CIS Microsoft Exchange Server 2010 Benchmark [imported]

v1.1.0 – 03-24-2015

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1
Table of Contents 2
Overview 4
Intended Audience 4
Consensus Guidance 5
Typographical Conventions 6
Recommendation Definitions 7
Title 7
Assessment Status 7
Automated 7
Manual 7
Profile 7
Description 7
Rationale Statement 7
Impact Statement 8
Audit Procedure 8
Remediation Procedure 8
Default Value 8
References 8
CIS Critical Security Controls® (CIS Controls®) 8
Additional Information 8
Profile Definitions 9
Acknowledgements 10
Recommendations 11
1 Transport 11
1.1 Set 'Maximum send size - connector level' to '10240' (Automated) 12
1.2 Set 'Maximum receive size - organization level' to '10240' (Automated) 13
1.3 Set 'Enable Sender ID agent' to 'True' (Automated) 14
1.4 Set 'External send connector authentication: DNS Routing' to 'True' (Manual) 15
1.5 Set 'Configure Sender Filtering' to 'Reject' (Automated) 16
1.6 Set 'Enable Sender reputation' to 'True' (Automated) 17
1.7 Set 'Maximum number of recipients - organization level' to '5000' (Automated) 18
1.8 Set 'External send connector authentication: Ignore Start TLS' to 'False' (Automated) 19
1.9 Set 'Configure login authentication for POP3' to 'SecureLogin' (Automated) 20
1.10 Set receive connector 'Configure Protocol logging' to 'Verbose' (Automated) 21
1.11 Set send connector 'Configure Protocol logging' to 'Verbose' (Automated) 22

1.12 Set 'External send connector authentication: Domain Security' to 'True' (Automated) 23
1.13 Set 'Message tracking logging - Transport' to 'True' (Automated) 24
1.14 Set 'Message tracking logging - Mailbox' to 'True' (Automated) 25
1.15 Set 'Configure login authentication for IMAP4' to 'SecureLogin' (Automated) 26
1.16 Set 'Turn on Connectivity logging' to 'True' (Automated) 27
1.17 Set 'Maximum send size - organization level' to '10240' (Automated) 28
1.18 Set 'Maximum receive size - connector level' to '10240' (Automated) 29

2 Mailbox 30

2.1 Set 'Mailbox quotas: Issue warning at' to '1991680' (Manual) 31
2.2 Set 'Mailbox quotas: Prohibit send and receive at' to '2411520' (Manual) 32
2.3 Set 'Mailbox quotas: Prohibit send at' to '2097152' (Manual) 33
2.4 Set 'Keep deleted mailboxes for the specified number of days' to '30' (Automated) 34
2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Automated) 35
2.6 Set 'Allow simple passwords' to 'False' (Automated) 36
2.7 Set 'Enforce Password History' to '4' (Automated) 37
2.8 Set 'Password Expiration' to '90' (Automated) 38
2.9 Set 'Minimum password length' to '4' (Automated) 39
2.10 Set 'Configure startup mode' to 'TLS' (Automated) 40
2.11 Set 'Refresh interval' to '1' (Automated) 41
2.12 Set 'Configure dial plan security' to 'Secured' (Automated) 42
2.13 Set 'Allow access to voicemail without requiring a PIN' to 'False' (Automated) 43
2.14 Set 'Retain deleted items for the specified number of days' to '14' (Automated) 44
2.15 Set 'Allow unmanaged devices' to 'False' (Automated) 45
2.16 Set 'Require encryption on device' to 'True' (Automated) 46
2.17 Set 'Time without user input before password must be re-entered' to '15' (Automated) 47
2.18 Set 'Require alphanumeric password' to 'True' (Automated) 48
2.19 Set 'Require client MAPI encryption' to 'True' (Automated) 49
2.20 Set 'Number of attempts allowed' to '10' (Automated) 50
2.21 Set 'Require password' to 'True' (Automated) 51

3 Other 52

3.1 Set cmdlets 'Turn on Administrator Audit Logging' to 'True' (Automated) 53
3.2 Set 'Require Client Certificates' to 'Required' (Manual) 54
3.3 Set 'Turn on script execution' to 'RemoteSigned' (Automated) 55
3.4 Set 'Turn on Administrator Audit Logging' to 'True' (Automated) 56
3.5 Set 'Enable automatic replies to remote domains' to 'False' (Automated) 57
3.6 Set 'Allow basic authentication' to 'False' (Automated) 58
3.7 Set 'Enable non-delivery reports to remote domains' to 'False' (Automated) 59
3.8 Set 'Enable OOF messages to remote domains' to 'None' (Automated) 60
3.9 Set 'Enable automatic forwards to remote domains' to 'False' (Automated) 61
3.10 Set 'Enable S/MIME for OWA 2010' to 'True' (Automated) 62
3.11 Set mailbox 'Turn on Administrator Audit Logging' to 'True' (Automated) 63

Appendix: Summary Table 64

Appendix: Change History 68

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Exchange Server 2010 SP2 and SP3. This guide was tested against Microsoft Exchange Server 2010 SP2 and SP3. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Exchange Server 2010 SP2 or SP3 on a Microsoft Windows platform.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - CAS Services Security**

  Items in this profile apply to the Client Access Server role and intend to:

  - Be practical and prudent,
  - Provide a clear security benefit, and
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Edge Services Security**

  Items in this profile apply to the Edge Server role and intend to:

  - Be practical and prudent,
  - Provide a clear security benefit, and
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Hub Services Security**

  Items in this profile apply to the Hub Server role and intend to:

  - Be practical and prudent,
  - Provide a clear security benefit, and
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Mailbox Services Security**

  Items in this profile apply to the Mailbox Server role and intend to:

  - Be practical and prudent,
  - Provide a clear security benefit, and
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - UM Services Security**

  Items in this profile apply to the Unified Messaging Server role and intend to:

  - Be practical and prudent,
  - Provide a clear security benefit, and
  - Not inhibit the utility of the technology beyond acceptable means.

