnectionTimeout 00:20:00 –PreAuthenticatedConnectionTimeout 00:01:00*

Scoring Status: Scorable

8.6. Restrict number of IMAP connections

Description: If IMAP cannot be disabled require a maximum number of connections.

Rationale: Failure to limit the number of IMAP connections, or setting a limit that is too high may result in excessive network congestion and prevent users from accessing Exchange's services.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ImapSettings | select identity, MaxConnections*

Remediation:

EMShell > *Set-ImapSettings –identity <name> –MaxConnections 500*

Scoring Status: Scorable

8.7. Remove Legacy Web Applications

Description: Remove legacy web support if legacy mailbox support is not needed.

Rationale: If not necessary for legacy support of Exchange 2000 and 2003 removal of these web applications will help reduce the Exchange attack surface. Please note once deleted manual reentry will be necessary to recover this functionality. Only perform this step if you are sure you do not need to support legacy services. If your

organization may need legacy services in the future choose to disable or block the applications instead.

Recommendation Level: Enterprise

Audit:

IIS> <server name>-> Web Sites->Default Web Site-> {Exchange, Exchweb, Exadmin, Public}

EMShell > *Get-OwaVirtualDirectory*

Remediation Deletion:

IIS> Right Click and Delete Exchange, Exchweb, Exadmin, Public

EMShell >

```
Remove-OwaVirtualDirectory -Identity "Exchange (Default Web
Site)"
Remove-OwaVirtualDirectory -Identity "Exchweb (Default Web Site)"
Remove-OwaVirtualDirectory -Identity "Exadmin (Default Web Site)"
Remove-OwaVirtualDirectory -Identity "Public (Default Web Site)"
```

Scoring Status: Scorable

8.8. Restrict Web Authentication Methods

Description: Disable unneeded authentication methods for Exchange web applications.

Rationale: For web services and applications that cannot be disabled and removed from IIS ensure reasonable authentication methods are selected. These include Autodiscover, Exchange, EWS, Exadmin, Exchweb, Microsoft-Exchange-ActiveSync, OAB, OWA, Public, and UnifiedMessaging.

Recommendation Level: Enterprise

Audit:

IIS> *<Server Name>->Web Sites-><Site Name>*
Right Click Properties
Tab Directory Security
Authentication and access control

Remediation:

IIS> *<Server Name> - >Web Sites -> <Site Name>*
Right Click Properties
Tab Directory Security

Authentication and access control

X = Enabled

	Auto	Exco	EWS	ExAd	Exchweb	Active Sync	OAB	OWA	Public	UM
Integ	X	X	X	X	X				X	X
Digest										
Basic		X				X (only if not using certs)	X	X	X	
Passport										

Scoring Status: Scorable

8.9. Require SSL for Web Applications

Description: Enable and require SSL for all web application in Exchange.

Rationale: For web services and applications that cannot be disabled and removed from IIS require that all traffic be secure to the end user. These include Autodiscover, Exchange, EWS, Exadmin, Exchweb, Microsoft-Exchange-ActiveSync, OAB, OWA, Public, and UnifiedMessaging.

Recommendation Level: Enterprise

Audit:

IIS > *<Server Name>->Web Sites->Default Web Site*
Right Click Properties
Tab Directory Security
Secure Communications
Click Edit

Remediation:

IIS > *Click Server Certificate*
Follow wizard steps to create a secure certificate

Secure Communications
Click Edit
Require Secure Channel SSL: checked
Require 128-bit encryption: checked

Scoring Status: Scorable

8.10. Disable Web Anonymous Access

Description: Require authenticated access to all web apps.

Rationale: For web services and application that cannot be disabled and removed from IIS require only authenticated access. These include Autodiscover, Exchange, EWS, Exadmin, Exchweb, Microsoft-Exchange-ActiveSync, OAB, OWA, Public, and UnifiedMessaging. This is the default setting for Exchange 2007.

