Center for Internet Security®

CIS Microsoft Office Outlook 2016

v1.0.1 - 09-30-2016

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This is the final release of the Microsoft Office Outlook 2016 Benchmark v1.1.0. CIS encourages you to migrate to a more recent, supported version of this technology.

This document, Security Configuration Benchmark for Microsoft Outlook 2016, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Outlook 2016 running on Windows 10. This guide was tested against Microsoft Office 2016. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document 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 Outlook 2016 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

Acknowledgements

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

Editor
Jordan Rakoske

Microsoft's Security Compliance Management Toolkit was an excellent resource in the development of this Benchmark.

Recommendations

1 User Configuration

1.1 Account Settings

This section contains settings to configure all Outlook account settings

1.1.1 E-mail

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.1.2 Exchange

The section contains settings on how outlook connects with Exchange.

1.1.2.1 Cached Exchange Mode

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.1.2.2 Offline Address Book

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.1.2.3 (L1) Ensure 'Authentication with Exchange server.' is set to 'Enabled:Kerberos/NTLM Password Authentication' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls which authentication method Outlook uses to authenticate with Microsoft Exchange Server. Note - Exchange Server supports the Kerberos authentication protocol and NTLM for authentication. The Kerberos protocol is the more secure authentication method and is supported on Windows 2000 Server and later versions. NTLM authentication is supported in pre-Windows 2000 environments.

If you enable this policy setting, you can choose from three different options for controlling how Outlook authenticates with Microsoft Exchange Server:
- Kerberos/NTLM password authentication. Outlook attempts to authenticate using the Kerberos authentication protocol. If this attempt fails, Outlook attempts to authenticate using NTLM. This option is the default configuration.
- Kerberos password authentication. Outlook attempts to authenticate using the Kerberos protocol only.
- NTLM password authentication. Outlook attempts to authenticate using NTLM only.
If you disable or do not configure this policy setting, Outlook will attempt to authenticate using the Kerberos authentication protocol. If it cannot (because no Windows 2000 or later domain controllers are available), it will authenticate using NTLM. The recommended state for this setting is: `Enabled:Kerberos/NTLM Password Authentication`.

NOTE: When connecting to Office 365, this setting must be set to **Disabled**.

Rationale:

Exchange Server supports the Kerberos authentication protocol and NTLM for authentication. The Kerberos protocol is the more secure authentication method and is supported on Windows 2000 Server and later versions. NTLM authentication is supported

in pre-Windows 2000 environments.
By default, Outlook will attempt to authenticate using the Kerberos authentication protocol. If it cannot (because no Windows 2000 or later domain controllers are available), it will authenticate using NTLM.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security:authenticati
onservice
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\Exchange\Authentication with Exchange Server
```

Then set the `Select the authentication with Exchange server.` option to `Kerberos/NTLM Password Authentication`.

Impact:

The recommended value for this setting in the Microsoft baselines enforces the default configuration, and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.1.2.4 (L1) Ensure 'Automatically configure profile based on Active Directory Primary SMTP address' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users who are joined to a domain in an Active Directory environment can change the primary SMTP address used when setting up accounts in Outlook.
If you enable this policy setting, users cannot change the SMTP settings Outlook retrieves from Active Directory when setting up a new account.
If you disable or do not configure this policy setting, if a user is joined to a domain in an Active Directory environment and does not have an e-mail account configured, Outlook populates the e-mail address field of the New Account Wizard with the primary SMTP address of the user who is currently logged on to Active Directory. The user can change the address to configure a different account, or click Next to use the default settings from Active Directory. The recommended state for this setting is: `Enabled`.

Rationale:

By default, if a user is joined to a domain in an Active Directory environment and does not have an e-mail account configured, Outlook populates the e-mail address field of the New Account Wizard with the primary SMTP address of the user who is currently logged on to Active Directory. The user can change the address to configure a different account, or click Next to use the default settings from Active Directory.
If users are allowed to change this address, they could incorrectly configure their environment or misrepresent their identity.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\autodiscover\zeroconf
igexchange
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\Exchange\Automatically configure profile based on Active Directory Primary
SMTP address
```

Impact:

Enabling this setting could prevent users from configuring Outlook as desired in some unusual cases (for example, if Active Directory is temporarily inaccessible during setup). However, most users should experience no significant usability issues.

Default Value:

Not configured

1.1.2.5 (L1) Ensure 'Do not allow users to change permissions on folders' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents users from changing their mail folder permissions.
If you enable this policy setting, Outlook users cannot change permissions on folders; the settings on the Permissions tab are disabled. Enabling this policy setting does not affect existing permissions, and users can still change permissions by sending a sharing message.
If you disable or do not configure this policy setting, Outlook users can change the permissions for folders under their control by using the Permissions tab of the Properties dialog box for the folder. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Outlook users can change the permissions for folders under their control by using the Permissions tab of the Properties dialog box for the folder, or by sending a sharing message. If users change the permissions on a folder they control, it might cause sensitive information in items stored in the folder to be compromised by exposing it to unauthorized people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\folders\disab
leeditpermissions
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\Exchange\Do not allow users to change permissions on folders
```

Impact:

Enabling this setting prevents Outlook users from sharing folders they control with other users. Users who want to share folders will need to ask an administrator to make the necessary change.

Default Value:

Not configured

1.1.2.6 (L1) Ensure 'Enable RPC encryption' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook uses remote procedure call (RPC) encryption to communicate with Microsoft Exchange servers.
If you enable this policy setting, Outlook uses RPC encryption when communicating with an Exchange server. Note - RPC encryption only encrypts the data from the Outlook client computer to the Exchange server. It does not encrypt the messages themselves as they traverse the Internet.
If you disable or do not configure this policy setting, RPC encryption is still used by default. This setting allows you to override the corresponding per-profile setting. The recommended state for this setting is: `Enabled`.

Rationale:

By default, the remote procedure call (RPC) communication channel between an Outlook client computer and an Exchange server is not encrypted. If a malicious person is able to eavesdrop on the network traffic between Outlook and the server, they might be able to access confidential information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\rpc\enablerpcencryption
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account Settings\Exchange\Enable RPC encryption
```

Impact:

Enabling this setting should not have any significant effect on users. However, there is always a trade-off between secure communication and performance, so you should

evaluate the performance impact of encrypting every connection from the Outlook client computer and the Exchange server.

Default Value:

Not configured

1.1.3 Exchange ActiveSync

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.1.4 IMAP

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.1.5 Internet Calendars

This section includes setting for configuring Internet Calendars.

1.1.5.1 (L1) Ensure 'Automatically download attachments' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook downloads files attached to Internet Calendar appointments.
If you enable this policy setting, Outlook automatically downloads all Internet Calendar appointment attachments
If you disable or do not configure this policy setting, Outlook does not download attachments when retrieving Internet Calendar appointments. The recommended state for this setting is: `Disabled`.

Rationale:

Files attached to Internet Calendar appointments could contain malicious code that could be used to compromise a computer.
By default, Outlook does not download attachments when retrieving Internet Calendar appointments.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\webcal\enable
attachments
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\Internet Calendars\Automatically download attachments
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Default Value:

Not configured

1.1.5.2 (L1) Ensure 'Do not include Internet Calendar integration in Outlook' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine whether or not you want to include Internet Calendar integration in Outlook. The Internet Calendar feature in Outlook enables users to publish calendars online (using the webcal:// protocol) and subscribe to calendars that others have published. When users subscribe to an Internet calendar, Outlook queries the calendar at regular intervals and downloads any changes as they are posted.
If you enable this policy setting, all Internet calendar functionality in Outlook is disabled.
If you disable or do not configure this policy setting, Outlook allows users to subscribe to Internet calendars. The recommended state for this setting is: `Enabled`.