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:

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.
Microsoft's Security Compliance Management Toolkit was an excellent resource in the development of this Benchmark. CIS also extends special recognition to the development teams of those resources. Readers are encouraged to download the toolkit to access many great resources, including tools such as GPOAccelerator and DCM Configuration Packs, which aid in the rapid deployment of security configuration policies

Editor
David Berube

Recommendations

1 Transport

Rules taking action on messages while they're in transit **Applies to :**

```
Set-SendConnector
Set-SenderFilterConfig
Set-SenderReputationConfig
Set-ReceiveConnector
Set-TransportServer
Set-TransportService
Set-TransportConfig
Set-PopSettings
Set-ImapSettings
```

1.1 Set 'Maximum send size - connector level' to '10240' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

This setting limits the total size of messages at the connector level. This includes the message header, the message body, and any attachments. For internal message flow, Exchange Server uses the custom X-MS-Exchange-Organization-OriginalSize: message header to record the original message size of the message as it enters the Exchange Server organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing.

Rationale:

This setting somewhat limits the impact a malicious user or a computer with malware can have on the Exchange infrastructure by restricting the size of incoming messages.

Impact:

Users will not be able to send messages larger than the limit.

Audit:

Execute the following cmdlet and ensure MaxMessageSize is set to '10240':

```
<strong>get-sendconnector "</strong><strong><strong>Connection to
Contoso.com</strong>" | fl -property MaxMessageSize</strong>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<strong>Set-SendConnector "Connection to Contoso.com" -MaxMessageSize
10240KB</strong>
```

Default Value:

10240

1.2 Set 'Maximum receive size - organization level' to '10240' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

This limit includes the message header, the message body, and any attachments. For internal message flow, Exchange Server uses the custom X-MS-Exchange-Organization-OriginalSize: message header to record the original message size of the message as it enters the Exchange Server organization. Whenever the message is checked against the specified message size limits, either the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing.

Rationale:

This setting somewhat limits the impact that a malicious user or a computer with malware can have on the Exchange infrastructure by restricting the size of incoming messages.

Impact:

Users will not be able to receive messages larger than the limit.

Audit:

Execute the following cmdlet and ensure MaxReceiveSize is set to '10240 ':

```
 <strong>Get-TransportConfig | fl -property </strong><strong><span
class="st"><em>MaxReceiveSize</em></span></strong>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<strong>Set-TransportConfig </strong><strong><span class="st">-
<em>MaxReceiveSize</em></span> 10240KB</strong>
```

Default Value:

10240

1.3 Set 'Enable Sender ID agent' to 'True' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

The Sender ID agent is an antispam agent enabled on Exchange servers that perform the Edge Transport server role. Sender ID tries to verify that every e-mail message originates from the Internet domain from which it claims to have been sent. Sender ID checks the address of the server that sends the message against a registered list of servers that the domain owner has authorized to send e-mail.

Rationale:

Spam consumes a large amount of network bandwidth and server capacity. In addition, it is often the source of malicious software.

Impact:

Some legitimate messages may be blocked.

Audit:

Execute the following cmdlet and ensure InternalSMTPServers is set to 'True ':

```
<span>Get-TransportConfigSenderIDConfig | Formatfl -Listproperty
InternalSMTPServersEnabled</span>
```

Remediation:

To remediate this settings, execute the following cmdlet :

```
<span>Set-SenderIDConfig -Enabled $true</span>
```

Default Value:

True

1.4 Set 'External send connector authentication: DNS Routing' to 'True' (Manual)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

Select this option to use DNS to route outbound mail. If enabled the connector will use DNS to resolve the IP address of the remote SMTP server.

Rationale:

Basic authentication sends credentials across the network in plaintext. DNS routing helps protect connections from tampering or interception by unauthorized users.

Impact:

The organization's servers will only be able to send e-mail to remote servers that are located through DNS routing.

Audit:

Execute the following cmdlet and ensure DNSRoutingEnabled is set to 'True':

```
Get-SendConnector "Connection to Contoso.com" | fl -property
DNSRoutingEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-SendConnector "Connection to Contoso.com" -DNSRoutingEnabled $true
```

Default Value:

False

1.5 Set 'Configure Sender Filtering' to 'Reject' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

By default, sender filtering is enabled on a computer performing the Edge Transport server role for inbound messages from the Internet that are not authenticated. These messages are handled as external messages. You can disable the Sender Filter agent in individual computer configurations by using the Exchange Management Console or the Exchange Management Shell. When you enable the Sender Filter agent on a computer running Exchange, it filters all messages from all Receive connectors on that computer. Only messages from external sources are filtered. External sources are defined as non-authenticated sources. These are considered anonymous Internet sources.

Rationale:

Spam consumes a large amount of network bandwidth and server capacity. In addition, it is often the source of malicious software.

Impact:

Some legitimate messages may be blocked.

Audit:

Execute the following cmdlet and ensure Enabled is set to 'True':

```
Get-SenderFilterConfig | fl -property Enabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-SenderFilterConfig -Enabled $true
```

Default Value:

True

1.6 Set 'Enable Sender reputation' to 'True' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

When sender reputation is enabled on a computer, sender reputation filters all messages from all Receive connectors on that computer. Only messages from external sources are filtered. External sources are defined as non-authenticated sources, which are considered anonymous Internet sources.

Rationale:

Spam consumes a large amount of network bandwidth and server capacity. In addition, it is often the source of malicious software.

Impact:

Some legitimate messages may be blocked if the threshold is set too high.

Audit:

Execute the following cmdlet and ensure SenderBlockingEnabled and OpenProxyDetectionEnabled are set to 'True':

```
Get-SenderReputationConfig
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-SenderReputationConfig -SenderBlockingEnabled $true -
OpenProxyDetectionEnabled $true
```

Default Value:

True

1.7 Set 'Maximum number of recipients - organization level' to '5000' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to control the total number of message recipients. When a message is first composed, the recipients exist in the To:, Cc:, and Bcc: header fields. When the message is submitted for delivery, the message recipients are converted into RCPT TO: entries in the message envelope. A distribution group is counted as a single recipient during message submission.

Rationale:

This setting somewhat limits the impact that a malicious user or a computer with malware can have on the Exchange infrastructure by restricting the number of recipients for any single message.

Impact:

Users will not be able to send a message to more recipients than the limit.