Recommendation Level: Enterprise

Audit:

IIS><*Server Name> -> Web Sites -> <Site Name>*
Right Click Properties
Tab Directory Security
Authentication and access control
Click Edit
Enable anonymous access

Remediation:

IIS><*Server Name> -> Web Sites -> <Site Name>*
Right Click Properties
Tab Directory Security
Authentication and access control
Click Edit
Enable anonymous access: Unchecked

Scoring Status: Scorable

8.11. Enable Logging for Default Website

Description: Enable logging of web connections and requests to the default website.

Rationale: Logging should be enabled for the default website to provide an audit trail of attempted connections to this virtual server. In the case of an attack on the IIS server, these logs could contain useful details regarding the time and nature of the attack. Due to the size of log files, the files should be regularly copied to external storage and deleted from the server to conserve memory. Log files should be retained for at least one month. The format of the log files is largely a matter of preference for the administrator.

Recommendation Level:

Audit:

IIS-> *<Server Name> -> Web Sites -> Default Web Site*
Right Click Properties
Tab Website
Enable Logging

Remediation:

IIS-> *<Server Name> -> Web Sites -> Default Web Site*
Right Click Properties
Tab Website
Enable Logging: Checked

Scoring Status: Scorable

8.12. Enable Policy for ActiveSync

Description: Create and assign a policy for the ActiveSync service.

Rationale: Mobile devices are prone to theft, loss, and attack. Enabling and configuring an ActiveSync policy will help reduce the risk to the Exchange infrastructure if a mobile device goes missing. Configuring an ActiveSync policy will also help to ensure that mobile devices are in sync with corporate security policy.

Recommendation Level: Enterprise

Audit:

EMC*-> Microsoft Exchange-> Organization Configuration -> Client Access -> Exchange ActiveSync Mailbox Policies*

EMShell > *Get-ActiveSyncMailboxPolicy*

Remediation:

EMC-> *Microsoft Exchange -> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click

New Exchange ActiveSyncMailbox Policy

Enter Name : <name>
Allow NonProvisionable Devices: Unchecked
Allow Attachments to be downloaded to device : Checked
Require Password: Checked
Require alphanumeric password: Checked
Enable password recovery: Checked
Require Encryption on device: Checked
Allow simple password: Unchecked
Minimum Password Length: Checked, 8
Time without user input before password must be re-entered: 15
Password Expiration: Checked, 90
Enforce Password History: 5

Right Click on <name> Policy

WSS/UNC Access
Windows File Shares: Unchecked
Windows SharePoint Services: Unchecked

Finally assign the policy to relevant users.

EMShell > *New-ActiveSyncMailboxPolicy -name* ***<name>***

Set-ActiveSyncMailboxPolicy -identity ***<name>*** *-AllowNonProvisionableDevices $false -AllowSimpleDevicePassword $false -AlphanumericDevicePasswordRequired $true -AttachmentsEnabled $true -DeviceEncryptionEnabled $true -DevicePasswordEnabled $true -DevicePasswordExpiration 90 -DevicePasswordHistory 5 -DevicePolicyRefreshInterval 24.00:00:00 -MaxAttachmentSize 3MB -WSSAccessEnabled $false -UNCAccessEnabled $false -MinDevicePasswordLength 8 -MaxDevicePasswordFailedAttempts 10 -MaxInactivityTimeDeviceLock 00:15:00*

To assign the policy to a single user

*Set-CASMailbox <user> -ActiveSyncMailboxPolicy(Get-ActiveSyncMailboxPolicy "****<name>****").Identity*

To assign the policy to all users

*Get-Mailbox | Set-CASMailbox -ActiveSyncMailboxPolicy(Get-ActiveSyncMailboxPolicy "****<name>****").Identity*

Scoring Status: Scorable

8.13. Forbid ActiveSync NonProvisionable Devices

Description: Disable active sync for devices that do not accept security policy updates from the Exchange server.