Rationale:

The Internet Calendar feature in Outlook enables users to publish calendars online (using the webcal:// protocol) and subscribe to calendars that others have published. When users subscribe to an Internet calendar, Outlook queries the calendar at regular intervals and downloads any changes as they are posted.
By default, Outlook allows users to subscribe to Internet calendars. If your organization has policies that govern the use of external resources such as Internet calendars, this feature might enable users to violate those policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\webcal\disabl
e
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\Internet Calendars\Do not include Internet Calendar integration in Outlook
```

Impact:

Enabling this setting can cause disruptions for users who subscribe to Internet calendars from within Outlook. These users will have to use another method to access Internet calendar data.

Default Value:

Not configured

1.1.6 RSS Feeds

This section contains settings for configuring RSS Feeds within outlook.

1.1.6.1 (L1) Ensure 'Download full text of articles as HTML attachments' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook automatically makes an offline copy of the RSS items as HTML attachments.
If you enable this policy setting, Outlook automatically makes an offline copy of RSS items as HTML attachments.
If you disable or do not configure this policy setting, Outlook will not automatically make an offline copy of RSS items as HTML attachments. The recommended state for this setting is: `Disabled`.

Rationale:

Many RSS feeds use messages that contain a brief summary of a larger message or an article with a link to the full content. Users can configure Outlook to automatically download the linked content as message attachments for individual RSS feeds. If a feed is frequently updated or typically contains very large messages and is not AutoArchived regularly, downloading full articles can cause the affected message store to become very large, which can affect the performance of Outlook.
By default, Outlook does not automatically download the full text of RSS entries when retrieving feeds.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\rss\enableful
ltexthtml
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\RSS Feeds\Download full text of articles as HTML attachments
```

Impact:

This setting enforces the default configuration and therefore should have minimal impact on most users. Disabling this setting could cause minor disruptions for users who are accustomed to reading articles as HTML attachments within Outlook. These users will have to click the View article link to open such articles in the default Web browser.

Default Value:

Not configured

1.1.6.2 (L1) Ensure 'Synchronize Outlook RSS Feeds with Common Feed List' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook subscribes to the Common Feed List, which is made available to multiple RSS clients. The Common Feed List is a hierarchical set of RSS Feeds to which clients such as Outlook, the Feeds list in Internet Explorer 7, and the Feed Headlines Sidebar gadget in Windows Vista can subscribe.
If you enable this policy setting, Outlook automatically subscribes to RSS Feeds added in Internet Explorer, and Outlook RSS Feeds are synchronized with the Common Feed List so they are available in Internet Explorer. Be aware that third-party applications besides Internet Explorer can add RSS Feeds to the Common Feed List, and if you enable this setting Outlook automatically subscribes to those RSS Feeds as well.
If you disable or do not configure this policy setting, Outlook maintains its own list of RSS Feeds and does not automatically subscribe to RSS Feeds that are added to the Common Feed List. The recommended state for this setting is: `Disabled`.

Rationale:

The Common Feed list is a hierarchical set of RSS feeds to which clients such as Outlook , the Feeds list in Internet Explorer 7, and the Feed Headlines Sidebar gadget in Windows Vista can subscribe.
If Outlook subscribes to a very large feed list, performance and availability can be affected, especially if Outlook is configured to download full RSS message bodies or if the feed list is not AutoArchived regularly.
By default, Outlook maintains its own list of feeds and does not automatically subscribe to RSS feeds that are added to the Common Feed List.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\rss\synctosys
cfl
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\RSS Feeds\Synchronize Outlook RSS Feeds with Common Feed List
```

Impact:

Disabling this setting can cause disruptions for users who are accustomed to accessing the Common Feed List in Outlook. Users will still have access to the Common Feed List through Internet Explorer 7 and other client programs. Disabling this setting does not prevent users from maintaining a separate RSS Feeds subscriptions list in Outlook.

Default Value:

Not configured

1.1.6.3 (L1) Ensure 'Turn Off RSS Feature' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the RSS aggregation feature in Outlook is enabled.

If you enable this policy setting, the RSS aggregation feature in Outlook is disabled.

If you disable or do not configure this policy setting, users can subscribe to RSS Feeds from within Outlook and read RSS items like e-mail messages.

Rationale:

By default, users can subscribe to RSS feeds from within Outlook and read RSS items like e-mail messages. If your organization has policies that govern the use of external resources such as RSS feeds, allowing users to subscribe to the RSS feed in Outlook might enable them to violate those policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\16.0\Outlook\PST\options\rss\disab
le
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Account
Settings\RSS Feeds\Turn Off RSS Feature
```

Impact:

Enabling this setting might cause some disruptions for users who are accustomed to reading RSS feeds in Outlook. It does not affect the performance of other RSS clients, such as Internet Explorer 7.

Default Value:

Not Configured

1.1.7 SharePoint Lists

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.2 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.3.1 Custom

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.3.2 Predefined

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.4 Form Region Settings

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.5 InfoPath Integration

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.6 Meeting Workspace

This section contains settings for configuring Meeting Workspace.

1.6.1 (L1) Ensure 'Check to disable users from adding entries to server list' is set to Enabled:Publish default, disallow others (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook users can add entries to the list of SharePoint servers when establishing a meeting workspace.
If you enable this policy setting, you can choose between two options to determine whether Outlook users can add entries to the published server list:

- Publish default, allow others. This option is the default configuration in Outlook.
- Publish default, disallow others. This option prevents users from adding servers to the default published server list.

If you disable or do not configure this policy setting, when users create a meeting workspace, they can choose a server from a default list provided by administrators or manually enter the address of a server that is not listed. This is the equivalent of Enabled -- Publish default, allow others. The recommended state for this setting is: `Enabled:Publish default, disallow others`.

Rationale:

If users are able to manually enter the addresses of servers that are not approved by the organization, they could use servers that do not meet your organization's information security requirements, which could cause sensitive information to be at risk.

By default, when users create a meeting workspace, they can choose a server from a default list provided by administrators or manually enter the address of a server that is not listed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Meeting Workspace\Disable user entries to server list\Disable user entries to server list
```

Then set the `Check to disable users from adding entries to server list` option to `Publish default, disallow others`.

Impact:

If you configure this setting to "Publish default, disallow others," users in your organization who have a legitimate need to use servers other than those in the published server list will need to obtain administrative assistance.

Default Value:

Not configured

1.7 MIME to MAPI Conversion

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.8 Miscellaneous

This section contains settings for configuring Miscellaneous outlook and PST settings.

1.8.1 Miscellaneous

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.8.2 PST Settings

This section contains settings for configuring PST Settings.

1.8.2.1 (L1) Ensure 'PST Null Data On Delete' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to force Outlook to fully nullify deleted data in users' Personal Folder files (.pst) at the time that the data is deleted.

If you enable this policy setting, data is immediately nullified in PST files when deleted.

If you disable or do not configure this policy setting, data remains in PST files until it is purged or overwritten by the user. The recommended state for this setting is: Enabled.

Rationale:

By default, when a users' Personal Folder files (.pst) at the time that the data is deleted, the data inside the .pst file is retained in the available storage. Attackers could potentially recover the data by using tools used to view disk block or recover deleted files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\16.0\Outlook\PST\pstnullfreeondele
te
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Miscellaneous\PST
Settings
```

Impact:

Users may experience a delay in deleting a .pst file as it will take some time to write nulls to every location in the .pst file when deleted.

Default Value:

Not Configured

1.9 Outlook Options

This section contains settings for configuring Outlook options.

1.9.1 Customize Ribbon

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.2 Delegates

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.3 Mail

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.3.1 Compose Messages

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.4 Mail Format

This section contains settings for configuring Mail format.

1.9.4.1 International Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.4.2 Internet Formatting

This section contains settings for configuring Internet Formatting.

1.9.4.2.1 Message Format

This section contains settings for configuring Message Format.

1.9.4.2.2 (L1) Ensure ' Outlook Rich Text Options' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Outlook sends Rich Text Format (RTF) messages to Internet recipients.

If you enable this policy setting, you may choose from the following for handling RTF messages addressed to recipients on the Internet:

* Convert to Plain Text format - Outlook converts the message to plain text format in the default character set. Any message formatting will be lost.

If you disable or do not configure this policy setting, Outlook automatically converts RTF formatted messages that are sent over the Internet to HTML format, so that the message formatting is maintained and attachments are received. The recommended state for this setting is: `Enabled`.