Audit:

Execute the following cmdlet and ensure PickupDirectoryMaxRecipientsPerMessage is set to '5000':

```
Get-TransportServer -Identity "Server01"
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-TransportServer -Identity "Server01" -
PickupDirectoryMaxRecipientsPerMessage 5000
```

Default Value:

5000

1.8 Set 'External send connector authentication: Ignore Start TLS' to 'False' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

If this setting is enabled then you will not be able to configure mutual authentication TLS, referred to as "External send connector authentication: Domain Security" in this baseline.

Rationale:

Basic authentication sends credentials across the network in plaintext. TLS helps protect credentials from interception by unauthorized users.

Impact:

The organization's servers will only be able to send e-mail to remote servers that TLS.

Audit:

Execute the following cmdlet and ensure IgnoreSTARTTLS is set to 'False':

```
<span>Get-SendConnector </span><span><span>-identity <connector_name> | fl -
property </span>IgnoreSTARTTLS</span>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<span>set-SendConnector </span><span><span>-identity <connector_name>
</span>-IgnoreSTARTTLS: $false</span>
```

Default Value:

True

1.9 Set 'Configure login authentication for POP3' to 'SecureLogin' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

POP3 transmits all data, including user credentials and potentially sensitive messages, in plaintext. Using this setting to enable TLS ensures that POP3 network traffic is encrypted, and it allows the client to verify the server's address.

Rationale:

An attacker who can intercept or eavesdrop on the POP3 traffic could view sensitive information.

Impact:

Clients that do not support TLS will not be able to access e-mail via POP3.

Audit:

Execute the following cmdlet and ensure SecureLogin is set to 'SecureLogin':

```
Get-PopSettings  | fl -property LoginType
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-PopSettings -LoginType SecureLogin
```

Default Value:

SecureLogin

1.10 Set receive connector 'Configure Protocol logging' to 'Verbose' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

A protocol log is a record of the SMTP activity between messaging servers as part of message delivery. This SMTP activity occurs on Send connectors and Receive connectors that are configured on Hub Transport servers and Edge Transport servers. By default, protocol logging is disabled.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure ProtocolLoggingLevel is set to 'None':

```
Get-ReceiveConnector "IDENTITY" | fl -property ProtocolLoggingLevel
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector "IDENTITY" -ProtocolLoggingLevel Verbose
```

Default Value:

None

1.11 Set send connector 'Configure Protocol logging' to 'Verbose' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

A protocol log is a record of the SMTP activity between messaging servers as part of message delivery. This SMTP activity occurs on Send connectors and Receive connectors that are configured on Hub Transport servers and Edge Transport servers. By default, protocol logging is disabled.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure ProtocolLogginglevel is set to 'Verbose':

```
Get-SendConnector "IDENTITY" | fl -property ProtocolLoggingLevel
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-SendConnector "IDENTITY" -ProtocolLoggingLevel Verbose
```

Default Value:

None

1.12 Set 'External send connector authentication: Domain Security' to 'True' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

It is preferable to use Exchange Authentication or IPsec for external send connectors. However, if you must use Basic authentication to enable Domain Security, using (Mutual Auth TLS) for external send connectors helps to protect credentials and e-mail sent to other organizations. If enabled the Send connector will attempt to establish a mutual Transport Layer Security (TLS) connection with remote servers when sending mail. There are additional configuration steps required before you can start using TLS. For more information about how to configure mutual TLS, see Using Domain Security: Configuring Mutual TLS: http://technet.microsoft.com/en-us/library/bb123543(EXCHG.140).aspx

Rationale:

Basic authentication sends credentials across the network in plaintext. Domain Security (Mutual Auth TLS) helps protect credentials from interception by unauthorized users.

Impact:

The organization's servers will only be able to send e-mail to remote servers that support Domain Security (Mutual Auth TLS).

Audit:

Execute the following cmdlet and ensure DomainSecureEnabled is set to 'True':

```
 get-sendconnector -Identity <SendConnectorIdParameter> | fl
<em>DomainSecureEnabled</em>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<em>set</em>-<em>sendconnector</em> -Identity <SendConnectorIdParameter> -
<em>DomainSecureEnabled</em> $true
```

Default Value:

False

1.13 Set 'Message tracking logging - Transport' to 'True' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

A message tracking log provides a detailed log of all message activity as messages are transferred to and from a computer running Exchange. Message tracking is available on Hub Transport servers, Edge Transport servers, and Mailbox servers. By default, message tracking is enabled.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure MessageTrackingLogEnabled is set to 'True':

```
Get-TransportServer Mailbox01 | fl -property MessageTrackingLogEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-TransportServer Mailbox01 -MessageTrackingLogEnabled $true
```

Default Value:

True

1.14 Set 'Message tracking logging - Mailbox' to 'True' (Automated)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

A message tracking log provides a detailed log of all message activity as messages are transferred to and from a computer running Exchange. Message tracking is available on Hub Transport servers, Edge Transport servers, and Mailbox servers. By default, message tracking is enabled.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure MessageTrackingLogEnabled is set to 'True':

```
Get-TransportServer Mailbox01 | fl -property -MessageTrackingLogEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-TransportServer Mailbox01 -MessageTrackingLogEnabled $true
```

Default Value:

True

1.15 Set 'Configure login authentication for IMAP4' to 'SecureLogin' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

IMAP4 transmits all data, including user credentials and potentially sensitive messages, in plaintext. Using this setting to enable SSL ensures that IMAP4 network traffic is encrypted, and it allows the client to verify the server's address.

Rationale:

An attacker who can intercept or eavesdrop on the IMAP4 traffic could view sensitive information.

Impact:

Clients that do not support TLS will not be able to access e-mail via IMAP.

Audit:

Execute the following cmdlet and ensure LoginType is set to 'SecureLogin':

```
Get-ImapSettings | fl -property LoginType
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ImapSettings<strong> -LoginType SecureLogin</strong>
```

Default Value:

SecureLogin

1.16 Set 'Turn on Connectivity logging' to 'True' (Automated)

Profile Applicability:

- Level 1 - Edge Services Security

Description:

A connectivity log is a record of the SMTP connection activity of the outbound message delivery queues to the destination Mailbox server, smart host, or domain. Connectivity logging is available on Hub Transport servers and Edge Transport servers. By default, connectivity logging is disabled.