Rationale: Devices which connect to the Exchange infrastructure should adhere to a uniform security policy and configuration. Allowing devices which are not able to be provisioned can put your infrastructure at unnecessary risk.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*
Right Click on Policy, Select properties

Allow NonProvisionable Devices

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, AllowNonProvisionableDevices*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*
Right Click on Policy, Select properties

Allow NonProvisionable Devices : Unchecked

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -AllowNonProvisionableDevices $false*

Scoring Status: Scorable

8.14. Forbid ActiveSync Simple Device Password

Description: Require a strong password from mobile devices to be entered before unlocking and authenticating.

Rationale: Mobile devices are far reaching extensions to an IT infrastructure. While acting as remote clients they should adhere and conform to the same standards as devices on your local network. Requiring password complexity is a recommended industry practice and should be followed for mobile devices as well.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange -> Organization Configuration -> Client Access -> Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Allow simple password

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, AllowSimpleDevicePassword*

Remediation:

EMC-> *Microsoft Exchange -> Organization Configuration -> Client Access -> Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties

Password Tab
Allow simple password: Unchecked

EMShell > *Set-ActiveSyncMailboxPolicy –identity <name> -AllowSimpleDevicePassword $false*

Scoring Status: Scorable

8.15. Disable ActiveSync WSS/UNC Access

Description: If not needed disable Windows file share and SharePoint access.

Rationale: WSS and UNC provided file share access for mobile devices. If the functionality is not needed by mobile users then it should be disabled to reduced Exchanges attack surface and exposure to internal file shares.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange -> Organization Configuration -> Client Access -> Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
General Tab
WSS/UNC Access
Windows File Shares
Windows SharePoint Services

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, WSSAccessEnabled,UNCAccessEnabled*

Remediation:

EMC *-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on <name> Policy, Select Properties
General Tab
WSS/UNC Access

Windows File Shares: Unchecked
Windows SharePoint Services: Unchecked

EMShell > *Set-ActiveSyncMailboxPolicy –identity <name> -WSSAccessEnabled $false –UNCAccessEnabled $false*

Scoring Status: Scorable

8.16. Require ActiveSync Password

Description: Require that mobile devices utilize a password to unlock.

Rationale: A password should be necessary to unlock the mobile device this will help secure and sensitive information that is stored on the device it in the event of loss or theft.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require Password

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, DevicePasswordEnabled*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require Password: Checked

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordEnabled $true*

Scoring Status: Scorable

8.17. Require ActiveSync Alphanumeric Password

Description: Require that the active sync password be an alphanumeric password instead of a simple numeric password.

Rationale: Simple number passwords are trivial to brute force and lend themselves to both shortness and reuse. To ensure proper password resistance from brute force attacks and alphanumeric password is required.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require alphanumeric password

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, AlphanumericDevicePasswordRequired*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require alphanumeric password: Checked

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -AlphanumericDevicePasswordRequired $true*

Scoring Status: Scorable

8.18. Require ActiveSync Minimum Password Length

Description: Require an active sync password length of at least 8 characters.

Rationale: Short passwords less than 8 characters are trivial to brute force requiring a longer password helps ensure the security of the device and account.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange -> Organization Configuration -> Client Access -> Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Minimum password length

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, MinDevicePasswordLength*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Minimum password length : Checked, 8

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -MinDevicePasswordLength 8*

Scoring Status: Scorable

8.19. Require ActiveSync Password Expiration

Description: Require ActiveSync passwords to expire every 60 days.

Rationale: The longer a password is used the less secure it becomes. Require users to change passwords every 60 days or what is in sync with corporate security policies.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Password Expiration

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, DevicePasswordExpiration*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Password Expiration : Checked, 60

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordExpiration 60*

Scoring Status: Scorable

8.20. Require ActiveSync Password History

Description: Store a password history of 5 passwords for ActiveSync.

