

# CIS Microsoft Exchange Server 2019 Benchmark

v1.0.0 - 06-30-2023

# 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

<b>Terms of Use</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Overview</b> .....	<b>5</b>
<b>Intended Audience</b> .....	<b>5</b>
<b>Consensus Guidance</b> .....	<b>6</b>
<b>Typographical Conventions</b> .....	<b>7</b>
<b>Recommendation Definitions</b> .....	<b>8</b>
<b>Title</b> .....	<b>8</b>
<b>Assessment Status</b> .....	<b>8</b>
<b>Automated</b> .....	<b>8</b>
<b>Manual</b> .....	<b>8</b>
<b>Profile</b> .....	<b>8</b>
<b>Description</b> .....	<b>8</b>
<b>Rationale Statement</b> .....	<b>8</b>
<b>Impact Statement</b> .....	<b>9</b>
<b>Audit Procedure</b> .....	<b>9</b>
<b>Remediation Procedure</b> .....	<b>9</b>
<b>Default Value</b> .....	<b>9</b>
<b>References</b> .....	<b>9</b>
<b>CIS Critical Security Controls® (CIS Controls®)</b> .....	<b>9</b>
<b>Additional Information</b> .....	<b>9</b>
<b>Profile Definitions</b> .....	<b>10</b>
<b>Acknowledgements</b> .....	<b>12</b>
<b>Recommendations</b> .....	<b>13</b>
<b>1 Edge Transport Server</b> .....	<b>13</b>
1.1 (L1) Ensure 'Enable sender ID agent' is configured (Automated) .....	14
1.2 (L1) Ensure 'Configure sender filtering' is set to 'Enabled' (Automated).....	16
1.3 (L1) Ensure 'Sender reputation' is configured (Automated).....	18
1.4 (L1) Ensure 'Blank sender field' is configured (Automated) .....	20
1.5 (L1) Ensure 'Spam quarantine mailbox exists' is set to '' (Manual).....	22
1.6 (L1) Ensure 'SCL Quarantine' is 'Enabled' (Automated).....	24
1.7 (L1) Ensure 'Nonexistent recipients' is set to 'True' (Manual) .....	26
1.8 (L1) Ensure 'Attachment Filtering Agent' is configured (Automated).....	28
1.9 (L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated) .....	32
1.10 (L1) Ensure 'Transport Pickup Directory Path' is not set (Automated) .....	34
1.11 (L1) Ensure 'Exchange recipient filter' is set to 'True' (Automated).....	36

1.12 (L1) Ensure 'Internet-facing receive connectors' is set to 'Tls, BasicAuth, BasicAuthRequireTls' (Automated) .....	38
<b>2 Mailbox Server .....</b>	<b>40</b>
<b>2.1 Database and Retention .....</b>	<b>40</b>
2.1.1 (L1) Ensure 'Mailbox quotas: Issue warning at' is set to " (Automated).....	41
2.1.2 (L1) Ensure 'Retain deleted items for the specified number of days' is set to '14' (Automated) .....	43
2.1.3 (L1) Ensure 'Mailbox quotas: Prohibit send and receive at' is set to " (Automated) .....	45
2.1.4 (L1) Ensure 'Mailbox quotas: Prohibit send at' is set to " (Automated).....	47
2.1.5 (L1) Ensure 'Keep deleted mailboxes for the specified number of days' is set to '30' (Automated)....	49
2.1.6 (L1) Ensure 'Do not permanently delete items until the database has been backed up' is set to 'True' (Automated) .....	51
<b>2.2 Mail Flow .....</b>	<b>53</b>
2.2.1 (L1) Ensure 'Transport Pickup Directory Path' is not set (Automated) .....	54
2.2.2 (L1) Ensure 'Maximum send size: Organization level' is set to '25' (Automated) .....	56
2.2.3 (L1) Ensure 'Maximum receive size: Organization level' is set to '25' (Automated).....	58
2.2.4 (L1) Ensure 'Maximum send size: Connector level' is set to '25' (Automated) .....	60
2.2.5 (L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated) .....	62
2.2.6 (L1) Ensure 'Send connector timeout' is set to '10' (Automated).....	64
2.2.7 (L1) Ensure 'Receive connector timeout' is set to '5' (Automated) .....	66
2.2.8 (L1) Ensure 'External send connector authentication: DNS routing' is set to 'True' (Automated) .....	68
2.2.9 (L1) Ensure 'External send connector authentication: IgnoreStartTls' is set to 'False' (Automated) .....	70
2.2.10 (L1) Ensure 'External send connector authentication: Domain security' is set to 'True' (Automated) .....	72
<b>2.3 Recipient and Client .....</b>	<b>74</b>
2.3.1 (L2) Ensure 'Enable non-delivery reports to remote domains' is set to 'False' (Automated).....	75
2.3.2 (L2) Ensure 'Enable OOF messages to remote domains' is set to 'None' (Automated) .....	77
2.3.3 (L1) Ensure 'Enable automatic replies to remote domains' is set to 'False' (Automated) .....	78
2.3.4 (L1) Ensure 'Enable automatic forwards to remote domains' is set to 'False' (Automated) .....	80
2.3.5 (L1) Ensure 'Enable S/MIME for OWA' is set to 'True' (Automated).....	82
2.3.6 (L1) Ensure 'Require client MAPI encryption' is set to 'True' (Automated) .....	84
<b>2.4 Services and Authentication .....</b>	<b>86</b>
2.4.1 (L1) Ensure 'POP3' Windows services are 'Disabled' (Automated).....	87
2.4.2 (L1) Ensure 'IMAP4' Windows services are 'Disabled' (Automated).....	89
2.4.3 (L1) Ensure 'Receive connector' is set to 'Tls' (Manual).....	91
2.4.4 (L2) Ensure 'Send Exchange Customer Experience reports' is set to 'False' (Automated).....	93
2.4.5 (L1) Ensure 'SMTP automated banner response' is set to '220 SMTP Server Ready' (Automated) .....	95
<b>3 Mobile Device Management .....</b>	<b>97</b>
3.1 (L1) Ensure 'Allow simple passwords' is set to 'False' (Automated).....	98
3.2 (L1) Ensure 'Allow unmanaged devices' is set to 'False' (Automated) .....	100
3.3 (L1) Ensure 'Enforce password history' is set to '4' or greater (Automated) .....	102
3.4 (L1) Ensure 'Minimum password length' is set to '4' or more (Automated).....	104
3.5 (L1) Ensure 'Number of attempts allowed' is set to '10' (Automated) .....	106
3.6 (L1) Ensure 'Password expiration' is set to '365' or less (Automated) .....	108
3.7 (L1) Ensure 'Refresh interval' is set to '1' (Automated).....	110
3.8 (L1) Ensure 'Require alphanumeric password' is set to 'True' (Automated) .....	112
3.9 (L1) Ensure 'Require encryption on device' is set to 'True' (Automated) .....	114
3.10 (L1) Ensure 'Require password' is set to 'True' (Automated) .....	116
3.11 (L1) Ensure 'Time without user input before password must be re-entered' is set to '15' (Automated) .....	118
<b>4 Logging .....</b>	<b>120</b>
4.1 (L1) Ensure 'Receive connector: Configure protocol logging' is set to 'Verbose' (Automated) .....	121

4.2 (L1) Ensure 'Turn on administrator audit logging' is set to " (Automated) .....	123
4.3 (L1) Ensure 'Turn on connectivity logging' is set to 'True' (Automated).....	125
4.4 (L1) Ensure 'Send connector: Configure protocol logging' is set to 'Verbose' (Automated).....	127
4.5 (L1) Ensure 'Message tracking logging' is set to 'True' (Automated).....	129
<b>Appendix: Summary Table .....</b>	<b>131</b>
<b>Appendix: Change History .....</b>	<b>136</b>

# 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 Windows Exchange Server 2019.

This secure configuration guide is based on Microsoft Windows Exchange Server 2019 and was tested against Microsoft Windows Exchange Server 2019. Both UI and PowerShell guidance will be provided when possible. Although deploying Windows Server Core with Exchange Server 2019 provides significant attack surface reduction, CIS aims to evaluate the UI and PowerShell methods on both Desktop Experience and Core systems. Server Core should be strongly considered when deploying a new Microsoft Server of any type.

To obtain the latest version of this secure configuration guide, please visit <https://www.cisecurity.org/cis-benchmarks/>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto: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 2019 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
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
< <i>italic font in brackets</i> >	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
<b>Note</b>	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 - Edge Services Security**

Items in this profile apply to the Edge Server role and exhibit one or more of the following characteristics:

- be the starting baseline for most organizations;
- 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 exhibit one or more of the following characteristics:

- be the starting baseline for most organizations;
- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - MDM Services Security**

Items in this profile apply to the Mobile Device Management and exhibit one or more of the following characteristics:

- be the starting baseline for most organizations;
- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Mailbox Services Security**

Items in this profile apply to the Mailbox Server role and exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability;
- may negatively inhibit the utility or performance of the technology; and
- limit the ability of remote management/access.

**Note:** Implementation of Level 2 requires that both Level 1 and Level 2 settings are applied.

## 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:

### **Editor**

Caleb Eifert  
Jennifer Jarose  
Matthew Woods

### **Contributor**

Todd Curley  
Ryan Elder  
Niven Sawmynaden  
Andre Zufferey

# Recommendations

## 1 Edge Transport Server

This section contains recommendations for the Edge Transport Server.