Rationale:

If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure ConnectivityLogEnabled is set to 'True':

```
Get-TransportServer <Identity> | fl -property ConnectivityLogEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-TransportServer <Identity> -ConnectivityLogEnabled $true
```

Default Value:

False

1.17 Set 'Maximum send size - organization level' to '10240' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

This limit includes the message header, the message body, and any attachments. For internal message flow, Exchange Server uses the custom X-MS-Exchange-Organization-OriginalSize: message header to record the original message size of the message as it enters the Exchange Server organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing.

Rationale:

This setting somewhat limits the impact that a malicious user or a computer with malware can have on the Exchange infrastructure by restricting the size of outgoing messages.

Impact:

Users will not be able to send a message larger than the limit.

Audit:

Execute the following cmdlet and ensure MaxSendSize is set to '10240':

```
<strong><span>Get-TransportConfig | fl -</span></strong><span class="\"diff-
html-removed\""><span>propert</span><span>y</span></span><strong><span>
MaxSendSize</span></strong>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<strong>Set-TransportConfig -MaxSendSize 10240KB</strong>
```

Default Value:

10240

1.18 Set 'Maximum receive size - connector level' to '10240' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to limit the total size of messages at the connector level. This includes the message header, the message body, and any attachments. For internal message flow, Exchange Server uses the custom X-MS-Exchange-Organization-OriginalSize: message header to record the original message size of the message as it enters the Exchange Server organization. Whenever the message is checked against the specified message size limits, the lower value of the current message size or the original message size header is used. The size of the message can change because of content conversion, encoding, and agent processing.

Rationale:

This setting somewhat limits the impact a malicious user or a computer with malware can have on the Exchange infrastructure by restricting the size of incoming messages.

Impact:

Users will not be able to receive messages larger than the limit.

Audit:

Execute the following cmdlet and ensure MaxMessageSize is set to '10240KB':

```
Get-ReceiveConnector "Connection from Contoso.com" | fl -property
MaxMessageSize
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 10240KB
```

Default Value:

10240

2 Mailbox

Rules taking action on mailbox, unified messaging, address books and public folders
Applies to :

```
``Set-MailboxDatabase
Set-ActiveSyncMailboxPolicy
Set-UMService
Set-UMMailboxPolicy ``
Set-UMDialPlan
Set-CASMailbox
```

2.1 Set 'Mailbox quotas: Issue warning at' to '1991680' (Manual)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

You can configure this setting to automatically warn mailbox users that their mailbox is approaching its storage limit. To specify the storage limit, select the check box for this capability, and then specify in kilobytes (KB) how much content users can store in their mailboxes before a warning e-mail message is sent to them. You can enter a value between 0 and 2,147,483,647 KB (2.1 terabytes).

Rationale:

If users exceed their mailbox limits without warning, they may miss important messages requiring them to take immediate action to mitigate a security risk.

Impact:

Users will receive a warning when their mailboxes reach the specified value.

Audit:

Execute the following cmdlet and ensure IssueWarningQuota is set to '1991680KB':

```
<span>Get-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span> | fl -
property IssueWarningQuota</span>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
<span>Set-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span> -
IssueWarningQuota 1991680KB</span>
```

Default Value:

1991680

2.2 Set 'Mailbox quotas: Prohibit send and receive at' to '2411520' (Manual)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

Configure this setting to prevent users from sending and receiving e-mail messages after their mailbox size reaches the specified limit. To specify this limit, select the check box, and then type the size of the mailbox in kilobytes (KB) at which you want to prohibit the sending and receiving of e-mail messages and notify the user. You can enter a value between 0 and 2,147,483,647 KB (2.1 terabytes).

Rationale:

If users exceed their mailbox limits without warning, they may miss important messages requiring them to take immediate action to mitigate a security risk.

Impact:

Users will be unable to send or receive messages when their mailboxes reach the specified value.

Audit:

Execute the following cmdlet and ensure ProhibitSendReceiveQuota is set to '2411520KB':

```
Get-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span> | fl -property
ProhibitSendReceiveQuota
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span>  -
ProhibitSendReceiveQuota 2411520KB
```

Default Value:

2411520

2.3 Set 'Mailbox quotas: Prohibit send at' to '2097152' (Manual)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

You can configure this setting to prevent users from sending new e-mail messages after their mailboxes reach a specified limit. To specify this limit, select the check box for this capability, and then type the size of the mailbox in kilobytes (KB) at which you want to prohibit the sending and receiving of e-mail messages and notify the user. You can enter a value between 0 and 2,147,483,647 KB (2.1 terabytes).

Rationale:

This setting prevents users from sending messages when their mailbox is approaching its size limit. However, they can continue to receive messages.

Impact:

Users will be unable to send messages when their mailboxes reach the specified value.

Audit:

Execute the following cmdlet and ensure ProhibitSendQuota is set to '2097152KB':

```
Get-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span> | fl -property
ProhibitSendQuota
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase <span>"EXCHANGE01\Mailbox Database"</span>  -
ProhibitSendQuota 2097152KB
```

Default Value:

2097152

2.4 Set 'Keep deleted mailboxes for the specified number of days' to '30' (Automated)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

You can use this setting to specify how long deleted mailboxes are retained before they are permanently removed from the database. Defining a reasonable retention period facilitates recovering accidentally deleted mailboxes while controlling the volume of storage that retained mailboxes require.

Rationale:

Administrators may want to recover accidentally deleted mailboxes or they may need to recover deliberately deleted mailboxes for legal or managerial reasons.

Impact:

The impact should be small: additional storage space will be required for storing deleted mailboxes until they are purged.

Audit:

Execute the following cmdlet and ensure MailboxRetention is set to '30.00:00:00':

```
<span>Get-Mailboxdatabase "EXCHANGE01\Mailbox Database" </span>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-Mailboxdatabase "EXCHANGE01\Mailbox Database"  -MailboxRetention
30.00:00:00
```

Default Value:

30

2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Automated)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

This setting allows you to ensure that items are not permanently deleted until the database has been backed up.

Rationale:

To ensure that accidentally deleted items can be recovered, they should not be permanently deleted until the database is backed up.