Rationale: Storing password history ensures that passwords are not reused within a reasonable period of time.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Enforce password history

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, DevicePasswordHistory*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Enforce password history: 5

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -DevicePasswordHistory 5*

Scoring Status: Scorable

8.21. Require ActiveSync Encryption

Description: For Windows Mobile 6.0 Devices this controls the storage card encryption on the device

Rationale: Storage cards often hold downloaded attachments, contact lists, and other sensitive company information. Requiring ActiveSync encryption helps to minimize the risk in the case of a lost device or storage card. However, only Windows Mobile 6.0 devices currently support this option.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require encryption on device

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, DeviceEncryptionEnabled*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Require encryption on device: Checked

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -DeviceEncryptionEnabled $true*

Scoring Status: Scorable

8.22. Restrict ActiveSync Attachment Size

Description: Restrict the attachment size that can be downloaded or sent from a mobile device.

Rationale: Allowing attachments that are too large can quickly fill up the storage space on a mobile device. Limiting the size of attachments sent helps ensure the reliability and stability of such devices.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
General Tab
Maximum Attachment Size

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, MaxAttachmentSize*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client*

Access->Exchange ActiveSync Mailbox Policies

Right Click on Policy, Select properties
General Tab
Maximum Attachment Size: 3000

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -MaxAttachmentSize 3Mb*

Scoring Status: Scorable

8.23. Require ActiveSync Policy Refresh

Description: Require that the active sync policy be refreshed on the device once every 24 hours.

Rationale: A devices security policy or settings may be replaced, wiped, or reconfigured. Pushing the policy to a mobile device every 24 hours ensures the device's policy is synced with the Exchange server and the corporate security policy.

Recommendation Level: Enterprise

Audit:

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, DevicePolicyRefreshInterval*

Remediation:

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -DevicePolicyRefreshInterval 24.00:00:00*

Scoring Status: Scorable

8.24. Restrict ActiveSync Maximum Password Attempts

Description: Restrict the maximum number of password attempts a user can make to authenticate to a device.

Rationale: Mobile devices are at high risk to both loss and theft. Setting a password attempt limit can help minimize the risk of user credentials, sensitive information such as email, documents, attachments, and contacts stored on the device.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Number of attempts allowed

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, MaxDevicePasswordFailedAttempts*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
General Tab
Number of attempts allowed: 8

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -MaxDevicePasswordFailedAttempts 8*

Scoring Status: Scorable

8.25. Require ActiveSync Certificate Based Authentication

Description: Enable and use ActiveSync certificate authentication.

Rationale: Client certificate based authentication provides mutual identification and authorization ensuring both end points of the ActiveSync communication are trusted entities.

Recommendation Level: Special Security

Audit:

EMC-> *Server Configuration->Client Access*
Exchange Active Sync
Microsoft-Server-ActiveSync
Right Click Select Properties
Authentication (tab)
Select

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, ClientCertAuth*

Remediation:

EMC-> *Server Configuration->Client Access*
Exchange Active Sync
Microsoft-Server-ActiveSync

Right Click Select Properties
Authentication (tab)
Select Require Client Certificates
Deselect BasicAuthEnabled
Click Ok

EMShell > *Set-ActiveSyncVirtualDirectory -Identity :"ExchSrvr\Microsoft-Server-ActiveSync (Default Web Site)" -BasicAuthEnabled:$false -ClientCertAuth:"Required"*

Scoring Status: Scorable
Additional Resources: http://technet.microsoft.com/en-us/library/aa997575.aspx

8.26. Require ActiveSync Inactivity Lockout Time

Description: Require that the ActiveSync device lock itself after a period of inactivity.

Rationale: Mobile devices are often left unattended or lost in public places. Requiring the device to lock after 15 minutes minimizes the window for opportunity of attack should a device be tampered with, lost, or stolen.

Recommendation Level: Enterprise

Audit:

EMC*-> Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
Password Tab
Time without user input before password must be re-entered

EMShell > *Get-ActiveSyncMailboxPolicy | Select identity, MaxInactivityTimeDeviceLock*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Client Access->Exchange ActiveSync Mailbox Policies*

Right Click on Policy, Select properties
General Tab
Time without user input before password must be re-entered : 15

EMShell > *Set-ActiveSyncMailboxPolicy -identity <name> -MaxInactivityTimeDeviceLock 00:15:00*

Scoring Status: Scorable

8.27. Disable Outlook Anywhere

Description: If not required disable Outlook Anywhere.