Organizations that have adopted a third-party party solution to handle Edge related transport services for their mail flow may consider opting out of this section.

Implementation of the Edge Transport recommendations should be considered on a case-by-case basis. The Benchmark is written in a way that will allow organizations to adopt built in services within Exchange that do not have access to these additional third-party party services.

## 1.1 (L1) Ensure 'Enable sender ID agent' is configured (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. Rejecting messages that have evidence of spoofing will reduce the possibility of users falling victim to phishing attacks.

### Impact:

Some legitimate messages may be blocked.

### Audit:

Execute the below cmdlet:

```
Get-SenderIdConfig | fl Name,Enabled,SpoofedDomainAction
```

- Ensure `Enabled` is set to `True`
- Ensure `SpoofedDomainAction` is set to `Reject`

### Remediation:

To implement the recommended state, execute the below cmdlet:

```
Set-SenderIdConfig -Enabled $true -SpoofedDomainAction Reject
```

### Default Value:

Enabled: `True`

SpoofedDomainAction: `StampStatus`

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.2 (L1) Ensure 'Configure sender filtering' is set to 'Enabled' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

Sender filtering compares a list of blocked senders that's maintained by the Exchange administrator.

**Note:** For more information on how to create the list for blocked senders, please visit: [Use the Exchange Management Shell to configure blocked senders and domains for sender filtering](#)

**Note #2:** Sender filtering is enabled (by default) on a system performing the Edge Transport server role.

### 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 implement the recommended state, execute the following PowerShell cmdlet:

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

### Default Value:

True

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-senderfilterconfig?view=exchange-ps#-enabled>
2. <https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/sender-filtering-procedures?view=exchserver-2019#use-the-exchange-management-shell-to-configure-blocked-senders-and-domains-for-sender-filtering>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.3 (L1) Ensure 'Sender reputation' is configured (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

Sender reputation filters all messages from all receive connectors on that system and only messages from external sources are filtered. External sources are defined as non-authenticated sources, which are considered anonymous internet sources.

This recommendation configures several parameters:

- `Enabled` parameter enables or disables sender reputation on the Exchange server.
- `SenderBlockingEnabled` parameter specifies whether sender reputation blocks senders whose sending system fails an open proxy test.
- `OpenProxyDetectionEnabled` parameter specifies whether sender reputation tries to determine whether the sender's address is an open proxy by connecting to the originating IP address.
- `SrlBlockThreshold` specifies the SRL rating that must be met or exceeded for sender reputation to block a sender.

### Rationale:

Sender reputation is part of the Microsoft Exchange anti-spam functionality that can help with the filtering and blocking of spam messages. Malicious actors can exploit open proxy servers to send spam, launch attacks, or engage in other attacks while masking their identity. When Exchange checks if the sender is an OpenProxy this can help mitigate attacks from those types of senders.

### Impact:

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

**Warning:** If a proxy server for outbound Internet access is used, the properties of the proxy server must be defined by using the `ProxyServerName`, `ProxyServerPort`, and `ProxyServerType` parameters.

**Note:** The values of `OpenProxyDetectionEnabled` and `SenderBlockingEnabled` can both be set to `$true`, but they both can't be set to `$false`. If one value is `$true` and the other is `$false`, and the `$true` value is changed to `$false`, the parameter that was previously `$false` will automatically change to `$true`.

**Note #2:** Open proxy server detection requires the following open outbound TCP ports: 23, 80, 1080, 1081, 3128, and 6588.

## Audit:

Execute the following cmdlet and ensure `SenderBlockingEnabled` and `OpenProxyDetectionEnabled` are set to `True` and `SrlBlockThreshold` is set to 6:

```
Get-SenderReputationConfig | fl  
SenderBlockingEnabled,OpenProxyDetectionEnabled,SrlBlockThreshold
```

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SenderReputationConfig -Enabled $true -SenderBlockingEnabled $true -  
OpenProxyDetectionEnabled $true -SrlBlockThreshold 6
```

## Default Value:

`SenderBlockingEnabled True`

`OpenProxyDetectionEnabled True`

`SrlBlockThreshold 7`

## References:

1. <https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/sender-reputation?view=exchserver-2019>
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-senderreputationconfig?view=exchange-ps#-openproxydetectionenabled>
3. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-senderreputationconfig?view=exchange-ps#-senderblockingenabled>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.4 (L1) Ensure 'Blank sender field' is configured (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

When the Sender Filter Agent takes on messages from blocked senders or domains, the Action parameter is what is used when deciding what to do with these messages.

### Rationale:

Anonymous emails (messages with blank sender fields) cannot be replied to. Emails that are sent with blank sender fields could be trying to hide their true origin and allows them to avoid responses and possibly spam receivers of the message. It is less risky and more resource-efficient to filter these messages upon receipt rather than forwarding them to be evaluated and risking possible infection.

### Impact:

Anonymous emails are automatically rejected

### Audit:

Execute the following cmdlet and ensure `Action` is set to `Reject` and `BlankSenderBlockingEnabled` is set to `True` :

```
Get-SenderFilterConfig | fl Name, Action, BlankSenderBlockingEnabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SenderFilterConfig -Action Reject -BlankSenderBlockingEnabled $true
```

### Default Value:

`Action` `Reject`

`BlankSenderBlockingEnabled` `False`

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-senderfilterconfig?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.5 (L1) Ensure 'Spam quarantine mailbox exists' is set to '(Manual)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

This parameter is used to specify an SMTP address to be used as a spam quarantine mailbox.

**Note:** All messages that are equal to or greater than the value set in the `SCLQuarantineEnabled` parameter are sent to the SMTP address set in the `QuarantineMailbox` parameter.

### Rationale:

A spam quarantine mailbox is necessary to temporarily host filtered messages for evaluation by administrators or users. Having an archive such as this can be useful to recover messages that have been wrongfully filtered, prevent data loss, and can be helpful in providing a base of analysis so that refinements can be made to the filter in the future.

### Impact:

This mailbox should be monitored by an administrator for potential of blocking sender.

### Audit:

Execute the following cmdlet and ensure `QuarantineMailbox` is set to a valid working e-mail address.

```
Get-ContentFilterConfig | Select Name, QuarantineMailbox
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ContentFilterConfig -QuarantineMailbox '<QuarantineMailbox SmtAddress>'
```

### Default Value:

Not Configured.

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-contentfilterconfig?view=exchange-ps>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.6 (L1) Ensure 'SCL Quarantine' is 'Enabled' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

Spam Confidence Level (SCL) is a rating assigned to incoming email messages by the Content Filter agent in Exchange Server. It is a measure of the likelihood that an email is spam based on various content analysis techniques and spam detection algorithms. The SCL value ranges from 0 to 9, with 9 being the highest level of confidence that the email is spam.

Ensure `SCLQuarantineEnabled` is set to `True`

### Rationale:

E-mails with a high Spam Confidence Level (SCL) will be quarantined. This involves moving it to a designated quarantine e-mail address, separating it from the regular inbox of the recipient in order to prevent users interacting with malicious e-mails.

### Impact:

False positives may occur when setting `SCLQuarantineThreshold` to lower values.

### Audit:

Execute the following cmdlet and ensure `SCLQuarantineEnabled` is set to `True` and `SCLQuarantineThreshold` is set to 6 or lower.

```
Get-ContentFilterConfig | fl Name,QuarantineMailbox,SCL*
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ContentFilterConfig -SCLQuarantineEnabled $true -SCLRejectThreshold 8 -  
SCLQuarantineThreshold 6
```

**NOTE:** The `SCLRejectThreshold` must be greater than the `SCLQuarantineThreshold` when enabling the Quarantine and is why it is changed in this instance.

### Default Value:

`SCLQuarantineEnabled`: `False`

`SCLQuarantineThreshold`: 9

`SCLRejectThreshold`: 7

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-contentfilterconfig?view=exchange-ps>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.7 (L1) Ensure 'Nonexistent recipients' is set to 'True' (Manual)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

This parameter is used to decide if messages whose recipient doesn't exist in the organization are blocked. When this parameter is set to `$true`, the Recipient Filter Agent blocks these messages.

**Note:** The `Set-RecipientFilterConfig` cmdlet must be enabled

### Rationale:

Spam originators may use a technique that involves first creating fabricated names, and then monitors for rejected emails due to non-existent recipients. Emails with names who are not rejected are then used for future spam mailings. To deprive the spam originator of valuable information, it is recommended to receive all messages, then evaluate and dispose of them as deemed necessary.

### Impact:

Some legitimate messages might be blocked.

### Audit:

Execute the following cmdlet and ensure `RecipientValidationEnabled` is set to `True`:

```
Get-RecipientFilterConfig | Select Name, RecipientValidationEnabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RecipientFilterConfig -RecipientValidationEnabled $true
```

### Default Value:

False

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-recipientfilterconfig?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## *1.8 (L1) Ensure 'Attachment Filtering Agent' is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Edge Services Security

### **Description:**

The attachment filtering on Edge Transport servers restricts attachments that users receive in email messages. Attachment filtering is performed by the Attachment Filtering agent, which is available only on Edge Transport servers, and is unchanged from Exchange Server 2010.

Ensure the `Attachment Filtering Agent` is Enabled, and the extension filtering list is configured to the desired state.

### **Rationale:**

Attachment filtering will allow the blocking of file extensions that are regularly abused by bad actors for nefarious purposes, including phishing, malware distribution, and macros. The list of extensions in the audit and remediation sections includes a collection found in the CIS Microsoft 365 Benchmark, Microsoft Office Benchmark, DISA STIG, and the Exchange Server defaults.

### **Impact:**

Attachments on emails that match the filtering list will be removed and replaced with a text file. The original message will be sent to the recipient along with the replaced attachment. This is the default behavior.

## Audit:

To ensure the Attachment Filtering Agent is enabled execute the below cmdlet:

```
Get-TransportAgent "Attachment Filtering Agent"
```

To ensure the list of blocked extensions matches the recommended state execute `Get-AttachmentFilterEntry` and compare it against the list below or run the following script:

```
$attachmentExtensions = @(
    "*.ace", "*.ade", "*.adp", "*.ani", "*.app", "*.appx", "*.arj", "*.asx",
    "*.bas", "*.bat", "*.cab", "*.chm",
    "*.cmd", "*.com", "*.cpl", "*.crt", "*.csh", "*.dbf", "*.dcr", "*.deb",
    "*.dex", "*.dif", "*.dir", "*.dll",
    "*.doc", "*.dot", "*.docm", "*.elf", "*.exe", "*.fxp", "*.hlp", "*.hta",
    "*.htc", "*.htm", "*.html", "*.img",
    "*.inf", "*.ins", "*.iso", "*.isp", "*.jar", "*.jnlp", "*.js", "*.jse",
    "*.kext", "*.ksh", "*.lha", "*.lib",
    "*.lnk", "*.lzh", "*.macho", "*.mda", "*.mdb", "*.mde", "*.mdt", "*.mdw",
    "*.mdz", "*.mht", "*.mhtml", "*.msc",
    "*.msi", "*.msix", "*.msp", "*.mst", "*.ops", "*.pcd", "*.pif", "*.plg",
    "*.ppa", "*.ppt", "*.ppam", "*.prf",
    "*.prg", "*.ps1", "*.ps11", "*.ps11xml", "*.ps1xml", "*.ps2", "*.ps2xml",
    "*.psc1", "*.psc2", "*.reg", "*.rev",
    "*.scf", "*.scr", "*.sct", "*.shb", "*.shs", "*.shtm", "*.shtml",
    "*.slk", "*.spl", "*.stm", "*.swf", "*.sys",
    "*.uif", "*.url", "*.vb", "*.vbe", "*.vbs", "*.vxd", "*.wsc", "*.wsf",
    "*.wsh", "*.xlam", "*.xla", "*.xlc",
    "*.xll", "*.xls", "*.xlsm", "*.xlt", "*.xlw", "*.xml", "*.xnk", "*.xz",
    "*.z"
)

# Get the existing attachment filter entries
$existingEntries = Get-AttachmentFilterEntry

$missingCount = 0

# Iterate over the master list and check if each extension is present in the
attachment filter
foreach ($extension in $attachmentExtensions) {
    $found = $existingEntries | Where-Object { $_.Name -eq $extension }

    if (!$found) {
        $missingCount++
        Write-Host "Extension $extension is missing from the attachment
filter list." -ForegroundColor Yellow
    }
}

if ($missingCount -eq 0) {
    Write-Host "All extensions from the reference list are present." -
ForegroundColor Green
}
```

**NOTE:** This list has been collected from various CIS Benchmarks and includes the Exchange Defaults. It is not exhaustive. This and the remediation script can be modified for the organization's needs or exceptions.

## Remediation:

Execute the following cmdlet to enable the Filtering Agent:

```
Enable-TransportAgent "Attachment Filtering Agent"
```

Execute the bellow script to create the desired attachment filtering state:

```
$attachmentExtensions = @(
    *.ace, *.ade, *.adp, *.ani, *.app, *.appx, *.arj, *.asx,
    *.bas, *.bat, *.cab, *.chm,
    *.cmd, *.com, *.cpl, *.crt, *.csh, *.dbf, *.dcr, *.deb,
    *.dex, *.dif, *.dir, *.dll,
    *.doc, *.dot, *.docm, *.elf, *.exe, *.fxp, *.hlp, *.hta,
    *.htc, *.htm, *.html, *.img,
    *.inf, *.ins, *.iso, *.isp, *.jar, *.jnlp, *.js, *.jse,
    *.kext, *.ksh, *.lha, *.lib,
    *.lnk, *.lzh, *.macho, *.mda, *.mdb, *.mde, *.mdt, *.mdw,
    *.mdz, *.mht, *.mhtml, *.msc,
    *.msi, *.msix, *.msp, *.mst, *.ops, *.pcd, *.pif, *.plg,
    *.ppa, *.ppt, *.ppam, *.prf,
    *.prg, *.ps1, *.ps11, *.ps11xml, *.ps1xml, *.ps2, *.ps2xml,
    *.psc1, *.psc2, *.reg, *.rev,
    *.scf, *.scr, *.sct, *.shb, *.shs, *.shtm, *.shtml,
    *.slk, *.spl, *.stm, *.swf, *.sys,
    *.uif, *.url, *.vb, *.vbe, *.vbs, *.vxd, *.wsc, *.wsf,
    *.wsh, *.xlam, *.xla, *.xlc,
    *.xll, *.xls, *.xlsm, *.xlt, *.xlw, *.xml, *.xnk, *.xz,
    *.z
)

foreach ($extension in $attachmentExtensions) {
    $result = Add-AttachmentFilterEntry -Name $extension -Type FileName -
ErrorAction SilentlyContinue

    if ($result) {
        Write-Host "Successfully added attachment $extension" -
ForegroundColor Green
    } else {
        Write-Host "Attachment $extension already exists in the list." -
ForegroundColor Red
    }
}
```

## Default Value:

By default these extensions are blocked in Exchange:

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

## References:

1. <https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/attachment-filtering-procedures?view=exchserver-2019>
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/add-attachmentfilterentry?view=exchange-ps>
3. <https://learn.microsoft.com/en-us/deployoffice/compat/office-file-format-reference>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>9.6 Block Unnecessary File Types</b> Block unnecessary file types attempting to enter the enterprise's email gateway.			
v7	<b>0.0 Explicitly Not Mapped</b> Explicitly Not Mapped			

## 1.9 (L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

This setting limits the size of a message a user can receive. Receive size includes the header 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 25:

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

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 25MB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Receive Connectors" tab.
3. Double-click on the receive connector to be modified.
4. Change the `Maximum receive message size (MB)` : to 25 and click Save.

**Default Value:**

36 MB (37,748,736 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/message-size-limits?view=exchserver-2019>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.10 (L1) Ensure 'Transport Pickup Directory Path' is not set (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

The Pickup directory is used by the Transport service on Mailbox servers and Edge Transport servers to insert message files directly into the transport pipeline. When properly formatted email message files are copied to the Pickup directory, they are submitted for delivery automatically. It is a legacy feature that can be used by administrators for mail flow testing, or by applications that must create and submit their own messages.

Ensure `PickupDirectoryPath` is set to `$null`

### Rationale:

Disabling the Pickup directory is recommended to prevent potential abuse by attackers or insiders seeking to exploit side channel attacks. Dropping a file in the Pickup folder bypasses the normal authentication process of Exchange, creating a risk of sensitive data leakage or malicious email distribution through this unauthenticated side channel.

### Impact:

The directory will be unavailable for testing purposes unless an administrator explicitly enables it and then later disables it. If an application requires access to this directory, then additional controls should be enabled such as restricting NTFS permissions on the folder.

### Audit:

Execute the following cmdlet and ensure `PickupDirectoryPath` is set to `$null` or is blank:

```
Get-TransportService | fl Identity,PickupDirectoryPath
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet to disable the Pickup Directory on the Edge Transport server:

```
Get-TransportService | Set-TransportService -PickupDirectoryPath $null
```

### Default Value:

%programfiles%\Microsoft\Exchange Server\V15\TransportRoles\Pickup

**References:**

1. <https://learn.microsoft.com/en-us/exchange/pickup-directory-and-replay-directory-exchange-2013-help>
2. <https://learn.microsoft.com/en-us/exchange/mail-flow/mail-flow?view=exchserver-2019>
3. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-transportservice?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.11 (L1) Ensure 'Exchange recipient filter' is set to 'True' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

This policy setting specifies whether the Recipient Filter agent is enabled on the system. The recipient filter uses a recipient block list to identify messages that aren't allowed to enter the organization. The recipient filter also uses the local recipient directory to reject messages sent to invalid recipients.

### Rationale:

Spam consumes a large amount of network bandwidth and server capacity. In addition, it is often the source of malicious software. Rejecting messages that have evidence of spoofing will reduce the possibility of users falling victim to phishing attacks.

### Impact:

Legitimate email could be blocked by the agent.

**Note:** The recipient Filter agent is available on Mailbox servers, but it shouldn't be configured. When recipient filtering on a Mailbox server detects one invalid or blocked recipient in a message that contains other valid recipients, the message is rejected.