Impact:

The impact of enabling this setting should be minimal. More storage space will be required until any pending items are permanently deleted.

Audit:

Execute the following cmdlet and ensure RetainDeletedItemsUntilBackup is set to 'True':

```
Get-MailboxDatabase <Mailbox Database Name> | fl -property
RetainDeletedItemsUntilBackup
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase <Mailbox Database Name> -RetainDeletedItemsUntilBackup
$true
```

Default Value:

False

2.6 Set 'Allow simple passwords' to 'False' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can configure this setting to require strong passwords to unlock mobile devices before they can connect via ActiveSync to an Exchange server.

Rationale:

Allowing simple passwords can make it easier for an attacker to correctly guess them.

Impact:

Users will be forced to use strong passwords.

Audit:

Execute the following cmdlet and ensure AllowSimpleDevicePassword is set to 'False':

```
Get-ActiveSyncMailboxPolicy | fl -property AllowSimpleDevicePassword
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy <Profile> -AllowSimpleDevicePassword $false
```

Default Value:

True

2.7 Set 'Enforce Password History' to '4' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Retaining the password history ensures that old passwords will not be reused within a reasonable timeframe.

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through a brute force attack. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this setting, users will be able to use the same small number of passwords repeatedly.

Impact:

The major impact of this setting configuration is that it requires users to create a new password every time they change an old one. Requiring users to change their passwords to new unique values increases the risk of users writing them down to not forget them. Another risk is that users may create passwords that change incrementally to make them easier to remember but also easier to guess. An example of this would be password01, password02, and so on.

Audit:

Execute the following cmdlet and ensure DevicePasswordHistory is set to '4':

```
Get-ActiveSyncMailboxPolicy | fl -property DevicePasswordHistory
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy <Profile> -DevicePasswordHistory 4
```

Default Value:

0

2.8 Set 'Password Expiration' to '90' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can configure this setting to specify how long before passwords expire and users must change them.

Rationale:

The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring this setting to 0 so that users are never required to change their passwords is a major security risk because doing so allows a compromised password to be used by a malicious user for as long as the valid user has authorized access to the system.

Impact:

Configuring the value of this setting too low requires users to change their passwords very often. This can reduce security in the organization, because users might write their passwords in an unsecured location or lose them. Configuring the value of this setting too high also reduces the level of security in an organization, because it allows potential attackers more time to discover user passwords or to use compromised accounts.

Audit:

Execute the following cmdlet and ensure DevicePasswordExpiration is set to '90':

```
Get-ActiveSyncMailboxPolicy | fl -property DevicePasswordExpiration
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy <Profile> -DevicePasswordExpiration 90
```

Default Value:

Unlimited

2.9 Set 'Minimum password length' to '4' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can configure this setting to specify a minimum password length for device passwords. Long passwords can provide increased security. However, long passwords can decrease device usability.

Rationale:

Types of password attacks include dictionary attacks that use common words and phrases, and brute force attacks that use character combinations. Attackers also sometimes try to obtain an account database so they can use tools to discover accounts and passwords.

Impact:

Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave password information in an unsecured location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Audit:

Execute the following cmdlet and ensure MinDevicePasswordLength is set to '4':

```
Get-ActiveSyncMailboxPolicy | fl -property MinDevicePasswordLength
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy <Profile> -MinDevicePasswordLength 4
```

Default Value:

4

2.10 Set 'Configure startup mode' to 'TLS' (Automated)

Profile Applicability:

- Level 1 - UM Services Security

Description:

Use this setting to start the UM Server in secure mode. This forces all dial plans to use TLS.

Rationale:

Communications between other VOIP systems and Exchange that are not protected by TLS are vulnerable to being captured by a malicious third party.

Impact:

VOIP systems that do not support TLS will be blocked from connecting to your Exchange servers after this is applied.

Audit:

Execute the following cmdlet and ensure UMStartUpMode is set to 'TCP':

```
Get-UMServer -Identity MyUMServer1 | fl -property UMStartUpMode
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-UMServer -Identity MyUMServer1 -UMStartUpMode TLS
```

Default Value:

TCP

2.11 Set 'Refresh interval' to '1' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can configure this setting to specify how often in hours that policy settings should be refreshed. Refreshing the policy settings sends a fresh copy of the policy down to devices.

Rationale:

Organizational requirements change, and new vulnerabilities may be discovered, so it is likely that ActiveSync policy settings will change. For these reasons, it is important to configure a refresh interval to ensure that the latest policy settings are applied to the devices in your organization.

Impact:

Clients will attempt to acquire the latest policy at a shorter interval impacting server and client bandwidth.

Audit:

Execute the following PowerShell script.

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property -
DevicePolicyRefreshInterval
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -DevicePolicyRefreshInterval
00:60:00
```

Default Value:

Unlimited

2.12 Set 'Configure dial plan security' to 'Secured' (Automated)

Profile Applicability:

- Level 1 - UM Services Security

Description:

Use this setting to protect individual dial plans if the UM Server cannot be started in TLS Mode. To use this setting, the UM Server must be started in DUAL Mode.

Rationale:

If the UM role is not started in secure mode, each dial plan is individually vulnerable to traffic being captured by a malicious third party.

Impact:

VOIP systems that do not support TLS will be blocked from connecting to your Exchange servers after this is applied.

Audit:

Execute the following cmdlet and ensure VoIPSecurity is set to 'Secured':

```
Get-UMDialPlan -identity MySecureDialPlan | fl -property VoIPSecurity
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Secured
```

Default Value:

Unsecured

2.13 Set 'Allow access to voicemail without requiring a PIN' to 'False' (Automated)

Profile Applicability:

- Level 1 - UM Services Security

Description:

Use this setting to ensure PIN access to mailbox data via voice is required.

Rationale:

If PINLess access is enabled, the mailbox data is unsecured and vulnerable to capture when being accessed via the phone

Impact:

All mailbox data could be obtained through the voicemail system

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-UMMailboxPolicy -id MyUMMailboxPolicy | fl -property
AllowPinlessVoiceMailAccess
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowPinlessVoiceMailAccess $false
```

Default Value:

False

2.14 Set 'Retain deleted items for the specified number of days' to '14' (Automated)

Profile Applicability:

- Level 1 - Mailbox Services Security

Description:

You can use this setting to specify how long deleted messages are retained before they are permanently removed from the database. Defining a reasonable retention period facilitates recovering accidentally deleted messages while controlling the volume of storage that retained messages require.