Rationale:

Outlook users can choose to compose messages in HTML, Rich Text, or plain text formats. For composing formatted messages, Microsoft recommends the widely-used HTML format but Rich Text Format (RTF) can also be used when sending messages within an organization that uses Microsoft Exchange.

By default, Outlook automatically converts RTF formatted messages that are sent over the Internet to HTML format, so that the message formatting is maintained and attachments are received. If this configuration is changed, recipients might not be able to read messages, or might not receive them with the proper formatting and attachments.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\16.0\Outlook\options\mail\message
rtf format
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Mail Format\Internet Formatting\Outlook Rich Text Options
```

Impact:

If you configure this setting to "Convert to Plain Text format" Outlook will remove any formatting applied to RTF messages when sent to recipients over the Internet. Users who compose messages in HTML or plain text format will not be affected by this setting.

1.9.4.2.3 (L1) Ensure 'Plain Text Options' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to control how plain text messages are formatted when they are sent from Outlook.
If you enable this policy setting, text is automatically wrapped in Internet e-mail messages and attachments are encoded in UUENCODE format.
If you disable this policy setting, Outlook uses the standard MIME format to encode attachments in plain text Outlook messages. Users will not be able to change this configuration.
If you do not configure this policy setting, the behavior is the equivalent of setting the policy to Disabled, but users can modify plain text options in Outlook when required by clicking Tools, clicking Options, clicking the Mail Format tab, clicking Internet Format, and changing the values under "Plain text options". The recommended state for this setting is: `Disabled`.

Rationale:

If outgoing mail is formatted in certain ways, for example if attachments are encoded in UUENCODE format, attackers might manipulate the messages for their own purposes. If UUENCODE formatting is used, an attacker could manipulate the encoded attachment to bypass content filtering software.
By default, Outlook automatically wraps plain text messages at 76 characters and uses the standard MIME format to encode attachments in plain text messages. However, these settings can be altered to allow e-mail to be read in plain text e-mail programs that use a non-standard line length or that cannot process MIME attachments.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Mail Format\Internet Formatting\Plain text options\: Encode attachments in
UUENCODE format
```

Impact:

If this setting is not configured, users can modify plain text options in Outlook when required by clicking Tools, clicking Options, clicking the Mail Format tab, clicking Internet Format, and changing the values under Plain text options. If you enable this policy setting, text is automatically wrapped in Internet e-mail messages and attachments are encoded in UUENCODE format.

Default Value:

Not configured

1.9.4.3 Stationery and Fonts

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.4.4 (L1) Ensure 'Do not allow signatures for e-mail messages' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to prevent Outlook users from adding signatures to e-mails they create, reply to, or forward.
If you enable this policy setting, Outlook users cannot manually add signatures to e-mails they create, reply to, or forward, nor will they be able to configure automatic signatures.
If you disable or do not configure this policy setting, Outlook users can add signatures to e-mail messages either manually or automatically. The recommended state for this setting is: `Disabled`.

Rationale:

By default, Outlook users can create and use signatures in e-mail messages. Users can add signatures to messages manually, and can also configure Outlook to automatically append signatures to new messages, to replies and forwards, or to all three. Signatures typically include details such as the user's name, title, phone numbers, and office location. If your organization has policies that govern the distribution of this kind of information, using signatures might cause some users to inadvertently violate these policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\common\mailsettings\disablesignatures
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Mail Format\Do not allow signatures for e-mail messages
```

Impact:

The recommended settings do not change the default configuration of Outlook, and therefore should not affect usability.

Default Value:

Not configured

1.9.5 Mail Setup

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.6 Other

This section contains settings for configuring Other settings within Outlook.

1.9.6.1 Advanced

This section contains settings for configuring Advanced settings withing Outlook.

1.9.6.1.1 Reminder Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.6.1.2 (L1) Ensure 'Do not allow folders in non-default stores to be set as folder home pages' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

By default, creating folder home pages for folders in non-default stores is blocked; you cannot define a folder home page for a folder that is in a non-default store. This setting allows you to unblock folder home pages for folders in non-default stores. Note that other settings might still prevent folder home pages from functioning. The recommended state for this setting is: `Enabled`.

Rationale:

Outlook allows users to designate Web pages as home pages for personal or public folders. When a user clicks on a folder, Outlook displays the home page the user has assigned to it. Although this feature provides the opportunity to create powerful public folder applications, scripts can be included on Web pages that access the Outlook object model, which exposes users to security risks.
By default, Outlook does not allow users to define folder home pages for folders in non-default stores. If this configuration is changed, users can create and access dangerous folder home pages for Outlook data files (.pst) and other non-default stores, which can compromise the security of the users' data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\nondefaultstorescript
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Other\Advanced\Do not allow folders in non-default stores to be set as folder
home pages
```

Impact:

For more information, see Configure security for Outlook folder home pages.

Default Value:

Not configured

1.9.6.1.3 (L1) Ensure 'Do not allow Outlook object model scripts to run for public folders' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook executes scripts that are associated with custom forms or folder home pages for public folders.
If you enable this policy setting, Outlook cannot execute any scripts associated with public folders, overriding any configuration changes on users' computers.
If you disable or do not configure this policy setting Outlook will automatically run any scripts associated with custom forms or folder home pages for public folders. The recommended state for this setting is: `Enabled`.

Rationale:

In Outlook, folders can be associated with custom forms or folder home pages that include scripts that access the Outlook object model. These scripts can add functionality to the folders and items contained within, but dangerous scripts can pose security risks.

By default, Outlook allows scripts included in custom forms or folder home pages for public folders to execute. If users inadvertently run dangerous scripts when using public folders, their computers or data could be at risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\publicfolderscript
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Options\Other\Advanced\Do not allow Outlook object model scripts to run for public folders
```

Impact:

If your organization uses custom forms or public folder home pages that contain scripts, enabling this setting can reduce their functionality or render them unusable. Consider surveying your organization's public folders for affected items before you enable this setting.

Default Value:

Not configured

1.9.6.1.4 (L1) Ensure 'Do not allow Outlook object model scripts to run for shared folders' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook executes scripts associated with custom forms or folder home pages for shared folders.
If you enable this policy setting, Outlook cannot execute any scripts associated with shared folders, overriding any configuration changes on users' computers.
If you disable this policy setting, Outlook will automatically run any scripts associated with custom forms or folder home pages for shared folders.
If you do not configure this policy setting, the behavior is the equivalent of setting the policy to Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

In Outlook, folders can be associated with custom forms or folder home pages that include scripts that access the Outlook object model. These scripts can add functionality to the folders and items contained within, but dangerous scripts can pose security risks.
By default, Outlook does not allow scripts included in custom forms or folder home pages for shared folders to execute. If this configuration is changed, users can inadvertently run dangerous scripts when using shared folders, which can put their computers or data at risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\sharedfolder
script
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Other\Advanced\Do not allow Outlook object model scripts to run for shared
folders
```

Impact:

Enabling this setting enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Default Value:

Not configured

1.9.6.1.5 (L1) Ensure 'Use Unicode format when dragging e-mail message to file system' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether e-mail messages dragged from Outlook to the file system are saved in Unicode or ANSI format.
If you enable this policy setting, when users drag an e-mail message from Outlook to the file system, Outlook uses the Unicode character encoding standard to create the message file, which preserves special characters in the message.
If you disable or do not configure this policy setting, when users drag an e-mail message from Outlook to the file system, the message file created is in ANSI format. The recommended state for this setting is: `Disabled`.