### Audit:

Execute the following cmdlet and ensure Enabled is set to `$true`:

```
Get-RecipientFilterConfig | Select Name, Enabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RecipientFilterConfig -Enabled $true
```

### Default Value:

True

### References:

1. <https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/antispam-protection?view=exchserver-2019#antispam-agents-on-edge-transport-servers>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 1.12 (L1) Ensure 'Internet-facing receive connectors' is set to 'Tls, BasicAuth, BasicAuthRequireTLS' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security

### Description:

This policy setting configures the advertised and accepted authentication mechanisms for the receive connector.

The primary function of receive connectors in the transport service is to accept authenticated and encrypted Simple Mail Transfer Protocol (SMTP) connections from other transport services on the local Mailbox server or remote Mailbox servers in the organization.

**Note:** Some available values have dependencies and exclusions:

- `None` is not compatible with other values.
- `BasicAuthRequireTLS` requires `BasicAuth` and `Tls`.
- `ExternalAuthoritative` can only be combined with `Tls`.
- `Tls` is required when `RequireTLS` parameter is `$true`.
- `ExternalAuthoritative`, requires `PermissionGroups` parameter to be `ExchangeServers`.

### Rationale:

Configuring this setting enables the encryption of email between servers. This reduces the risk of eavesdropping, interception, and alteration of the email.

### Impact:

There should be no impact to mail flow. If TLS connection is not established, BasicAuth will be used.

### Audit:

Execute the following cmdlet and ensure `AuthMechanism` is set to `Tls, BasicAuth, BasicAuthRequireTLS`:

```
Get-ReceiveConnector | Select Name, Identity, AuthMechanism
```

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector -Identity <'IdentityName'> -AuthMechanism 'Tls, BasicAuth, BasicAuthRequireTLS'
```

**Note:** If more than one receive connector exists on the Edge Transport server, run this command to update all receive connectors.

```
Get-ReceiveConnector | Set-ReceiveConnector -AuthMechanism 'Tls, BasicAuth, BasicAuthRequireTLS'
```

## Default Value:

N/A

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-receiveconnector?view=exchange-ps#-authmechanism>
2. <https://learn.microsoft.com/en-us/exchange/mail-flow/connectors/receive-connectors?view=exchserver-2019#default-receive-connectors-in-the-transport-service-on-mailbox-servers>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## **2 Mailbox Server**

This section contains recommendations for the server assigned the Mailbox role in Exchange Server 2019.

### **2.1 Database and Retention**

This section contains recommendations related to Database and Retention configuration.

## 2.1.1 (L1) Ensure 'Mailbox quotas: Issue warning at' is set to " (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can automatically warn mailbox users that their mailbox is approaching its storage limit. It's suggested that this warning be set up when 90% of the mailbox size has been reached. For example, if the mailbox size is 100GB, set the warning to 90GB or 94,371,840 KB.

A value between 0 and 2,147,483,647 KB (2.1 terabytes) can be set depending on the user's mailbox size.

### Rationale:

Unlimited mailbox sizes can cause the Exchange database to grow uncontrollably and consume all available disk space, potentially preventing the database from mounting properly. This can disrupt not only email services, but also other security measures that depend on timely communication.

### Impact:

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

### Audit:

Execute the following cmdlet and ensure `IssueWarningQuota` is set to `<value>KB`:

```
Get-MailboxDatabase "Mailbox Database" | fl -property IssueWarningQuota
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase "Mailbox Database" -IssueWarningQuota <value>KB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Change `Issue a warning at (GB) : to <value>` and click Save.

**Default Value:**

1.899 GB (2,039,480,320 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mailboxdatabase?view=exchange-ps#-issuewarningquota>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.1.2 (L1) Ensure 'Retain deleted items for the specified number of days' is set to '14' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting specifies how long deleted messages are retained before they are permanently removed from the database.

### Rationale:

Defining a reasonable retention period facilitates recovering accidentally deleted messages while controlling the volume of storage that retained messages require.

### Impact:

None - This is the default behavior.

### Audit:

Execute the following PowerShell cmdlet and ensure DeletedItemRetention is set to 14:

```
Get-MailboxDatabase "Mailbox Database" | fl -property DeletedItemRetention
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase "Mailbox Database" -DeletedItemRetention 14
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Change `Keep deleted items for (days)`: to 14 and click Save.

### Default Value:

14

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mailboxdatabase?view=exchange-ps#-deleteditemretention>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.4 <u>Enforce Data Retention</u></b> Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	●	●	●
v7	<b>0.0 <u>Explicitly Not Mapped</u></b> Explicitly Not Mapped			

## 2.1.3 (L1) Ensure 'Mailbox quotas: Prohibit send and receive at' is set to " (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can automatically prevent users from sending and receiving e-mail messages after their mailbox size reaches the specified limit. It's suggested that this warning be set up when 98% of the mailbox size has been reached. For example, if the mailbox size is 100 GB, set the warning to 98 GB or 102,760,448 KB.

A value between 0 and 2,147,483,647 KB (2.1 terabytes) can be set depending on the user's mailbox size.

### Rationale:

Unlimited mailbox sizes can cause the Exchange database to grow uncontrollably and consume all available disk space, potentially preventing the database from mounting properly. This can disrupt not only email services but also other security measures that depend on timely communication.

### 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 `<value>`:

```
Get-MailboxDatabase "Mailbox Database" | fl -property  
ProhibitSendReceiveQuota
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase "Mailbox Database" -ProhibitSendReceiveQuota <value>GB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Change `Prohibit send and receive at (GB):` to `<value>` and click Save.

**Default Value:**

2.3 GB (2,469,396,480 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mailboxdatabase?view=exchange-ps#-prohibitsendreceivequota>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.1.4 (L1) Ensure 'Mailbox quotas: Prohibit send at' is set to " (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can automatically prevent users from sending new e-mail messages after their mailboxes reach a specified limit. It's suggested that this warning be set up when 95% of the mailbox size has been reached. For example, if the mailbox size is 100 GB, set the warning to 95 GB or 99,614,720 KB.

A value between 0 and 2,147,483,647 KB (2.1 terabytes) can be set depending on the user's mailbox size.

### Rationale:

Unlimited mailbox sizes can cause the Exchange database to grow uncontrollably and consume all available disk space, potentially preventing the database from mounting properly. This can disrupt not only email services but also other security measures that depend on timely communication.

### 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 `<value>`:

```
Get-MailboxDatabase "Mailbox Database" | fl -property ProhibitSendQuota
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase "Mailbox Database" -ProhibitSendQuota <value>
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Change `Prohibit send at (GB)`: to `<value>` and click Save.

**Default Value:**

2 GB (2,147,483,648 bytes)

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.1.5 (L1) Ensure 'Keep deleted mailboxes for the specified number of days' is set to '30' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting specifies how long deleted mailboxes are retained before they are permanently removed from the database.

### Rationale:

Defining a reasonable retention period facilitates recovering accidentally or deliberately deleted mailboxes while controlling the volume of storage that retained mailboxes require.

### Impact:

None - This is the default behavior.

### Audit:

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

```
Get-Mailboxdatabase "Mailbox Database" | fl -property MailboxRetention
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

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

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Change `Keep deleted mailboxes for (days)`: to `30` and click Save.

### Default Value:

30

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mailboxdatabase?view=exchange-ps#-mailboxretention>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.4 <u>Enforce Data Retention</u></b> Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	●	●	●
v7	<b>0.0 <u>Explicitly Not Mapped</u></b> Explicitly Not Mapped			

## 2.1.6 (L1) Ensure 'Do not permanently delete items until the database has been backed up' is set to 'True' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can prohibit items from being 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:

Additional storage space will be required until any pending items are permanently deleted.

If using a 3rd party backup solution that does not set the backup parameters on the Mailbox database as it is backed up then this setting should be skipped. Native backup solutions will update the database bits properly, allowing for the `RetainDeletedItemsUntilBackup` parameter work as intended.

Failure to evaluate the organization's backup solution in conjunction with this setting will result in increased database growth. To see the backup parameters mentioned above

```
run Get-MailboxDatabase | fl *backup*
```

### Audit:

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

```
Get-MailboxDatabase "Mailbox Database" | fl -property  
RetainDeletedItemsUntilBackup
```

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MailboxDatabase "Mailbox Database" -RetainDeletedItemsUntilBackup $true
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Databases" tab.
3. Double-click the database and go to the "Limits" settings.
4. Ensure the `Don't permanently delete items until the database is backed up` box is checked and click `Save`.

## Default Value:

False

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.4 <u>Enforce Data Retention</u></b> Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.			
v7	<b>0.0 <u>Explicitly Not Mapped</u></b> Explicitly Not Mapped			

## **2.2 Mail Flow**

This section contains recommendations related to configuring various connectors impacting mail flow.

## 2.2.1 (L1) Ensure 'Transport Pickup Directory Path' is not set (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

The Pickup directory is used by the Transport service on Mailbox servers and Edge Transport servers to insert message files directly into the transport pipeline. When properly formatted email message files are copied to the Pickup directory, they are submitted for delivery automatically. It is a legacy feature that can be used by administrators for mail flow testing, or by applications that must create and submit their own messages.

Ensure `PickupDirectoryPath` is set to `$null`

### Rationale:

Disabling the Pickup directory is recommended to prevent potential abuse by attackers or insiders seeking to exploit side channel attacks. Dropping a file in the Pickup folder bypasses the normal authentication process of Exchange, creating a risk of sensitive data leakage or malicious email distribution through this unauthenticated side channel.