Rationale:

Users may want to recover accidentally deleted messages, or administrators may need to recover deliberately deleted messages for legal or managerial reasons.

Impact:

The impact should be small: additional storage space will be required for storing deleted messages until they are purged.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-MailboxDatabase -Identity MDB2 | fl -property DeletedItemRetention
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 14
```

Default Value:

14

2.15 Set 'Allow unmanaged devices' to 'False' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

This setting determines whether Exchange allow devices that do not accept security policy updates from the Exchange server to use ActiveSync.

Rationale:

Unmanaged devices are more likely to not comply with an organization's security policies and to be infected by malicious software.

Impact:

Users who configure their devices to block security policy or have devices that cannot receive security policy will be unable to use ActiveSync to connect to the server.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property
AllowNonProvisionableDevices
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -AllowNonProvisionableDevices
$false
```

Default Value:

False

2.16 Set 'Require encryption on device' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can use this setting to require device encryption. Configuring this setting to require device encryption increases security by encrypting all information on the storage cards for the device.

Rationale:

Unencrypted data on mobile devices is vulnerable to attack. Requiring ActiveSync encryption helps to minimize the risk of information being compromised in case a mobile device is lost.

Impact:

Devices that do not support data encryption will be unable to connect to Exchange servers in your organization.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity:<em>SalesPolicy</em> | fl -property
<em>RequireDeviceEncryption</em>
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity:<em>SalesPolicy</em> -
<em>RequireDeviceEncryption $true</em>
```

Default Value:

False

2.17 Set 'Time without user input before password must be re-entered' to '15' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can configure this setting to prompt the user for a password after the user's device has been inactive for a specified period of time. For example, if you configure the time period for this setting to 15 minutes, the user must enter the device password every time it has been idle for 15 minutes. If the device has been idle less than 15 minutes, the user is not required to re-enter the password.

Rationale:

Mobile devices are often left unattended or lost in public places. Requiring devices to lock after 15 minutes minimizes the window of opportunity for an attacker to tamper with a lost or stolen device.

Impact:

Users must re-enter their passwords each time their devices remain idle for 15 minutes or longer.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property
MaxInactivityTimeDeviceLock
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -MaxInactivityTimeDeviceLock
00:15:00
```

Default Value:

15

2.18 Set 'Require alphanumeric password' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Requiring users to include non-numeric characters in their passwords increases the strength of password security in your organization.

Rationale:

Not requiring alphanumeric passwords can make it easier for an attacker to correctly guess them.

Impact:

Users will be forced to use alphanumeric passwords.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property
AlphanumericDevicePasswordRequired
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -
AlphanumericDevicePasswordRequired $true
```

Default Value:

False

2.19 Set 'Require client MAPI encryption' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Certificates can reside in the certificate store on a mobile device or on a smart card. A certificate authentication method uses the Extensible Authentication Protocol (EAP) and the Transport Layer Security (TLS) protocol. During EAP-TLS certificate authentication, the client and the server prove their identities to each other. For example, an Exchange ActiveSync client presents its user certificate to the Client Access server, and the Client Access server presents its computer certificate to the mobile device to provide mutual authentication.

Rationale:

Communications between Outlook and Exchange that are sent unencrypted are vulnerable to being captured by a malicious third party.

Impact:

Client computers running earlier versions of Outlook or Outlook with profiles set to not use encryption will be blocked from connecting to your Exchange servers after this is applied.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-CASMailbox | fl -property MAPIEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-CASMailbox <Profile> -MAPIEnabled $true
```

Default Value:

False

2.20 Set 'Number of attempts allowed' to '10' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Use this setting to restrict the number of failed logon attempts a user can make.

Rationale:

There is a high risk that mobile devices will be lost or stolen. Enforcing this setting reduces the likelihood that an unauthorized user can guess the password of a device to access data stored on it.

Impact:

If you enable this setting, a locked-out account cannot be used again until an administrator either resets it or the account lockout duration expires. This setting will likely generate additional help desk calls. In fact, locked accounts cause the greatest number of help desk calls in many organizations.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property
MaxDevicePasswordFailedAttempts
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -
MaxDevicePasswordFailedAttempts 10
```

Default Value:

6

2.21 Set 'Require password' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Passwords should be necessary to unlock mobile devices because they will help secure sensitive information stored on the devices in the event of loss or theft.

Rationale:

Allowing users to access devices without passwords means that anyone with physical access to them can view data on the devices.

Impact:

Users will have to re-enter their password each time they want to use their device.

Audit:

To view the current setting, execute the following PowerShell cmdlet:

```
Get-ActiveSyncMailboxPolicy -Identity MyPolicy | fl -property
DevicePasswordEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ActiveSyncMailboxPolicy -Identity MyPolicy -DevicePasswordEnabled $true
```

Default Value:

False

3 Other

Rules that are not covered by other categories

Applies to :

```
Set-ExecutionPolicy
Set-RemoteDomain
Set-OwaVirtualDirectory
Set-AdminAuditLogConfig
```

3.1 Set cmdlets 'Turn on Administrator Audit Logging' to 'True' (Automated)

Profile Applicability:

- Level 1 - UM Services Security

Description:

Administrator audit logging is used to provide a log of the settings that are changed by administrators anywhere in the system. By default this setting is turned on to ensure discovery of configuration related security breaches.

Rationale:

Administrators may be able to reconfigure the system to expose a vulnerability with no record of the changes made.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure is set to '*':