Rationale:

By default, when users drag e-mail messages from Outlook to a Windows Explorer window or to their Desktop, Outlook creates a .msg file using the native character encoding format for the configured locale (the so-called "ANSI" format). If this setting is Enabled, Outlook uses the Unicode character encoding standard to create the message file, which preserves special characters in the message.
However, Unicode text is vulnerable to homograph attacks, in which characters are replaced by different but similar-looking characters. For example, the Cyrillic letter? (U+0430) appears identical to the Latin letter a (U+0061) in many typefaces, but is actually a different character. Homographs can be used in "phishing" attacks to convince victims to visit fraudulent Web sites and enter sensitive information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\general\msgfo
rmat
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Other\Advanced\Use Unicode format when dragging e-mail message to file system
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.9.6.2 AutoArchive

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.6.3 (L1) Ensure 'Make Outlook the default program for E-mail, Contacts, and Calendar' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook is the default program for e-mail, contacts, and calendar services.
If you enable this policy setting, the "Make Outlook the default program for E-mail, Contacts, and Calendar" check box on the General tab of the Office Center is selected and users cannot change it.
If you disable this policy setting, users cannot make Outlook the default program for these services.
If you do not configure this policy setting, Outlook is made the default program for e-mail, contacts, and calendar services when it is installed, although users can designate other programs as the default programs for these services. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Outlook is made the default program for E-mail, contacts, and calendar services when it is installed, although users can designate other programs as the default programs for these services. If another application is used to provide these services and your organization does not ensure the security of that application, it could be exploited to gain access to sensitive information or launch other malicious attacks.
If your organization has policies that govern the use of personal information management software, allowing users to change the default configuration could enable them to violate such policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\general\check
default client
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Other\Make Outlook the default program for E-mail, Contacts, and Calendar
```

Impact:

In most environments that use the Microsoft Office system, Outlook is often already the default program for e-mail, contacts, and calendaring for most users. Therefore, enabling this setting is unlikely to cause usability issues.

Default Value:

Not configured

1.9.7 Out of Office Assistant

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8 Preferences

This section contains setting for configuring preferences within Outlook.

1.9.8.1 Calendar Options

This section contains settings for configuring Calendar Options within Outlook.

1.9.8.1.1 Free/Busy Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.1.2 Office.com Sharing Service

This section contains settings for configuring Office.com Sharing Services.

1.9.8.1.2.1 (L1) Ensure 'Access to published calendars' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines what restrictions apply to users who publish their calendars on Office.com or third-party World Wide Web Distributed Authoring and Versioning (WebDAV) servers.
If you enable or disable this policy setting, calendars that are published on Office.com must have restricted access (users other than the calendar owner/publisher who wish to view the calendar can only do so if they receive invitations from the calendar owner), and users cannot publish their calendars to third-party DAV servers.
If you do not configure this policy setting, users can share their calendars with others by publishing them to the Office.com Calendar Sharing Services and to a server that supports the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. Office.com allows users to choose whether to restrict access to their calendars to people they invite, or allow unrestricted access to anyone who knows the URL to reach the calendar. DAV access restrictions can only be achieved through server and folder permissions, and might require the assistance of a server administrator to set up and maintain. The recommended state for this setting is: `Enabled`.

Rationale:

By default, users can share their calendars with others by publishing them to the Microsoft Office.com Calendar Sharing Services and to a server that supports the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. Office.com allows users to choose whether to restrict access to their calendars to people they invite, or allow unrestricted access to anyone who knows the URL to reach the calendar. DAV access restrictions can only be achieved through server and folder permissions, and might require the assistance of a server administrator to set up and maintain.
If a calendar is visible to anyone on Office.com or third-party DAV servers, sensitive information might be revealed contained in calendar appointments.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\pubcal\restri
ctedaccessonly
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\Calendar Options\Office.com Sharing Service\Access to published
calendars
```

Impact:

Most users probably don't want to make their calendars available to every user on Office.com, so the effect will likely be minimal in most environments.

Default Value:

Not configured

1.9.8.1.2.2 (L1) Ensure 'Prevent publishing to a DAV server' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook users can publish their calendars to a DAV server.
If you enable this policy setting, Outlook users cannot publish their calendars to a DAV server.
If you disable or do not configure this policy setting, Outlook users can share their calendars with others by publishing them to a server that supports the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Outlook users can share their calendars with others by publishing them to a server that supports the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. Unlike the Microsoft Office.com Calendar Sharing Service, which allows users to manage other people's access to their calendars, DAV access restrictions can only be accomplished through server and folder permissions, and might require the assistance of the server administrator to set up and maintain. If these permissions are not managed properly, unauthorized people could access sensitive information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\pubcal\disabledav
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Options\Preferences\Calendar Options\Office.com Sharing Service\Prevent publishing to a DAV server
```

Impact:

Enabling this setting will cause disruptions for Outlook users who publish their calendar data to a DAV server. Such users will need to publish their calendar data to a different resource, such as the Microsoft Online Calendar Sharing Service, or stop publishing their calendar data. Users who do not publish calendar data will not be affected by this setting.

Default Value:

Not configured

1.9.8.1.2.3 (L1) Ensure 'Prevent publishing to Office.com' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook users can publish their calendars to the Office.com Calendar Sharing Service.
If you enable this policy setting, Outlook users cannot publish their calendars to Office.com. If you disable do not configure this policy setting, Outlook users can share their calendars with selected others by publishing them to the Microsoft Outlook Calendar Sharing Service. Users can control who can view their calendar and at what level of detail. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Outlook users can share their calendars with selected others by publishing them to the Microsoft Office Outlook Calendar Sharing Service. Users can control who can view their calendar and at what level of detail. If your organization has policies that govern access to external resources such as Office.com, allowing users to publish their calendars might enable them to violate those policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\pubcal\disableofficeonline
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Options\Preferences\Calendar Options\Office.com Sharing Service\Prevent publishing to Office.com
```

Impact:

Enabling this setting will cause disruptions for Outlook users who publish their calendar data to Microsoft Office.com. Such users will have to publish their calendar data to a different resource or stop publishing their calendar data. Users who do not publish calendar data will not be affected by this setting.

Default Value:

Not configured

1.9.8.1.2.4 (L1) Ensure 'Restrict level of calendar details users can publish' is set to Enabled:Disables 'Full details' and 'Limited details' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the level of calendar details that Outlook users can publish to the Microsoft Outlook Calendar Sharing Service.

If you enable this policy setting, you can choose from three levels of detail:

* All options are available - This level of detail is the default configuration.

* Disables 'Full details'

* Disables 'Full details' and 'Limited details'

If you disable or do not configure this policy setting, Outlook users can share their calendars with selected others by publishing them to the Microsoft Outlook Calendar Sharing Service. Users can choose from three levels of detail:

* Availability only - Authorized visitors will see the user's time marked as Free, Busy, Tentative, or Out of Office, but will not be able to see the subjects or details of calendar items.

* Limited details - Authorized visitors can see the user's availability and the subjects of calendar items only. They will not be able to view the details of calendar items. Optionally, users can allow visitors to see the existence of private items.

* Full details - Authorized visitors can see the full details of calendar items. Optionally, users can allow visitors to see the existence of private items. The recommended state for this setting is: `Enabled:Disables 'Full details' and 'Limited details'.`

Rationale:

By default, Outlook users can share their calendars with selected others by publishing them to the Microsoft Office Outlook Calendar Sharing Service. Users can choose from three levels of detail:

• Availability only. Authorized visitors will see the user's time marked as Free, Busy, Tentative, or Out of Office, but will not be able to see the subjects or details of calendar items.

• Limited details. Authorized visitors can see the user's availability and the subjects of calendar items only. They will not be able to view the details of calendar items. Optionally, users can allow visitors to see the existence of private items.

• Full details. Authorized visitors can see the full details of calendar items. Optionally, users can allow visitors to see the existence of private items and to access attachments within calendar items.