### Impact:

The directory will be unavailable for testing purposes unless an administrator explicitly enables it and then later disables it. If an application requires access to this directory, then additional controls should be enabled such as restricting NTFS permissions on the folder.

### Audit:

Execute the following cmdlet and ensure `PickupDirectoryPath` is set to `$null` or is blank:

```
Get-TransportService | fl Identity,PickupDirectoryPath
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet to disable the Pickup Directory on all servers with the Mailbox role

```
Get-TransportService | Set-TransportService -PickupDirectoryPath $null
```

**NOTE:** Edge Transport Servers must be configured directly.

### Default Value:

%programfiles%\Microsoft\Exchange Server\V15\TransportRoles\Pickup

**References:**

1. <https://learn.microsoft.com/en-us/exchange/pickup-directory-and-replay-directory-exchange-2013-help>
2. <https://learn.microsoft.com/en-us/exchange/mail-flow/mail-flow?view=exchserver-2019>
3. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-transportservice?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.2 (L1) Ensure 'Maximum send size: Organization level' is set to '25' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting limits the size of a message a user can send. Send size includes the 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 limits the impact that a malicious user or a system 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 25:

```
Get-TransportConfig | fl -property MaxSendSize
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-TransportConfig -MaxSendSize 25MB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Send Connectors" tab.
3. Click on "..." and select "Organization Transport Settings".
4. Change the `Maximum send message size (MB)` : to 25 and click Save.

**Default Value:**

10 MB (10,485,760 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/message-size-limits?view=exchserver-2019>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.3 (L1) Ensure 'Maximum receive size: Organization level' is set to '25' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can limit the size of messages received by the user. The message size includes the header, body, and any attachments for the email.

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 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 25:

```
Get-TransportConfig | fl -property MaxReceiveSize
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-TransportConfig -MaxReceiveSize 25MB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Receive Connectors" tab.
3. Click on "... " and select "Organization Transport Settings"
4. Change the `Maximum receive message size (MB)` : to 25 and click Save.

**Default Value:**

10 MB (10,485,760 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/message-size-limits?view=exchserver-2019#organizational-limits>
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-transportconfig?view=exchange-ps#-maxreceivesize>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.4 (L1) Ensure 'Maximum send size: Connector level' is set to '25' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting can limit the size of messages that are sent by the user at the connector level. The message size includes the header, body, and any attachments for the email.

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 25:

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

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SendConnector "Connection to Contoso.com" -MaxMessageSize 25MB
```

OR

Perform the following actions via the GUI:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Send Connectors" tab.
3. Double-click on the send connector to be modified.
4. Change the `Maximum send message size (MB)`: to 25 and click Save.

**Default Value:**

10 MB (10,485,760 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/message-size-limits?view=exchserver-2019#organizational-limits>
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-sendconnector?view=exchange-ps#-maxmessagesize>

## 2.2.5 (L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This setting limits the size of a message a user can receive. Receive size includes the header 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 25:

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

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 25MB
```

To set `MaxMessageSize` on all receive connectors this command can be executed:

```
Get-ReceiveConnector | Set-ReceiveConnector -MaxMessageSize 25MB
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Receive Connectors" tab.
3. Double-click on the receive connector to be modified.
4. Change the `Maximum receive message size (MB)`: to 25 and click Save.

**Default Value:**

36 MB (37,748,736 bytes)

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/message-size-limits?view=exchserver-2019>

## 2.2.6 (L1) Ensure 'Send connector timeout' is set to '10' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This parameter controls the number of idle minutes before the connection to the Send connector is dropped, even if data is being actively transmitted.

**Note:** The `ConnectionTimeout` parameter must be higher than the `ConnectionInactivityTimeout` parameter.

### Rationale:

Connections may suffer from delays in message transfer once established. In order to allow new connections to be established, the timeout period should be reduced so that connections are not maintained for unnecessary periods of time.

### Impact:

Valid connections could be dropped.

### Audit:

Execute the following cmdlet and ensure `ConnectionInactivityTimeOut` is set to 00:10:00:

```
Get-SendConnector | Select Name, Identity, ConnectionInactivityTimeOut
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SendConnector -Identity <'IdentityName'> -ConnectionInactivityTimeOut  
00:10:00
```

### Default Value:

00:10:00 (10 minutes)

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-sendconnector?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.7 (L1) Ensure 'Receive connector timeout' is set to '5' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This parameter controls the number of idle minutes before the connection to the Receive connector is dropped, even if data is being actively transmitted.

**Note:** The `ConnectionTimeout` parameter must be higher than the `ConnectionInactivityTimeout` parameter.

### Rationale:

Connections may suffer from delays in message transfer once established. In order to allow new connections to be established, the timeout period should be reduced so that connections are not maintained for unnecessary periods of time.

### Impact:

Valid connections could be dropped.

### Audit:

Execute the following cmdlet and ensure `ConnectionTimeout` is set to `00:05:00`:

```
Get-ReceiveConnector | Select Name, Identity, ConnectionTimeout
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector -Identity <IdentityName> -ConnectionTimeout 00:05:00
```

Repeat the procedures for each Receive connector.

### Default Value:

00:10:00 (10 minutes)

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-receiveconnector?view=exchange-ps#-connectiontimeout>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.8 (L1) Ensure 'External send connector authentication: DNS routing' is set to 'True' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting determines if DNS is used to route outbound mail via the send connector.

### Rationale:

In order to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this send connector, multiple parameters must be configured. Configuring these parameters enables the use of TLS instead of basic authentication where credentials are sent across the network in plaintext.

The following parameters are addressed in separate recommendations in this benchmark.

- `DomainSecureEnabled` to `$true`
- `IgnoreStartTLS` to `$false`

### Impact:

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

**Warning:** If a `SmartHosts` parameter is specified, the `DNSRoutingEnabled` parameter must be set to `$false`.

### Audit:

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

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

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

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

### Default Value:

True

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-sendconnector?view=exchange-ps#-dnsroutingenabled>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.2.9 (L1) Ensure 'External send connector authentication: IgnoreStartTLS' is set to 'False' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting specifies whether to ignore the StartTLS option offered by a remote sending server. StartTLS is a protocol command used to inform the email server that the email client wants to upgrade from an insecure connection to a secure one using TLS or SSL.

### Rationale:

In order to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this send connector, multiple parameters must be configured (see below).

Configuring these parameters enables the use of TLS instead of basic authentication where credentials are sent across the network in plaintext.

The following parameters are addressed in separate recommendations in this benchmark.

- DomainSecureEnabled to \$true
- DNSRoutingEnabled to \$true

### 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 `IgnoreSTARTTLS` is set to `False`:

```
Get-SendConnector "Connector Name" | fl -property IgnoreSTARTTLS
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SendConnector "Connector Name" -IgnoreSTARTTLS $false
```

### Default Value:

None

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-sendconnector?view=exchange-ps#-ignorestarttls>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## 2.2.10 (L1) Ensure 'External send connector authentication: Domain security' is set to 'True' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This setting is part of the process to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this send connector. If this parameter is enabled, the Send connector will attempt to establish a mutual Transport Layer Security (TLS) connection with remote servers when sending mail.

### Rationale:

In order to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this send connector, multiple parameters must be configured (see below).

Configuring these parameters enables the use of TLS instead of basic authentication where credentials are sent across the network in plaintext.

The following parameters are addressed in separate recommendations in this benchmark.

- `DNSRoutingEnabled` to `$true`
- `IgnoreStartTLS` to `$false`

### 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 "Connector name" | fl DomainSecureEnabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-SendConnector "Connector name" -DomainSecureEnabled $true
```

### Default Value:

True

## References:

1. [https://learn.microsoft.com/en-us/previous-versions/exchange-server/exchange-140/bb123543\(v=exchg.140\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/exchange-server/exchange-140/bb123543(v=exchg.140)?redirectedfrom=MSDN)
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-sendconnector?view=exchange-ps#-domainsecureenabled>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## **2.3 Recipient and Client**

This section contains recommendations related to Recipient and Client configuration.

### 2.3.1 (L2) Ensure 'Enable non-delivery reports to remote domains' is set to 'False' (Automated)

#### Profile Applicability:

- Level 2 - Mailbox Services Security

#### Description:

This policy setting is used to determine if the server sends non-delivery reports (also known as NDRs or bounce messages) to remote domains.

#### Rationale:

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

#### Impact:

Remote users will not receive automated non-delivery reports.

**Note:** If Microsoft Exchange is being used as HUB, this setting is applicable. If not, an exception to this recommendation might be required.

#### Audit:

Execute the following cmdlet and ensure `NDREnabled` is set to `False`:

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

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RemoteDomain "RemoteDomain" -NDREnabled $false
```

#### Default Value:

True

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-remotedomain?view=exchange-ps#-ndrenabled>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u>                      Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><u>0.0 Explicitly Not Mapped</u>                      Explicitly Not Mapped</p>			

## 2.3.2 (L2) Ensure 'Enable OOF messages to remote domains' is set to 'None' (Automated)

### Profile Applicability:

- Level 2 - Mailbox Services Security

### Description:

This policy setting is used 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 `AllowedOOFTType` is set to `None`:

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

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFTType None
```

### Default Value:

External

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 2.3.3 (L1) Ensure 'Enable automatic replies to remote domains' is set to 'False' (Automated)

#### Profile Applicability:

- Level 1 - Mailbox Services Security

#### Description:

This policy setting is used to determine if the server automatically replies to remote domains. The `AutoReplyEnabled` parameter specifies whether to allow messages that are automatic replies from client email programs in an organization (for example, automatic reply messages that are generated by rules in Outlook).

#### Rationale:

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

#### Impact:

Remote users will not receive automated replies.

**Note:** If Microsoft Exchange is being used as HUB, this setting is applicable. If not, an exception to this recommendation might be required.

#### Audit:

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

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

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RemoteDomain "RemoteDomain" -AutoReplyEnabled $false
```

#### Default Value:

False

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-remotedomain?view=exchange-ps#-autoreplyenabled>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 2.3.4 (L1) Ensure 'Enable automatic forwards to remote domains' is set to 'False' (Automated)

#### Profile Applicability:

- Level 1 - Mailbox Services Security

#### Description:

This policy setting is used to determine if the server can send automatic forwards to remote domains.