```
Get-AdminAuditLogConfig | fl -property AdminAuditLogCmdlets
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets *
```

Default Value:

True

3.2 Set 'Require Client Certificates' to 'Required' (Manual)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Certificates can reside in the certificate store on a mobile device or on a smart card. A certificate authentication method uses the Extensible Authentication Protocol (EAP) and the Transport Layer Security (TLS) protocol. During EAP-TLS certificate authentication, the client and the server prove their identities to each other. For example, an Exchange ActiveSync client presents its user certificate to the Client Access server, and the Client Access server presents its computer certificate to the mobile device to provide mutual authentication.

Rationale:

The default behavior of Exchange is to only require Basic Authentication. This type of authentication occurs in plaintext, which increases the possibility that an attacker could capture a user's credentials. In addition to configuring this setting to require client certificates, you can further mitigate the risk that the default behavior poses by configuring IIS to require SSL or TLS user connections to the Exchange servers in your organization.

Impact:

Mobile devices will only be able to connect via ActiveSync if they have a trusted client certificate installed.

Audit:

Not Scorred:

```
N/A
```

Remediation:

To remediate this setting, use the following steps to configure IIS Server:

```
http://technet.microsoft.com/en-us/library/bb266938%28v=exchg.141%29.aspx
```

Default Value:

Not Configured

3.3 Set 'Turn on script execution' to 'RemoteSigned' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

Use this setting to configure the script execution policy that controls what script types users can run.

Rationale:

Unsigned scripts are at greater risk of containing unauthorized code.

Impact:

Extra configuration is required to setup Exchange servers to use an organization's public key infrastructure (PKI) certificates to sign scripts. In addition, a process must be established to explain how to test and sign scripts before they can run on production servers.

Audit:

Execute the following cmdlet and ensure RemoteSigned is set to 'RemoteSigned':

```
Get-ExecutionPolicy | fl -property  RemoteSigned
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-ExecutionPolicy RemoteSigned
```

Default Value:

RemoteSigned

3.4 Set 'Turn on Administrator Audit Logging' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Administrator audit logging is used to provide a log of the settings that are changed by administrators anywhere in the system. By default this setting is turned on to ensure discovery of configuration related security breaches.

Rationale:

Administrators may be able to reconfigure the system to expose a vulnerability with no record of the changes made.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure AdminAuditLogEnabled is set to 'true':

```
Get-AdminAuditLogConfig | fl -property AdminAuditLogEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

Default Value:

True

3.5 Set 'Enable automatic replies to remote domains' to 'False' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to determine if the server automatically replies to remote domains.

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct other types of attacks.

Impact:

Remote users will not receive automated reply messages.

Audit:

Execute the following cmdlet and ensure AutoReplyEnabled is set to 'False':

```
Get-RemoteDomain -Identity Contoso | fl -property AutoReplyEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-RemoteDomain -Identity Contoso -AutoReplyEnabled $false
```

Default Value:

False

3.6 Set 'Allow basic authentication' to 'False' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

Use this setting to determine whether you want to allow clients to use basic authentication.

Rationale:

The default behavior of Exchange is to only require Basic Authentication. This type of authentication occurs in plaintext, which increases the possibility that an attacker could capture a user's credentials. In addition to configuring this setting to require client certificates, you can further mitigate the risk that the default behavior poses by configuring IIS to require SSL or TLS user connections to the Exchange servers in your organization.

Impact:

Mobile devices will only be able to connect via ActiveSync if they do not use basic authentication.

Audit:

Execute the following cmdlet and ensure BasicAuthentication is set to 'True':

```
Get-OwaVirtualDirectory -Identity "owa (Default Web Site)" | fl -property
BasicAuthentication
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -
BasicAuthentication $false
```

Default Value:

True

3.7 Set 'Enable non-delivery reports to remote domains' to 'False' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to determines if the server automatically sends delivery reports to remote domains.

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct other types of attacks.

Impact:

Remote users will not receive automated non-delivery reports.

Audit:

Execute the following cmdlet and ensure NDREnabled is set to 'True':

```
Get-RemoteDomain -Identity Contoso  | fl -property NDREnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-RemoteDomain -Identity Contoso -NDREnabled $false
```

Default Value:

True

3.8 Set 'Enable OOF messages to remote domains' to 'None' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to determine if the server automatically forwards out-of-office messages to remote domains.

Rationale:

Attackers can use automated messages to determine whether a user is active, in the office, traveling, and so on. An attacker might use this information to conduct other types of attacks.

Impact:

Remote users will not receive automated out-of-office messages.

Audit:

Execute the following cmdlet and ensure AllowedOOFType is set to 'External':

```
Get-RemoteDomain "RemoteDomain" | fl -property AllowedOOFType
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType None
```

Default Value:

External

3.9 Set 'Enable automatic forwards to remote domains' to 'False' (Automated)

Profile Applicability:

- Level 1 - Hub Services Security

Description:

You can use this setting to determine if the server sends automatic forwards to remote domains.

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct other types of attacks.

Impact:

Remote users will not receive automated forward messages.

Audit:

Execute the following cmdlet and ensure AutoForwardEnabled is set to 'False':

```
Get-RemoteDomain -Identity Contoso | fl -property AutoForwardEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-RemoteDomain -Identity Contoso -AutoForwardEnabled $false
```

Default Value:

False

3.10 Set 'Enable S/MIME for OWA 2010' to 'True' (Automated)

Profile Applicability:

- Level 1 - CAS Services Security

Description:

You can enable this setting to allow users to download the S/MIME control to read and create signed and encrypted messages.

Rationale:

S/MIME uses digital signatures and encryption to protect against several classes of attacks including eavesdropping, impersonation, and tampering.

Impact:

Users will be able to use the S/MIME control when accessing their e-mail via OWA.

Audit:

Execute the following cmdlet and ensure SMimeEnabled is set to 'true':

```
Get-OWAVirtualDirectory -identity "owa (Default Web Site)" | fl -property
SMimeEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-OWAVirtualDirectory -identity "owa (Default Web Site)" -SMimeEnabled
$true
```

Default Value:

True

3.11 Set mailbox 'Turn on Administrator Audit Logging' to 'True' (Automated)

Profile Applicability:

- Level 1 - UM Services Security

Description:

Administrator audit logging is used to provide a log of the settings that are changed by administrators anywhere in the system. By default this setting is turned on to ensure discovery of configuration related security breaches.

Rationale:

Administrators may be able to reconfigure the system to expose a vulnerability with no record of the changes made.

Impact:

The impact should be small: additional storage space will be required and some processing power will be used to track and record information.