If users are allowed to publish limited or full details, sensitive information in their calendars could become exposed to parties who are not authorized to have that information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Options\Preferences\Calendar Options\Office.com Sharing Service\Restrict level of calendar details users can publish
```

Then set the `Restrict level of calendar details users can publish` option to `Disables 'Full details' and 'Limited details'.`

Impact:

Choosing Disables 'Full details' or Disables 'Full details' and 'Limited details' could cause disruptions for Outlook users who rely on the ability to publish details of their appointments to the Microsoft Office Outlook Calendar Sharing Service. These users will have to communicate appointment details to outside parties by other means.

Default Value:

Not configured

1.9.8.1.2.5 (L1) Ensure 'Restrict upload method' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook can automatically upload calendar updates to Office.com.
If you enable this policy setting, Outlook enforces the "Single Upload: Updates will not be uploaded from the Published Calendar Settings dialog" option, and calendar updates are not uploaded. Users will not be able to change this setting.
If you disable this policy setting Outlook automatically publishes calendar updates to Office.com at regular intervals and users will not be able to change this.
If you do not configure this policy setting, when users publish their calendar to Office.com using the Microsoft Outlook Calendar Sharing Service, Outlook updates the calendars online at regular intervals unless they click "Advanced" and select "Single Upload: Updates will not be uploaded from the Published Calendar Settings dialog". The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users publish their calendar to Microsoft Office.com using the Microsoft Office Outlook Calendar Sharing Service, Outlook updates the calendars online at regular intervals unless they click Advanced and select Single Upload: Updates will not be uploaded from the Published Calendar Settings dialog box. If your organization has policies that govern the use of external resources such as Microsoft Office.com, allowing Outlook to publish calendar updates automatically might violate those policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\pubcal\single uploadonly
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\Calendar Options\Office.com Sharing Service\Restrict upload method
```

Impact:

Enabling this setting could cause disruptions for users who publish their calendars to the Microsoft Office Outlook Calendar Sharing Service. These users will have to use the Single Upload option to manually update their calendars. If users do not publish regularly, their online calendars could become significantly out of date.

Default Value:

Not configured

1.9.8.1.3 Planner Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.1.4 Recurring Item Configuration

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.1.5 Schedule View

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.2 Contact Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.3 E-mail Options

This section contains settings for configuring E-mail Options within Outlook.

1.9.8.3.1 Advanced E-mail Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.3.1.1 Desktop Alert

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.3.2 Tracking Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.8.3.3 (L1) Ensure 'Read e-mail as plain text' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Outlook renders all e-mail messages in plain text format for reading. Outlook can display e-mail messages and other items in three formats: plain text, Rich Text Format (RTF), and HTML.
If you enable this policy setting, the "Read all standard mail in plain text" check box option is selected in the "E-mail Security" section of the Trust Center and users cannot change it. This option only changes the way e-mail messages are displayed; the original message is not converted to plain text format.
If you disable or do not configure this policy setting, Outlook displays e-mail messages in whatever format they were received in. The recommended state for this setting is: `Enabled`.

Rationale:

Outlook can display e-mail messages and other items in three formats: plain text, Rich Text Format (RTF), and HTML. By default, Outlook displays e-mail messages in whatever format they were received in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\readaspl
ain
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\E-mail Options\Read e-mail as plain text
```

Impact:

Enabling this setting forces Outlook to display all messages in plain text, which could cause disruptions for users who receive messages in HTML or RTF formats. Inline graphics in the messages will not display, and the text of formatted messages might become distorted or illegible.

Default Value:

Not configured

1.9.8.3.4 (L1) Ensure 'Read signed e-mail as plain text' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Outlook renders all digitally signed e-mail in plain text format for reading. Outlook can display e-mail messages and other items in three formats: plain text, Rich Text Format (RTF), and HTML.
If you enable this policy setting, the "Read all standard mail in plain text" check box option is selected in the "E-mail Security" section of the Trust Center and users cannot change it. This option only changes the way e-mail messages are displayed; the original message is not converted to plain text format.
If you disable or do not configure this policy setting, Outlook displays digitally signed e-mail messages in the format they were received in. The recommended state for this setting is: `Enabled`.

Rationale:

Outlook can display e-mail messages and other items in three formats: plain text, Rich Text Format (RTF), and HTML. By default, Outlook displays digitally signed e-mail messages in the format they were received in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\readsign
edasplain
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\E-mail Options\Read signed e-mail as plain text
```

Impact:

Enabling this setting forces Outlook to display signed messages in plain text, which could cause disruptions for users who receive signed messages in HTML or RTF formats. Inline graphics in the messages will not display, and the text of formatted messages might become distorted or illegible.

Default Value:

Not configured

1.9.8.4 Junk E-mail

This section contains settings for configuring Junk E-mail settings within Outlook.

1.9.8.4.1 (L1) Ensure 'Add e-mail recipients to users' Safe Senders Lists' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether recipients' e-mail addresses are automatically added to the user's Safe Senders List in Microsoft Outlook. Sometimes users will send e-mail messages to request that they be taken off a mailing list. If the e-mail recipient is then automatically added to the Safe Senders List, future e-mail messages from that address will no longer be sent to the users Junk E-mail folder, even if it would otherwise be considered junk.
If you enable this policy setting, all recipients of outgoing messages are automatically added to users' Safe Senders Lists. If users respond to junk e-mail senders while this policy setting is Enabled, all future junk e-mail from the same address will be considered safe.
If you disable this policy setting, recipients of outgoing messages are not automatically added to the Safe Senders List. Users must explicitly add addresses to the list.
If you do not configure this policy setting, recipients of outgoing messages are not added automatically to individual users' Safe Senders Lists. However, users can change this configuration in the Outlook user interface. The recommended state for this setting is: `Disabled`.

Rationale:

Sometimes users will send e-mail messages to request that they be taken off a mailing list. If the e-mail recipient is then automatically added to the Safe Senders List, future e mail messages from that address will no longer be sent to the users Junk E-mail folder, even if it would otherwise be considered junk.
By default, recipients of outgoing messages are not added automatically to individual users' Safe Senders Lists. However, users can change this configuration in the Outlook user interface.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\junkmail
trustoutgoingrecipients
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\Junk E-mail\Add e-mail recipients to users' Safe Senders Lists
```

Impact:

In most situations, modifying this setting will have minimal effect on usability. However, if users send e-mail messages to many recipients, manually adding the recipients to a Safe Senders List might affect productivity. In such situations, you can choose to enable the setting for some groups of users.

Default Value:

Not configured

1.9.8.4.2 (L1) Ensure 'Hide Junk Mail UI' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the Junk E-mail Filter is enabled in Outlook. The Junk E-mail Filter in Outlook is designed to intercept the most obvious junk e-mail, or spam, and send it to users' Junk E-mail folders. The filter evaluates each incoming message based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to discover whether or not it is probably spam.

If you enable this policy setting, junk e-mail filtering in Outlook is turned off entirely, in addition to hiding the filtering controls from users. In addition, you can use the "Junk E-mail Protection level" policy setting to preset a filtering level and prevent users from changing it. Note - This policy setting does not affect the configuration of the Microsoft Exchange Server Intelligent Message Filter (IMF), which provides server-level junk e-mail filtering.
If you disable or do not configure this policy setting, the Junk E-mail Filter in Outlook is enabled. The recommended state for this setting is: `Disabled`.

Rationale:

The Junk E-mail Filter in Outlook is designed to intercept the most obvious junk e-mail, or spam, and send it to users' Junk E-mail folders. The filter evaluates each incoming message based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to discover whether or not it is probably spam.

By default, the Junk E-mail Filter in Outlook is enabled. If this configuration is changed, users can receive large amounts of junk e-mail in their Inboxes, which could make it difficult for them to work with business-related e-mail messages.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\disableantispam
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\Junk E-mail\Hide Junk Mail UI
```

Impact:

The name of this setting is somewhat misleading, as enabling it turns off junk e-mail filtering in Outlook entirely, in addition to hiding the filtering controls from users. You can use the "Junk E-mail Protection level" setting to preset a filtering level and prevent users from changing it.

This setting does not affect the configuration of the Microsoft Exchange Server Intelligent Message Filter (IMF), which provides server-level junk e-mail filtering.

Default Value:

Not configured

1.9.8.4.3 (L1) Ensure 'Junk E-mail protection level: Select level:' is set to Enabled:High (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls your Junk E-mail protection level. The Junk E-mail Filter in Outlook helps to prevent junk e-mail messages, also known as spam, from cluttering user's Inbox. The filter evaluates each incoming message based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to discover whether or not it is probably spam.
If you enable this policy setting, you can select one of the four listed options available. After you select an option, users will not be able to change it.
If you disable this policy setting, Outlook reverts to the user-defined protection level.
If you do not configure this policy setting, users can change their junk e-mail filtering options. The recommended state for this setting is: `Enabled:High`.