#### Rationale:

Data leakage can occur if an email with sensitive data is forwarded to an account that is not secure or sanctioned by the organization.

#### Impact:

Remote users will not receive automated forward messages.

**Note:** If Microsoft Exchange is being used as HUB, this setting is applicable. If not, an exception to this recommendation might be required.

#### Audit:

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

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

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RemoteDomain "RemoteDomain" -AutoForwardEnabled $false
```

#### Default Value:

False

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-remotedomain?view=exchange-ps#-autoforwardenabled>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 2.3.5 (L1) Ensure 'Enable S/MIME for OWA' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - Mailbox Services Security

#### Description:

This policy setting is used to control whether users are allowed to download the Secure/Multipurpose Internet Mail Extensions (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.

This is the default value.

#### Audit:

Execute the following cmdlet and ensure `SMimeEnabled` is set to `True`:

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

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

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

#### Default Value:

True

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/get-owavirtualdirectory?view=exchange-ps>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

### 2.3.6 (L1) Ensure 'Require client MAPI encryption' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - Mailbox Services Security

#### Description:

This policy setting specifies whether encryption is required for Remote Procedure call (RPC) client connections.

**Note:** This recommendation only applies if RPC over HTTP is enabled in the organization. In Exchange 2019 MAPI over HTTP is enabled by default.

#### Rationale:

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

#### 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. This is the default behavior so the impact is minimal to nothing.

#### Audit:

Execute the following PowerShell cmdlet and ensure EncryptionRequired is set to `True`:

```
Get-RpcClientAccess | fl -property EncryptionRequired
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-RpcClientAccess -Server "Server" -EncryptionRequired $true
```

#### Default Value:

True

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-rpcclientaccess?view=exchange-ps#-encryptionrequired>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

## **2.4 Services and Authentication**

This section contains recommendations related to Services and Authentication configuration.

## 2.4.1 (L1) Ensure 'POP3' Windows services are 'Disabled' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

Post Office Protocol 3 (POP3) is an email protocol for receiving email messages from a server and transferring to a client device. On Exchange Server 2019 with the Mailbox role installed, it is set to manual startup by default.

### Rationale:

POP3 is an outdated protocol that has a number of weaknesses versus MAPI and Exchange ActiveSync. POP3 can send credentials in the clear if not configured properly, has limited authentication capabilities, and a lack of proper message handling can result in misplaced or lost e-mails and folders when moving between devices. This may result in data loss for the end user. ActiveSync and MAPI, in contrast, offer superior security by default, provide an enhanced user experience, and are Microsoft's primary focus for support and improvement.

### Impact:

Devices that require POP3 to function will be unable to receive e-mail from the Exchange Server. This should not be a problem for most client applications as Outlook 2013 and newer support modern authentication methods (OAuth) and protocols.

If an organization is required to use POP3 then care must be taken to only enable POP3, the `PopEnabled` parameter, for the mailbox in question.

### Audit:

Execute the following PowerShell cmdlet and ensure the `StartType` of both `MSExchangePop3` and `MSExchangePOP3BE` are set to `Disabled`

```
Get-Service MSExchangePOP3* | ft Name,DisplayName,Status,StartType
```

### Remediation:

To implement the recommended state, execute the following PowerShell commands:

```
Stop-Service MSExchangePop3,MSExchangePop3BE  
Get-Service MSExchangePOP3,MSExchangePOP3BE | Set-Service -StartupType  
Disabled
```

### Default Value:

`StartType: Manual`

**References:**

1. <https://learn.microsoft.com/en-us/exchange/clients/pop3-and-imap4/configure-pop3?view=exchserver-2019>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## 2.4.2 (L1) Ensure 'IMAP4' Windows services are 'Disabled' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

Internet Message Access Protocol version 4 (IMAP4) is an email protocol for sending and receiving email between a client and server. Unlike POP3 it can synchronize email and folders between the client and server. On Exchange Server 2019 with the Mailbox role installed, it is set to manual startup by default.

### Rationale:

IMAP4 by default is configured to use basic authentication, which can potentially expose credentials in plain text. While it can be configured to use SSL/TLS for encryption, it is important to disable unnecessary services that duplicate the functionality of more widely used and supported protocols. ActiveSync and MAPI, in contrast, offer superior security by default, provide an enhanced user experience, and are Microsoft's primary focus for support and improvement. By disabling IMAP4, organizations can reduce their attack surface and prioritize the use of more secure and feature-rich protocols.

### Impact:

Devices that require IMAP4 to function will be unable to send or receive email from the Exchange Server. This should not be a problem for most client applications as Outlook 2013 and newer support modern authentication methods (OAuth) and protocols.

If an organization is required to use IMAP4 then care must be taken to only enable IMAP4, the `ImapEnabled` parameter, for the mailbox in question.

### Audit:

Execute the following PowerShell cmdlet and ensure the `StartType` of both `MSExchangeImap4` and `MSExchangeIMAP4BE` are set to `Disabled`

```
Get-Service MSExchangeImap4* | ft Name,DisplayName,Status,Starttype
```

### Remediation:

To implement the recommended state, execute the following PowerShell commands:

```
Stop-Service MSExchangeImap4,MSExchangeIMAP4BE  
Get-Service MSExchangeImap4,MSExchangeIMAP4BE | Set-Service -StartupType  
Disabled
```

### Default Value:

StartType: Manual

**References:**

1. <https://learn.microsoft.com/en-us/exchange/clients/pop3-and-imap4/configure-imap4?view=exchserver-2019>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 2.4.3 (L1) Ensure 'Receive connector' is set to 'TLS' (Manual)

#### Profile Applicability:

- Level 1 - Mailbox Services Security

#### Description:

This policy setting configures the advertised and accepted authentication mechanisms for the receive connector.

The primary function of receive connectors in the front-end transport service is to accept anonymous and authenticated Simple Mail Transfer Protocol (SMTP) connections in the Exchange environment.

**Note:** Some available values have dependencies and exclusions:

- `None` is not compatible with other values.
- `BasicAuthRequireTLS` requires `BasicAuth` and `Tls`.
- `ExternalAuthoritative` can only be combined with `Tls`.
- `Tls` is required when `RequireTLS` parameter is `$true`.
- `ExternalAuthoritative`, requires `PermissionGroups` parameter to be `ExchangeServers`.

#### Rationale:

Configuring this setting enables the encryption of email between client and servers. This reduces the risk of eavesdropping, interception, and alteration of the email and adds protection by encrypting the sender and recipient information that cannot be encrypted by the sender.

#### Impact:

No impact is expected.

#### Audit:

Execute the following cmdlet and ensure `AuthMechanism` is set to `Tls`:

```
Get-ReceiveConnector | Select Name, Identity, AuthMechanism
```

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector -Identity <'IdentityName'> -AuthMechanism 'Tls'
```

**Note:** If more than one receive connector exists on the mailbox server, run this command to update all receive connectors.

```
Get-ReceiveConnector | Set-ReceiveConnector -AuthMechanism 'Tls'
```

## Default Value:

N/A

## References:

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/connectors/receive-connectors?view=exchserver-2019#default-receive-connectors-in-the-front-end-transport-service-on-mailbox-servers>
2. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-receiveconnector?view=exchange-ps#-authmechanism>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## 2.4.4 (L2) Ensure 'Send Exchange Customer Experience reports' is set to 'False' (Automated)

### Profile Applicability:

- Level 2 - Mailbox Services Security

### Description:

This parameter specifies whether the Exchange server is enrolled in the Windows Customer Experience Improvement Program (CEIP). This is a voluntary program that collects information on users and their computers in order to help Microsoft improve features and solve common issues.

### Rationale:

The Windows Customer Experience Improvement Program (CEIP) collects information such as user's encounters with Exchange, hardware configurations and usage, and information about configuration settings in general. Although the program claims it does not collect personal information, there is no way to verify what information gets collected.

### Impact:

The system will not be enrolled in the Windows Customer Experience Improvement Program (CEIP).

### Audit:

Execute the following cmdlet and ensure `CustomerFeedbackEnabled` is set to `false`:

```
Get-OrganizationConfig | Select Name, Identity, CustomerFeedbackEnabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-OrganizationConfig -CustomerFeedbackEnabled $false
```

### References:

1. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618322\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj618322(v=ws.11))

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u>                      Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><u>0.0 Explicitly Not Mapped</u>                      Explicitly Not Mapped</p>			

## 2.4.5 (L1) Ensure 'SMTP automated banner response' is set to '220 SMTP Server Ready' (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

This policy setting specifies a custom SMTP 220 banner which is displayed to remote messaging servers that connect to the receive connector.