Audit:

Execute the following cmdlet and ensure AdminAuditLogEnabled is set to 'True':

```
Get-AdminAuditLogConfig | fl -property AdminAuditLogEnabled
```

Remediation:

To remediate this setting, execute the following PowerShell cmdlet:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled true
```

Default Value:

True

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Transport**		
1.1	Set 'Maximum send size - connector level' to '10240' (Automated)	☐	☐
1.2	Set 'Maximum receive size - organization level' to '10240' (Automated)	☐	☐
1.3	Set 'Enable Sender ID agent' to 'True' (Automated)	☐	☐
1.4	Set 'External send connector authentication: DNS Routing' to 'True' (Manual)	☐	☐
1.5	Set 'Configure Sender Filtering' to 'Reject' (Automated)	☐	☐
1.6	Set 'Enable Sender reputation' to 'True' (Automated)	☐	☐
1.7	Set 'Maximum number of recipients - organization level' to '5000' (Automated)	☐	☐
1.8	Set 'External send connector authentication: Ignore Start TLS' to 'False' (Automated)	☐	☐
1.9	Set 'Configure login authentication for POP3' to 'SecureLogin' (Automated)	☐	☐
1.10	Set receive connector 'Configure Protocol logging' to 'Verbose' (Automated)	☐	☐
1.11	Set send connector 'Configure Protocol logging' to 'Verbose' (Automated)	☐	☐
1.12	Set 'External send connector authentication: Domain Security' to 'True' (Automated)	☐	☐
1.13	Set 'Message tracking logging - Transport' to 'True' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.14	Set 'Message tracking logging - Mailbox' to 'True' (Automated)	☐	☐
1.15	Set 'Configure login authentication for IMAP4' to 'SecureLogin' (Automated)	☐	☐
1.16	Set 'Turn on Connectivity logging' to 'True' (Automated)	☐	☐
1.17	Set 'Maximum send size - organization level' to '10240' (Automated)	☐	☐
1.18	Set 'Maximum receive size - connector level' to '10240' (Automated)	☐	☐
2	**Mailbox**		
2.1	Set 'Mailbox quotas: Issue warning at' to '1991680' (Manual)	☐	☐
2.2	Set 'Mailbox quotas: Prohibit send and receive at' to '2411520' (Manual)	☐	☐
2.3	Set 'Mailbox quotas: Prohibit send at' to '2097152' (Manual)	☐	☐
2.4	Set 'Keep deleted mailboxes for the specified number of days' to '30' (Automated)	☐	☐
2.5	Set 'Do not permanently delete items until the database has been backed up' to 'True' (Automated)	☐	☐
2.6	Set 'Allow simple passwords' to 'False' (Automated)	☐	☐
2.7	Set 'Enforce Password History' to '4' (Automated)	☐	☐
2.8	Set 'Password Expiration' to '90' (Automated)	☐	☐
2.9	Set 'Minimum password length' to '4' (Automated)	☐	☐
2.10	Set 'Configure startup mode' to 'TLS' (Automated)	☐	☐
2.11	Set 'Refresh interval' to '1' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.12	Set 'Configure dial plan security' to 'Secured' (Automated)	☐	☐
2.13	Set 'Allow access to voicemail without requiring a PIN' to 'False' (Automated)	☐	☐
2.14	Set 'Retain deleted items for the specified number of days' to '14' (Automated)	☐	☐
2.15	Set 'Allow unmanaged devices' to 'False' (Automated)	☐	☐
2.16	Set 'Require encryption on device' to 'True' (Automated)	☐	☐
2.17	Set 'Time without user input before password must be re-entered' to '15' (Automated)	☐	☐
2.18	Set 'Require alphanumeric password' to 'True' (Automated)	☐	☐
2.19	Set 'Require client MAPI encryption' to 'True' (Automated)	☐	☐
2.20	Set 'Number of attempts allowed' to '10' (Automated)	☐	☐
2.21	Set 'Require password' to 'True' (Automated)	☐	☐
3	**Other**		
3.1	Set cmdlets 'Turn on Administrator Audit Logging' to 'True' (Automated)	☐	☐
3.2	Set 'Require Client Certificates' to 'Required' (Manual)	☐	☐
3.3	Set 'Turn on script execution' to 'RemoteSigned' (Automated)	☐	☐
3.4	Set 'Turn on Administrator Audit Logging' to 'True' (Automated)	☐	☐
3.5	Set 'Enable automatic replies to remote domains' to 'False' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.6	Set 'Allow basic authentication' to 'False' (Automated)	☐	☐
3.7	Set 'Enable non-delivery reports to remote domains' to 'False' (Automated)	☐	☐
3.8	Set 'Enable OOF messages to remote domains' to 'None' (Automated)	☐	☐
3.9	Set 'Enable automatic forwards to remote domains' to 'False' (Automated)	☐	☐
3.10	Set 'Enable S/MIME for OWA 2010' to 'True' (Automated)	☐	☐
3.11	Set mailbox 'Turn on Administrator Audit Logging' to 'True' (Automated)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
03-24-2015	1.1.0	Fixed numbering related to item 2.11 - Ticket #8
03-24-2015	1.1.0	Updated audit procedure for item 2.12 (VOIPSecurity=Secured) - Ticket #30
03-24-2015	1.1.0	Updated audit procedure for item 2.8 (DevicePasswordExpiration=90) - Ticket #29
03-24-2015	1.1.0	Updated audit procedure for item 2.7 (DevicePasswordHistory=4)- Ticket #28
03-24-2015	1.1.0	Updated audit procedure for item 2.6 (AllowSimpleDevicePassword=False)- Ticket #27
03-24-2015	1.1.0	Updated audit procedure for item 2.5 (RetainDeletedItemsUntilBackup=True)- Ticket #26
03-24-2015	1.1.0	Updated audit procedure for item 2.4 - Ticket #25
03-24-2015	1.1.0	Change 2.2 from Scored to Not Scored - Ticket #23
03-24-2015	1.1.0	Change 2.1 from Scored to Not Scored - Ticket #22
03-24-2015	1.1.0	Updated audit procedure for item 1.17 - Ticket #21
03-24-2015	1.1.0	Updated audit procedure for item 1.16 (ConnectivityLogEnabled=True) - Ticket #20
03-24-2015	1.1.0	Updated audit procedure for item 1.12