Rationale: If Outlook Anywhere access is not required then disable it to reduce Exchange's attack surface.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange->Server Configuration->Client Access-> <Name>*
Outlook Anywhere Enabled

EMShell > *Get-ClientAccessServer | select identity, OutlookAnywhereEnabled*

Remediation:

EMC-> *Microsoft Exchange->Server Configuration->Client Access-><Name>*

Right Click Disable Outlook Anywhere Policies

EMShell > *Set-ClientAccessServer -identity <name> -OutlookAnywhereEnabled $false*

Scoring Status: Scorable

9. Unified Messaging Role

9.1. Disable Faxing

Description: Unless required disable the ability for users to receive faxes.

Rationale: If the faxing service is not required then disable this feature to reduce the Exchange server attack surface.

Recommendation Level: Special Security

Audit:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) General
Allow users to receive faxes

EMShell > `Get-UMDialPlan | select identity, FaxEnabled`

Remediation:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) General
Allow users to receive faxes : Unchecked

EMShell > `Set-UMDialPlan -identity <name> -FaxEnabled $true`

Scoring Status: Scorable

9.2. Require PIN length

Description: Require user mailboxes have a minimum PIN length to authenticate access.

Rationale: A longer PIN lengthens the amount of time required to brute force a user's mailbox authentication, this coupled with a reasonable lockout policy makes brute forcing a users PIN a nontrivial task.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Mailbox Policies
Right Click <name> Properties
(Tab) PIN Policies
Minimum PIN length

EMShell > *Get-UMMailboxPolicy | select identity, MinPINLength*

Remediation:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Mailbox Policies
Right Click <name> Properties
(Tab) PIN Policies
Minimum PIN length : 6

EMShell > *Set-UMMailboxPolicy –identity <name> –MinPINLength 6*

Scoring Status: Scorable

9.3. Require PIN complexity

Description: Require that PIN be complex.

Rationale: When brute forcing or guessing PINs, common combinations are typically tried early in the guessing process. PINs should meet minimum requirements for complexity. Turning off allow common patterns will keep users from choosing simple repeating and sequential PINs. (Ex. 123456, 010101, 666666)

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Mailbox Policies
Right Click <name> Properties
(Tab) PIN Policies
Allow common patterns in PIN

EMShell > *Get-UMMailboxPolicy | select identity,*
AllowCommonPatterns

Remediation:

EMC-> *Microsoft Exchange->Unified Messaging*
(Tab) UM Mailbox Policies
Right Click <name> Properties
(Tab) PIN Policies
Allow common patterns in PIN: Unchecked

EMShell > *Set-UMMailboxPolicy -identity <name> -AllowCommonPatterns $false*

Scoring Status: Manual

R Restrict Allowed in-country/region groups

9.4. Restrict Allowed In-Country/Region Groups

Description: Restrict the country regions a particular dial plan can place calls to.

Rationale: Restricting the outbound dial plan can help reduce the risk of accidental or malicious long distance calls.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Organization Configuration->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) Dialing Rule Groups
In-Country/Region Rule Groups

EMShell > *Set-UMDialPlan | select identity, ConfiguredInCountryorRegionGroup*

Remediation:

EMC-> *Microsoft Exchange->Organization Configuration->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) Dialing Rule Groups
In-Country/Region Rule Groups
Click Add

EMShell > *Set-UMDialPlan -identity <name> -ConfiguredInCountryorRegionGroups "Local,9XXXXXXX, 9XXXXXXX,local"*

Scoring Status: Manual

9.5. Restrict Allowed International Groups

Description: Restrict the allowed international extensions a particular

Rationale: Restricting the outbound dial plan can help reduce the risk of accidental or malicious long distance calls.