### Rationale:

The default value could disclose information that can be used by a third-party to determine operating system and product release levels on the target server. This information can then be used for an attack.

### Impact:

N/A

### Audit:

Execute the following cmdlet and ensure `Banner` is set to `220 SMTP Server Ready`:

```
Get-ReceiveConnector | Select Name, Identity, Banner
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-ReceiveConnector -Identity <'IdentityName'> -Banner '220 SMTP Server Ready'
```

### Default Value:

220 <ServerName> Microsoft ESMTP MAIL service ready at <RegionalDay-Date-24HourTimeFormat><RegionalTimeZoneOffset>

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-receiveconnector?view=exchange-ps#-banner>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 3 Mobile Device Management

This section contains recommendations for Mobile Device Management (MDM).

**NOTE:** Organizations using third-party MDM solutions should evaluate the use case in applying recommendations in this section as the settings in the section could conflict.

Administrators should also evaluate the implications of users using personal devices in a Bring Your Own Device (BYOD) scenario. Connecting these to the company's Exchange server allows for the potential of remote wiping the device following 10 failed password attempts as per a CIS recommendation in this section.

### 3.1 (L1) Ensure 'Allow simple passwords' is set to 'False' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting configures the use of 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.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

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

```
Get-MobileDeviceMailboxPolicy | fl -property AllowSimplePassword
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -AllowSimplePassword $false
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Allow simple passwords` box is not checked and click Save.

#### Default Value:

True

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps>

## Additional Information:

```
Get-ActiveSyncMailboxPolicy Deperecated replacing with
```

```
Set-MobileDeviceMailboxPolicy cis.myredwood.net -AllowSimplePassword $false
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

## 3.2 (L1) Ensure 'Allow unmanaged devices' is set to 'False' (Automated)

### Profile Applicability:

- Level 1 - MDM Services Security

### Description:

This policy setting determines whether Exchange will 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.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

### Audit:

Execute the following PowerShell cmdlet and ensure `AllowNonProvisionableDevices` is set to `False`:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property  
AllowNonProvisionableDevices
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -AllowNonProvisionableDevices $false
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "General" settings.
4. Ensure the `Allow mobile devices that don't fully support these policies to synchronize` box is not checked and click `Save`.

**Default Value:**

False

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-allownonprovisionabledevices>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>13.5 <u>Manage Access Control for Remote Assets</u></b> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	<b>12.12 <u>Manage All Devices Remotely Logging into Internal Network</u></b> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

### 3.3 (L1) Ensure 'Enforce password history' is set to '4' or greater (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting configures the device password history.

#### 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:

Users will be required to create a new unique password every time it needs to be changed.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following cmdlet and ensure `DevicePasswordHistory` is set to 4 or greater:

```
Get-MobileDeviceMailboxPolicy | fl -property PasswordHistory
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -PasswordHistory 4
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Change the `Password recycle count` to 4 and click Save.

**Default Value:**

0

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-passwordhistory>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### 3.4 (L1) Ensure 'Minimum password length' is set to '4' or more (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting is used to specify a minimum password length for the device.

#### 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:

None - This is the default behavior.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following cmdlet and ensure `MinDevicePasswordLength` is set to 4 or greater:

```
Get-MobileDeviceMailboxPolicy | fl -property MinPasswordLength
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -MinPasswordLength 4
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Minimum password length` box is checked and change the value to 4 and click Save

**Default Value:**

4

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### 3.5 (L1) Ensure 'Number of attempts allowed' is set to '10' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting is used to restrict the number of failed logon attempts a user can make before an account is locked out.

#### Rationale:

This setting can reduce the likelihood that an unauthorized user can guess the password of a device to access data stored on it.

#### Impact:

A locked-out account cannot be used again until an administrator either resets it or the account lockout duration expires.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following PowerShell cmdlet and ensure `MaxPasswordFailedAttempts` is set to 10 or less:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property  
MaxPasswordFailedAttempts
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -MaxPasswordFailedAttempts 10
```

#### Default Value:

6

#### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-maxpasswordfailedattempts>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</u>                      Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.</p>		●	●
v7	<p><u>0.0 Explicitly Not Mapped</u>                      Explicitly Not Mapped</p>			

### 3.6 (L1) Ensure 'Password expiration' is set to '365' or less (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting is used to specify how long before a password expires.

#### 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.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following cmdlet and ensure `DevicePasswordExpiration` is set to 365 or less:

```
Get-MobileDeviceMailboxPolicy | fl -property PasswordExpiration
```

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -PasswordExpiration 90
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Enforce password lifetime (days)` box is checked change the value to 365 and click Save

## Default Value:

Unlimited

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-passwordexpiration>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

## 3.7 (L1) Ensure 'Refresh interval' is set to '1' (Automated)

### Profile Applicability:

- Level 1 - MDM Services Security

### Description:

This policy setting specifies how often in hours, that policy settings are refreshed.

### 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.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

### Audit:

Execute the following PowerShell script and ensure `DevicePolicyRefreshInterval` is set to `1:00:00`.

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property  
DevicePolicyRefreshInterval
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -DevicePolicyRefreshInterval  
'1:00:00'
```

### Default Value:

24 hours

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-devicepolicyrefreshinterval>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

### 3.8 (L1) Ensure 'Require alphanumeric password' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting ensures passwords meet the basic requirements for strong passwords.

#### Rationale:

Passwords that contain only alpha characters are extremely easy to discover with several publicly available tools.

#### Impact:

Users will be forced to use alphanumeric passwords.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following PowerShell cmdlet and ensure `AlphanumericPasswordRequired` is set to `False`:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property  
AlphanumericPasswordRequired
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -AlphanumericPasswordRequired $true
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Require an alphanumeric password` box is checked and click Save.

**Default Value:**

False

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>5.2 <u>Use Unique Passwords</u></b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### 3.9 (L1) Ensure 'Require encryption on device' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting specifies whether encryption is required on the mobile device before it is allowed to connect to the Exchange environment.

#### Rationale:

Unencrypted data on mobile devices can be vulnerable to attacks. 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 the Exchange server.

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's personal device.

#### Audit:

Execute the following PowerShell cmdlet and ensure `RequireDeviceEncryption` is set to `True`:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property  
RequireDeviceEncryption
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -RequireDeviceEncryption $true
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Require encryption on device` box is checked and click `Save`

**Default Value:**

False

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-activesyncmailboxpolicy?view=exchange-ps#-requiredeviceencryption>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>13.5 <u>Manage Access Control for Remote Assets</u></b> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	<b>12.12 <u>Manage All Devices Remotely Logging into Internal Network</u></b> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

### 3.10 (L1) Ensure 'Require password' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting determines if a password is required for the device.

#### Rationale:

Allowing users to access a device without a password means that anyone with physical access to it can view data on the device.

#### Impact:

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

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following PowerShell cmdlet and ensure `PasswordEnabled` is set to `True`:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property PasswordEnabled
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -PasswordEnabled $true
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Require a password` box is checked and click Save.

#### Default Value:

False

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-passwordenabled>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### 3.11 (L1) Ensure 'Time without user input before password must be re-entered' is set to '15' (Automated)

#### Profile Applicability:

- Level 1 - MDM Services Security

#### Description:

This policy setting prompts users for a password after the device has been inactive for a specified period of time.

#### Rationale:

Requiring devices to lock after 15 minutes minimizes the window of opportunity for an attacker to tamper with a lost or stolen device.

This is the default behavior.

#### Impact:

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

**Note:** This is a mobile device management setting. Use caution when applying these settings as they could have adverse effects depending on the environment, and internal policies around bring your own device (BYOD). These policies could affect a user's BYOD.

#### Audit:

Execute the following PowerShell cmdlet and ensure MaxInactivityTimeLock is set to 15:

```
Get-MobileDeviceMailboxPolicy "Profile" | fl -property MaxInactivityTimeLock
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-MobileDeviceMailboxPolicy "Profile" -MaxInactivityTimeLock 00:15:00
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mobile" on the left and click on the "Mobile device mailbox policies" tab.
3. Double-click the policy you wish to modify and go to the "Security" settings.
4. Ensure the `Require sign-in after the device has been inactive for (minutes)` box is checked and change the value to 15 and click Save.

**Default Value:**

15

**References:**

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-mobiledevicemailboxpolicy?view=exchange-ps#-maxinactivitytimelock>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

## 4 Logging

This section contains recommendations related to logging.

## 4.1 (L1) Ensure 'Receive connector: Configure protocol logging' is set to 'Verbose' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security
- Level 1 - Mailbox 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 with the transport service on Mailbox servers and Edge Transport servers.

### 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:

Additional storage space will be required for the log file.

**Note:** The default file size for the protocol log is *10MB* and is stored for a maximum of *30 days*. This may need to be adjusted to adhere to company retention policies.

**Warning:** Do not enable Protocol logging on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Those changes need to be made in the Transport service on the Mailbox server. The changes are then replicated to the Edge Transport server the next time EdgeSync synchronization occurs.

### Audit:

Execute the following cmdlet and ensure `ProtocolLoggingLevel` is set to `Verbose`:

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

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

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

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Receive Connectors" tab.
3. Double-click on the receive connector to be modified.
4. Change the `Protocol logging level` to `Verbose` and click Save.

## Default Value:

None

## References:

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/connectors/configure-protocol-logging?view=exchserver-2019>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 4.2 (L1) Ensure 'Turn on administrator audit logging' is set to " (Automated)

### Profile Applicability:

- Level 1 - Mailbox Services Security

### Description:

Administrator audit logging is used to provide a log of the settings that are changed by administrators anywhere in the system.

This recommendation incorporates the following parameters into one setting:

- AdminAuditLogEnabled
- AdminAuditLogCmdlets
- AdminAuditLogParameters
- AdminAuditLogExcludedCmdlets
- AdminAuditLogAgeLimit
- LogLevel

**Note:** Changes to the audit log configuration may take up to 60 minutes to be applied on computers that have the Exchange Management Shell open at the time a configuration change is made. For changes to apply immediately, close and reopen the Exchange Management Shell on each computer.

### Rationale:

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

### Impact:

Additional storage space will be required when setting LogLevel to verbose, but the increase is minimal even for very large environments.

### Audit:

Execute the following cmdlet and ensure AdminAuditLog parameters are set to the value specified in the Remediation Section:

```
Get-AdminAuditLogConfig | fl AdminAuditLog*,LogLevel
```

## Remediation:

To implement the recommended state, execute the following PowerShell script:

```
$params = @{
    AdminAuditLogEnabled = $True
    AdminAuditLogCmdlets = '*'
    AdminAuditLogParameters = '*'
    AdminAuditLogExcludedCmdlets = $null
    AdminAuditLogAgeLimit = '90.00:00:00'
    LogLevel = 'Verbose'
}

Set-AdminAuditLogConfig @params
```

## Default Value:

AdminAuditLogEnabled - True

AdminAuditLogCmdlets - \*

AdminAuditLogParameters - \*

AdminAuditLogExcludedCmdlets - None

AdminAuditLogAgeLimit - 90 days

LogLevel - None The CmdletName, ObjectName, Parameters (values), and the Caller, Succeeded and RunDate properties are included in log entries.

## References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

### 4.3 (L1) Ensure 'Turn on connectivity logging' is set to 'True' (Automated)

#### Profile Applicability:

- Level 1 - Edge Services Security
- Level 1 - Mailbox 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 can be configured with the transport service on Mailbox servers and Edge Transport servers.

#### 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:

Additional storage space will be required for the log file.

**Note:** The default file size for the protocol log is *10MB* and is stored for a maximum of *30 days*. This may need to be adjusted to adhere to company retention policies.

#### Audit:

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

```
Get-TransportService "EXCHANGE1" | fl -property ConnectivityLogEnabled
```

#### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-TransportService "EXCHANGE1" -ConnectivityLogEnabled $true
```

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Servers" on the left and click on the "Servers" tab.
3. Double-click the server and go to the "Transport logs" settings.
4. Ensure the `Enable connectivity log` box is checked and click **Save**.

**Default Value:**

False

**References:**

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/configure-connectivity-logging?view=exchserver-2019>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

## 4.4 (L1) Ensure 'Send connector: Configure protocol logging' is set to 'Verbose' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security
- Level 1 - Mailbox 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 with the transport service on Mailbox servers and Edge Transport servers.

### 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:

Additional storage space will be required for the log file.

**Note:** The default file size for the protocol log is *10MB* and is stored for a maximum of *30 days*. This may need to be adjusted to adhere to company retention policies.

**Warning:** Do not enable Protocol logging on an Edge Transport server that has been subscribed to the Exchange organization by using EdgeSync. Those changes need to be made in the Transport service on the Mailbox server. The changes are then replicated to the Edge Transport server the next time EdgeSync synchronization occurs.

### Audit:

Execute the following cmdlet and ensure `ProtocolLoggingLevel` is set to `Verbose`:

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

## Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

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

OR

Perform the following actions:

1. Launch the EAC (Exchange Administrative Center).
2. Go to "Mail Flow" on the left and click on the "Send Connectors" tab.
3. Double-click on the send connector to be modified.
4. Change the Protocol logging level to Verbose and click Save.

## Default Value:

None

## References:

1. <https://learn.microsoft.com/en-us/exchange/mail-flow/connectors/configure-protocol-logging?view=exchserver-2019>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 4.5 (L1) Ensure 'Message tracking logging' is set to 'True' (Automated)

### Profile Applicability:

- Level 1 - Edge Services Security
- 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. The message tracking log can be configured with the transport service on Mailbox servers and Edge Transport servers.

### 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:

None - This is the default behavior.

### Audit:

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

```
Get-TransportService "EXCHANGE1" | fl -property MessageTrackingLogEnabled
```

### Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:

```
Set-TransportService "EXCHANGE1" -MessageTrackingLogEnabled $true
```

### Default Value:

True

### References:

1. <https://learn.microsoft.com/en-us/powershell/module/exchange/set-transportservice?view=exchange-ps#-messagetrackinglogenabled>
2. <https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/search-message-tracking-logs?view=exchserver-2019>

**Additional Information:**

Message tracking is available on Hub Transport servers, Edge Transport servers, and Mailbox servers.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>8.6 <u>Centralize Anti-malware Logging</u></b> Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		●	●

# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Edge Transport Server</b>		
1.1	(L1) Ensure 'Enable sender ID agent' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	(L1) Ensure 'Configure sender filtering' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Sender reputation' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L1) Ensure 'Blank sender field' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	(L1) Ensure 'Spam quarantine mailbox exists' is set to '<SmtpAddress>' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	(L1) Ensure 'SCL Quarantine' is 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	(L1) Ensure 'Nonexistent recipients' is set to 'True' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	(L1) Ensure 'Attachment Filtering Agent' is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	(L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.10	(L1) Ensure 'Transport Pickup Directory Path' is not set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	(L1) Ensure 'Exchange recipient filter' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.12	(L1) Ensure 'Internet-facing receive connectors' is set to 'Tls, BasicAuth, BasicAuthRequireTls' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Mailbox Server</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>2.1</b>	<b>Database and Retention</b>		
2.1.1	(L1) Ensure 'Mailbox quotas: Issue warning at' is set to '<value>' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	(L1) Ensure 'Retain deleted items for the specified number of days' is set to '14' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	(L1) Ensure 'Mailbox quotas: Prohibit send and receive at' is set to '<value>' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	(L1) Ensure 'Mailbox quotas: Prohibit send at' is set to '<value>' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	(L1) Ensure 'Keep deleted mailboxes for the specified number of days' is set to '30' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	(L1) Ensure 'Do not permanently delete items until the database has been backed up' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.2</b>	<b>Mail Flow</b>		
2.2.1	(L1) Ensure 'Transport Pickup Directory Path' is not set (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	(L1) Ensure 'Maximum send size: Organization level' is set to '25' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	(L1) Ensure 'Maximum receive size: Organization level' is set to '25' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	(L1) Ensure 'Maximum send size: Connector level' is set to '25' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	(L1) Ensure 'Maximum receive size: Connector level' is set to '25' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	(L1) Ensure 'Send connector timeout' is set to '10' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.7	(L1) Ensure 'Receive connector timeout' is set to '5' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	(L1) Ensure 'External send connector authentication: DNS routing' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	(L1) Ensure 'External send connector authentication: IgnoreStartTLS' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	(L1) Ensure 'External send connector authentication: Domain security' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3</b>	<b>Recipient and Client</b>		
2.3.1	(L2) Ensure 'Enable non-delivery reports to remote domains' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	(L2) Ensure 'Enable OOF messages to remote domains' is set to 'None' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	(L1) Ensure 'Enable automatic replies to remote domains' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	(L1) Ensure 'Enable automatic forwards to remote domains' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	(L1) Ensure 'Enable S/MIME for OWA' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	(L1) Ensure 'Require client MAPI encryption' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.4</b>	<b>Services and Authentication</b>		
2.4.1	(L1) Ensure 'POP3' Windows services are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	(L1) Ensure 'IMAP4' Windows services are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	(L1) Ensure 'Receive connector' is set to 'TLS' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.4	(L2) Ensure 'Send Exchange Customer Experience reports' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	(L1) Ensure 'SMTP automated banner response' is set to '220 SMTP Server Ready' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Mobile Device Management</b>		
3.1	(L1) Ensure 'Allow simple passwords' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	(L1) Ensure 'Allow unmanaged devices' is set to 'False' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	(L1) Ensure 'Enforce password history' is set to '4' or greater (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	(L1) Ensure 'Minimum password length' is set to '4' or more (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	(L1) Ensure 'Number of attempts allowed' is set to '10' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	(L1) Ensure 'Password expiration' is set to '365' or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	(L1) Ensure 'Refresh interval' is set to '1' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	(L1) Ensure 'Require alphanumeric password' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	(L1) Ensure 'Require encryption on device' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	(L1) Ensure 'Require password' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.11	(L1) Ensure 'Time without user input before password must be re-entered' is set to '15' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Logging</b>		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1	(L1) Ensure 'Receive connector: Configure protocol logging' is set to 'Verbose' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(L1) Ensure 'Turn on administrator audit logging' is set to '<values>' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	(L1) Ensure 'Turn on connectivity logging' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	(L1) Ensure 'Send connector: Configure protocol logging' is set to 'Verbose' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	(L1) Ensure 'Message tracking logging' is set to 'True' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
06/30/2023	1.0.0	Initial Public Release