Rationale:

The Junk E-mail Filter in Outlook is designed to intercept the most obvious junk e-mail, or spam, and send it to users' Junk E-mail folders. The filter evaluates each incoming message based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to discover whether or not it is probably spam.

By default, users can choose from four levels of junk e-mail filtering:

• No Automatic Filtering. Outlook does not evaluate incoming messages by content. Outlook continues to evaluate messages by using the domain names and e-mail addresses in the users' Blocked Senders Lists, and continues to move messages from blocked senders to users' Junk E-mail folders.

• Low. Outlook only moves the most obvious spam messages to users' Junk E-mail folders. This level is the default setting.

• High. Outlook intercepts most junk e-mail, but might incorrectly classify some legitimate messages as junk. Users are advised to check their Junk E-mail folders often.

• Safe Lists Only. Outlook moves all incoming messages to users' Junk E-mail folders except messages from someone on users' Safe Senders Lists and messages sent to mailing lists on users' Safe Recipients Lists.

If users choose an inappropriate setting, they might miss important messages or accumulate large amounts of junk e-mail in their Inboxes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Options\Preferences\Junk E-mail\Junk E-mail protection level
```

Then set the `Junk E-mail protection level: Select level:` option to `High`.

Impact:

Different users might receive different amounts of junk e-mail. Enabling this setting might result in setting the junk e-mail protection level too high for some users and too low for others.

Default Value:

Not configured

1.9.8.4.4 (L1) Ensure 'Trust e-mail from contacts' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook analyzes e-mail from users' Contacts when filtering junk e-mail.
If you enable this policy setting, the "Also trust E-mail from my Contacts" check box is selected in the Safe Senders tab of the Junk E-mail Options dialog and users cannot change it. E-mail addresses in users' Contacts list are treated as safe senders for purposes of filtering junk e-mail.
If you disable this policy setting, e-mail addresses in users' Contacts list are not treated as safe senders for purposes of filtering junk email, and users cannot change this configuration.
If you do not configure this policy setting, e-mail messages that are received from people who are listed in Contacts are considered safe by the Junk E-mail Filter, but users can change this configuration. The recommended state for this setting is: `Enabled`.

Rationale:

By default, e-mail addresses in users' Contacts list are treated as safe senders for purposes of filtering junk e-mail. If this configuration is changed, e-mail from users' Contacts might be misclassified as junk and cause important information to be lost.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\junkmail
trustcontacts
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Preferences\Junk E-mail\Trust e-mail from contacts
```

Impact:

Enabling this setting enforces the default configuration in Outlook, and is therefore unlikely to cause any significant usability issues for most users.

Default Value:

Not configured

1.9.8.5 Search Options

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.9 Right-to-Left

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.10 Spelling

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.9.11 (L1) Ensure 'Internet and Network Paths into Hyperlinks' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting specifies whether Outlook automatically turns text that represents Internet and network paths into hyperlinks. This option can also be configured by selecting the "Internet and network paths with hyperlinks" check box that is available on the Outlook | File | Options | Mail | Editor Options.... | Proofing | AutoCorrect Options… | AutoFormat tab on the user interface (UI).

If you enable or do not configure this policy setting, text in Outlook that represents internet and network paths are automatically turned into hyperlinks. This is the default behavior of Outlook.

If you disable this policy setting, text in Outlook that represents internet and network paths are not automatically turned into hyperlinks. The recommended state for this setting is: `Disabled.`

Rationale:

Users may receive emails from attackers that contain Internet or network paths to malicious content. Users may unintentionally click on hyperlinks if they are presented to the users automatically.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\16.0\Outlook\options\autoformat\pg
rfafo_25_1
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to Disabled.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook
Options\Internet and Network Paths into Hyperlinks
```

Impact:

Users will not be able to click on hyperlinks for Internet and network paths. Instead they will need to manually copy and paste the paths (if desired).

Default Value:

Not Configured

1.10 Outlook Social Connector

This section contains settings for configuring Outlook Social Connector.

1.10.1 (L1) Ensure 'Do Not Download Photos from Active Directory' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether contact photos are downloaded from the Active Directory.

If you enable this policy setting, contact photos are not downloaded.

If you disable or you do not configure this policy setting, contact photos are downloaded. The recommended state for this setting is: `Enabled`

Rationale:

Disabling or not configuring this setting allows Outlook to download contact photos from Active Directory. Photos downloaded from Active Directory could be shared on social networks, some organizations may not want portraits of their employees to circulate widely. For example: law enforcement, intelligence, and military agencies may need some of their staff to remain anonymous.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\Outlook\SocialConnector\DownloadPhotosFromAD
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Social Connector\Do Not Download Photos from Active Directory
```

Impact:

Enable this setting to prevent Outlook from downloading photos stored in Active Directory.

1.10.2 (L1) Ensure 'Turn Off Outlook Social Connector" is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to turn off the Outlook Social Connector.

If you enable this policy setting, the Outlook Social Connector is turned off.

If you disable or you do not configure this policy setting, the Outlook Social Connector is turned on. The recommended state for this setting is: `Enabled`

Rationale:

Disabling or not configuring this setting allows the Outlook Social Connector to remain which means that data may be synchronized between Outlook and the users' social networks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\Outlook\SocialConnector\RunOSC
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Outlook Social
Connector\Turn Off Outlook Social Connector
```

Impact:

Enabling this setting will disable the Outlook Social Connector, preventing users from synchronizing any data in Outlook with their social networks.

Default Value:

Not Configured

1.11 Outlook Today Settings

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.12 Search Folders

This section is intentionally blank and exists to ensure the structure of Outlook benchmarks is consistent.

1.13 Security

This section contains settings for configuring Security options.

1.13.1 Automatic Picture Download Settings

This section contains settings for configuring Automatic Picture Download Settings.

1.13.1.1 (L1) Ensure 'Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook automatically downloads external content in e-mail from senders in the Safe Senders List or Safe Recipients List.
If you enable this policy setting, Outlook automatically downloads content for e-mail from people in Safe Senders and Safe Recipients lists.
If you disable this policy setting, Outlook will not automatically download content from external servers for messages sent by people listed in users' Safe Senders Lists or Safe Recipients Lists. Recipients can choose to download external content on a message-by-message basis.
If you do not configure this policy setting, downloads are permitted when users receive e-mail from people listed in the user's Safe Senders List or Safe Recipients List. The recommended state for this setting is: `Disabled`.

Rationale:

Malicious e-mail senders can send HTML e-mail messages with embedded Web beacons, or pictures and other content from external servers that can be used to track whether specific recipients have opened a message. Viewing an e-mail message that contains a Web beacon provides confirmation that the recipient's e-mail address is valid, which leaves the recipient vulnerable to additional spam and harmful e-mail. To help protect users from Web beacons, Outlook can be configured to automatically block the display of external content in e-mail messages. However, because this configuration could block desirable content from display, Outlook can also be configured to automatically display external content in any messages sent by people who are listed in users' Safe Senders Lists or Safe Recipients Lists.
By default, Outlook automatically displays external content in e-mail messages from people listed in users' Safe Senders Lists or Safe Recipients Lists, and automatically blocks external content in other messages. If a malicious sender is accidentally added to a user's Safe

Senders List or Safe Recipients List, Outlook will display external content in all e-mail messages from the malicious sender, which could include Web beacons.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\unblockspecificsenders
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Automatic Picture Download Settings\Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists
```

Impact:

Disabling this setting means that Outlook does not automatically download external content for messages sent by people listed in users' Safe Senders Lists or Safe Recipients Lists. This configuration can cause some disruption for users who regularly receive HTML e-mail messages that contain graphics and other external content, because they will need to download content for each message individually.

Default Value:

Not configured

1.13.1.2 (L1) Ensure 'Block Trusted Zones' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether pictures from sites in the Trusted Sites security zone are automatically downloaded in Outlook e-mail messages and other items.
If you enable this policy setting, Outlook does not automatically download content from Web sites in the Trusted sites zone in Internet Explorer. Recipients can choose to download external content on a message-by-message basis.
If you disable or do not configure this policy setting, Outlook automatically downloads content from Web sites in the Trusted sites zone in Internet Explorer. The recommended state for this setting is: `Enabled`.