Recommendation Level: Enterprise

Audit:

EMC-> *Microsoft Exchange->Organization Configuration->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) Dialing Rule Groups
International Rule Groups

EMShell > *Set-UMDialPlan | select identity, ConfiguredInternationalGroups*

Remediation:

EMC-> *Microsoft Exchange-> Organization Configuration->Unified Messaging*
(Tab) UM Dial Plan
Right Click <name> Properties
(Tab) Dialing Rule Groups
International Rule Groups
Click Add

EMShell > *Set-UMDialPlan -identity <name> -ConfiguredInCountryorRegionGroups "Local,9XXXXXXX, 9XXXXXXX,local"*

Scoring Status: Manual

9.6. VoIP IPSec

Description: Use TLS or IPSec between your Unified Messaging server and VoIP/PBX gateway to secure communications.

Rationale: VoIP traffic is inherently insecure and sent across a network unencrypted. This allows the intercept or altering of VoIP communications by a malicious user. To increase the privacy and security of calls utilize TLS or IPSec tunnel between the Unified Messaging server and PBX. This however requires that the VoIP gateway supports TLS or IPSec.

Recommendation Level: Enterprise

Audit:
Remediation:

Enable IPSec between the Messaging server and VoIP gateway.

Scoring Status: Manual
Additional Resources:
http://technet.microsoft.com/en-us/library/bb124092.aspx
http://support.microsoft.com/?kbid=914841
http://technet2.microsoft.com/windowsserver/en/library/4f05f853-2eed-4ff8-b16f-e6228c050a6b1033.mspx?mfr=true

10. Post Installation

10.1. Configure Monitoring

Description: Monitor the basic health of Exchange.

Rationale: If a monitoring package like Operations Manager is not installed then monitoring should be configured to watch the basic health of Exchange. It is recommended to monitor CPU, memory, and logical disk utilization. Add other monitors as needed.

Recommendation Level: Enterprise

Remediation:

Microsoft Exchange->Toolbox
Click Performance Monitor

Exchange Server Performance Monitor

Console Root->Alerts
Right click New Alert Settings

Name CPU
Counter %Processor Time

Name Memory
Counter Free Memory Mb

Name Disk
Counter %Free Space

Scoring Status: Manual

10.2. Install Anti-Virus Software

Description: Install anti-virus software to scan for viruses and other malicious software embedded in email.

Rationale: Email is a common transport for viruses and other malicious software. Attackers will often try to ruse users into opening malicious attachments as a starting point for a larger attack on an infrastructure. Antivirus software helps to users from viruses and worm outbreaks that spread via email. Installation of an antivirus solution is critical to protecting infrastructure and highly recommended.

Recommendation Level: Enterprise
Audit: N/A
Remediation: N/A
Scoring Status: Manual

Additional Resources: http://technet.microsoft.com/en-us/library/bb201667.aspx

10.3. Security Configuration Wizard

Description: Run the Microsoft Security Configuration Wizard to lock down the server Exchange has been installed on.

Rationale: The Security Configuration Wizard will create a security policy and reduce the attack surface of both the Windows server and Exchange roles and services.

Recommendation Level: Enterprise

Remediation:
Start->Control Panel->Add Remove Programs
Click Add/Remove Windows Components
Select Security Configuration Wizard
Click next
Click Finish

Start->All Programs->Administrative Tools->Security Configuration Wizard

Scoring Status: Manual

Additional Resources:
http://technet.microsoft.com/en-us/library/aa998208.aspx

11. Appendix A: Change History

Date	Version	Changes for this version
December, 2007	1.0.0	Public Release
July 2nd, 2010	1.1.0	• Resolved inconsistency between summary table and detail section for 5.17 remediation steps. • Resolved inconsistency between summary table and detail section for 6.17 remediation steps. • Resolved inconsistency between summary table and detail section for 7.8 remediation steps. • Resolved inconsistency between summary table and detail section for 6.13 remediation steps. • Resolved inconsistency between summary table and detail section for 7.7 remediation steps. • Resolved error in remediation script in 8.13 • Resolved inconsistency between summary table and detail section for 8.19 remediation steps. • Resolved inconsistency between summary table and detail section for 8.24 remediation steps.