Rationale:

Malicious users can send HTML e-mail messages with embedded Web beacons, which are pictures and other content from external servers that can be used to track whether specific recipients open the message. Viewing an e-mail message that contains a Web beacon provides confirmation that the recipient's e-mail address is valid, which leaves the recipient vulnerable to additional spam and harmful e-mail.

To reduce the risk from Web beacons, Outlook disables external content in e-mail messages by default, unless the content is considered "safe" as determined by the check boxes in the Automatic Download section of the Trust Center. Depending on how these options are configured, safe content can include content in messages from addresses defined in the Safe Senders and Safe Recipients Lists used by the Junk E-mail filter, content from SharePoint discussion boards, and content from Web sites in the Trusted sites zone in Internet Explorer.

By default, Outlook considers trusted sites from Internet Explorer safe, and automatically downloads content from them, which could potentially include Web beacons.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\trustedz
one
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Automatic
Picture Download Settings\Block Trusted Zones
```

Impact:

Enabling this setting means that Outlook does not automatically download external content from Web sites in the Trusted sites zone. This configuration can cause some disruption for users who regularly receive HTML e-mail messages that contain graphics and other external content from sites in this zone, because they will need to download content for each message individually.

Default Value:

Not configured

1.13.1.3 (L1) Ensure 'Display pictures and external content in HTML e-mail' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook downloads untrusted pictures and external content located in HTML e-mail messages without users explicitly choosing to download them.
If you enable this policy setting, Outlook will not automatically download content from external servers unless the sender is included in the Safe Senders list. Recipients can choose to download external content from untrusted senders on a message-by-message basis.
If you disable this policy setting, Outlook does not display pictures and external content in HTML e-mail.
If you do not configure this policy setting, Outlook does not download external content in HTML e-mail and RSS items unless the content is considered safe. Content that Outlook can be configured to consider safe includes:

- Content in e-mail messages from senders and to recipients defined in the Safe Senders and Safe Recipients lists.
- Content from Web sites in Internet Explorer's Trusted Sites security zone.
- Content in RSS items.
- Content from SharePoint Discussion Boards. Users can control what content is considered safe by changing the options in the "Automatic Download" section of the Trust Center.

If Outlook's default blocking configuration is overridden, in the Trust Center or by some other method, Outlook will display external content in all HTML e-mail messages, including any that include Web beacons. The recommended state for this setting is: `Enabled`.

Rationale:

Malicious e-mail senders can send HTML e-mail messages with embedded Web beacons, which are pictures and other content from external servers that can be used to track whether specific recipients open the message. Viewing an e-mail message that contains a Web beacon provides confirmation that the recipient's e-mail address is valid, which leaves the recipient vulnerable to additional spam and harmful e-mail.

By default, Outlook does not download external content in HTML e-mail and RSS items unless the content is considered safe. Content that Outlook can be configured to consider safe includes:

- Content in e-mail messages from senders and to recipients defined in the Safe Senders and Safe Recipients lists.
- Content from Web sites in Internet Explorer's Trusted Sites security zone.
- Content in RSS items.
- Content from SharePoint Discussion Boards.

Users can control what content is considered safe by changing the options in the Automatic Download section of the Trust Center. If Outlook's default blocking configuration is overridden, in the Trust Center or by some other method, Outlook will display external content in all HTML e-mail messages, including any that include Web beacons.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\blockextcontent
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Automatic Picture Download Settings\Display pictures and external content in HTML e-mail
```

Impact:

Enabling this setting enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Default Value:

Not configured

1.13.1.4 (L1) Ensure 'Do not permit download of content from safe zones' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook automatically downloads content from safe zones when displaying messages.
If you enable this policy setting, Outlook will not automatically download content from safe zones. Recipients can choose to download external content from untrusted senders on a message-by-message basis.
If you disable this policy setting, content from safe zones will be downloaded automatically.
If you do not configure this policy setting, Outlook automatically downloads content from sites that are considered "safe," as defined in the Security tab of the Internet Options dialog box in Internet Explorer.
Important - Note that this policy setting is "backward." Despite the name, disabling the policy setting prevents the download of content from safe zones and enabling the policy setting allows it. The recommended state for this setting is: `Disabled`.

Rationale:

By default, Outlook automatically downloads content from sites that are considered "safe," as defined in the Security tab of the Internet Options dialog box in Internet Explorer. This configuration could allow users to inadvertently download Web beacons that reveal their identity to spammers and other malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\unblocksafezone
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Automatic Picture Download Settings\Do not permit download of content from safe zones
```

Impact:

Disabling this setting can cause some disruptions for Outlook users who receive many e-mail messages that include content from safe zones, because they will be required to download content for each message individually.

Default Value:

Not configured

1.13.2 Cryptography

This section contains settings for configuring Cryptography within Outlook.

1.13.2.1 Signature Status Dialog Box

This section contains settings for configuring Signature Status Dialog Box within Outlook.

1.13.2.1.1 (L1) Ensure 'Attachment Secure Temporary Folder' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to specify a folder path for the Secure Temporary Files folder rather than using the one that is randomly generated by Outlook.
If you enable this policy setting, you can specify a folder path for the Security Temporary Files folder rather than using the one that is randomly generated by Outlook.
If you disable or do not configure this policy setting, Outlook will assign the Secure Temporary Files folder a different random name for each user.
Important - If you must use a specific folder for Outlook attachments, it is recommended that you use a local directory (for best performance), that you place the folder under the Temporary Internet Files folder (to benefit from the enhanced security on that folder), and that the folder name is unique and difficult to guess. The recommended state for this setting is: `Disabled`.

Rationale:

The Secure Temporary Files folder is used to store attachments when they are opened in e-mail. By default, Outlook generates a random name for the Secure Temporary Files folder and saves it in the Temporary Internet Files folder. You can use this setting to designate a specific path and folder to use as the Secure Temporary Files folder. This configuration is not recommended, because it means that all users will have temporary Outlook files in the same predictable location, which is not as secure. If the name of this folder is well known, a malicious user or malicious code might target this location to try and gain access to attachments.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Status dialog box\Attachment Secure Temporary
Folder
```

Impact:

Disabling this setting enforces the default configuration of Outlook, and therefore is unlikely to cause usability issues for most users.
Important If you must use a specific folder for Outlook attachments, it is recommended that you use a local directory (for best performance), that you place the folder under the Temporary Internet Files folder (to benefit from the enhanced security on that folder), and that the folder name is unique and difficult to guess.

Default Value:

Not configured

1.13.2.1.2 (L1) Ensure 'Missing CRLs' is set to Enabled:Error (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook considers a missing certificate revocation list (CRL) a warning or an error. Digital certificates contain an attribute that shows where the corresponding CRL is located. CRLs contain lists of digital certificates that have been revoked by their controlling certification authorities (CAs), typically because the certificates were issued improperly or their associated private keys were compromised. If a CRL is missing or unavailable, Outlook cannot determine whether a certificate has been revoked. Therefore, an improperly issued certificate or one that has been compromised might be used to gain access to data.
If you enable this policy setting, you can choose between two options that determine how Outlook functions when a CRL is missing:

- Warning. This option is the default configuration in Outlook and ensures that Outlook displays a warning message when a CRL is missing.
- Error. This option ensures that Outlook displays an error message when a CRL is missing.

If you disable or do not configure this policy setting, Outlook displays a warning message when a CRL is not available. The recommended state for this setting is: `Enabled:Error`.

Rationale:

Digital certificates contain an attribute that shows where the corresponding CRL is located. CRLs contain lists of digital certificates that have been revoked by their controlling certification authorities (CAs), typically because the certificates were issued improperly or their associated private keys were compromised.
If a CRL is missing or unavailable, Outlook cannot determine whether a certificate has been revoked. Therefore, an improperly issued certificate or one that has been compromised might be used to gain access to data.
By default, Outlook displays a warning message when a CRL is not available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Status dialog box\Missing CRLs
```

Then set the `Indicate a missing CRL as a(n):` option to `Error`.

Impact:

Enabling this setting and choosing "Error" from the drop-down list will prevent Outlook users from using certificates when the appropriate CRL is not available to verify them, which could increase desktop support requests.

Default Value:

Not configured

1.13.2.1.3 (L1) Ensure 'Missing Root Certificates' is set to Enabled:Warning (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Outlook functions when a root certificate is missing.
If you enable this policy setting, you can choose from three options that determine how Outlook functions when a CRL is missing.
- Neither Error nor Warning. This option displays neither an error nor a warning, and enforces the default configuration in Outlook.
- Warning. This option ensures that Outlook displays a warning message when a CRL is missing.
- Error. This option ensures that Outlook displays an error message when a CRL is missing.
If you disable or do not configure this policy setting, users are not prompted with a warning or an error when a root certificate cannot be located. The recommended state for this setting is: `Enabled:Warning`.

Rationale:

When Outlook accesses a certificate, it validates that it can trust the certificate by examining the root certificate of the issuing CA. If the root certificate can be trusted, then certificates issued by the CA can also be trusted.
If Outlook cannot find the root certificate, it cannot validate that any certificates issued by that CA can be trusted. An attacker may compromise a root certificate and then remove the certificate in an attempt to conceal the attack.
By default, users are not prompted with a warning or an error when a root certificate cannot be located.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Status dialog box\Missing root certificates
```

Then set the `Indicate a missing root certificate as a(n):` option to `Warning`.

Impact:

Enabling this setting will prevent Outlook users from using certificates when the appropriate root certificate is not available to verify them, which could increase desktop support requests.

Default Value:

Not configured

1.13.2.1.4 (L1) Ensure 'Promote Level 2 errors as errors, not warnings' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to treat Level 2 errors as warnings instead of errors. Level 2 errors occur when the message signature appears to be valid, but there are other issues with the signature.
If you enable this policy setting, Level 2 errors will be treated as warnings.
If you disable or do not configure this policy setting, Level 2 errors will be treated as errors
When you specify a value for PromoteErrorsAsWarnings, note that potential Level 2 error conditions include the following:

- Unknown Signature Algorithm
- No Signing Certification Found
- Bad Attribute Sets
- No Issuer Certificate found
- No CRL Found
- Out-of-date CRL
- Root Trust Problem
- Out-of-date CTL

The recommended state for this setting is: `Disabled`.

Rationale:

Cryptographic errors in Outlook are classified as Level 1 (serious errors) or Level 2 (not as serious). By default, Outlook generates a warning, rather than an error, when a level 2 condition occurs: the certificate that generated the warning is treated as valid, and the user is not informed of the problem unless he or she opens the Signature Details dialog box and examines the certificate. Potential level 2 conditions include the following:

- Unknown Signature Algorithm
- No Signing Certification Found
- Bad Attribute Sets
- No Issuer Cert found
- No CRL Found
- Out of Date CRL
- Root Trust Problem

- Out of Date CRT

In some cases, treating level 2 conditions as warnings can cause users to overlook potentially significant signature problems.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\promoteerror
saswarnings
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Status dialog box\Promote Level 2 errors as
errors, not warnings
```

Impact:

Disabling this setting can cause disruptions for users who work with digital certificates in Outlook. These users may experience an increased number of errors that prevent them from working effectively with e-mail, which could increase desktop support requests.

Default Value:

Not configured

1.13.2.1.5 (L1) Ensure 'Retrieving CRLs (Certificate Revocation Lists)' is set to Enabled:When online always retrieve the CRL (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Outlook retrieves Certificate Revocation Lists to verify the validity of certificates. Certificate revocation lists (CRLs) are lists of digital certificates that have been revoked by their controlling certificate authorities (CAs), typically because the certificates were issued improperly or their associated private keys were compromised.
If you enable this policy setting, you can choose from three options to govern how Outlook uses CRLs:

- Use system Default. Outlook relies on the CRL download schedule that is configured for the operating system.
- When online always retrieve the CRL. This option is the default configuration in Outlook.
- Never retrieve the CRL. Outlook will not attempt to download the CRL for a certificate, even if it is online. This option can reduce security.

If you disable or do not configure this policy setting, when Outlook handles a certificate that includes a URL from which a CRL can be downloaded, Outlook will retrieve the CRL from the provided URL if Outlook is online. The recommended state for this setting is: `Enabled:When online always retrieve the CRL`.

Rationale:

Certificate revocation lists (CRLs) are lists of digital certificates that have been revoked by their controlling certificate authorities (CAs), typically because the certificates were issued improperly or their associated private keys were compromised.

By default, when Outlook handles a certificate that includes a URL from which a CRL can be downloaded, Outlook will retrieve the CRL from the provided URL if Outlook is online. If this configuration is changed, Outlook might improperly trust a revoked certificate, which could put users' computers and data at risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Status dialog box\Retrieving CRLs (Certificate
Revocation Lists)
```

Then set the . . . option to `When online always retrieve the CRL`.

Impact:

The recommended setting enforces the default configuration in Outlook, and therefore is unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.13.2.2 (L1) Ensure 'Do not display 'Publish to GAL' button' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook users can publish e-mail certificates to the Global Address List (GAL).
If you enable this policy setting, the "Publish to GAL" button does not display in the "E-mail Security" section of the Trust Center.
If you disable or do not configure this policy setting, Outlook users can publish their e-mail certificates to the GAL through the "E-mail Security" section of the Trust Center. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Outlook users can publish their e-mail certificates to the GAL through the E-mail Security section of the Trust Center. If your organization has policies that govern the use of digital certificates for signing and encrypting e-mail messages, allowing users to publish certificates might violate those policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\publishtogal
disabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Do not display 'Publish to GAL' button
```

Impact:

Enabling this setting prevents Outlook users from publishing their e-mail certificates to the GAL. Users who need to publish a new or updated certificate will have to contact an administrator.

Default Value:

Not configured

1.13.2.3 (L1) Ensure 'Do not provide Continue option on Encryption warning dialog boxes' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Outlook users are allowed to send e-mail messages after they see an encryption warning.
If you enable this policy setting, encryption warning dialog boxes do not contain a Continue button, which means that users must cancel the sending operation entirely.
If you disable or do not configure this policy setting, if Outlook users see an encryption-related dialog box when attempting to send a message, they can choose to dismiss the warning and send the message anyway. The recommended state for this setting is: `Enabled`.

Rationale:

By default, if Outlook users see an encryption-related dialog box when attempting to send a message, they can choose to dismiss the warning and send the message anyway. If users send messages after seeing an encryption error, it is likely that recipients will not be able to read them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\disablecontinueencryption
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Cryptography\Do not provide Continue option on Encryption warning dialog boxes
```

Impact:

Enabling this setting can cause disruptions if Outlook users attempt to send messages with encryption errors, although the errors themselves would likely cause disruptions in most cases if the messages were allowed to be sent.

Default Value:

Not configured

1.13.2.4 (L1) Ensure 'Message Formats' is set to Enabled:S/MIME and Fortezza (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls which message encryption formats Outlook can use. Outlook supports three formats for encrypting and signing messages: S/MIME, Exchange, and Fortezza.
If you enable this policy setting, you can specify whether Outlook can use S/MIME (the default), Exchange, or Fortezza encryption, or any combination of any of these options. Users will not be able to change this configuration.
If you disable or do not configure this policy setting, Outlook only uses S/MIME to encrypt and sign messages. If you disable this policy setting, users will not be able to change this configuration. The recommended state for this setting is: `Enabled:S/MIME and Fortezza`.

Rationale:

E-mail typically travels over open networks and is passed from server to server. Messages are therefore vulnerable to interception, and attackers might read or alter their contents. It is therefore important to have a mechanism for signing messages and providing end-to-end encryption.
Outlook supports three formats for encrypting and signing messages: S/MIME, Exchange, and Fortezza. By default, Outlook only uses S/MIME to encrypt and sign messages. If your organization has policies that mandate the use of specific encryption formats, allowing users to choose freely between these formats could cause them to violate such policies.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Message Formats
```

Then set the `Support the following message formats:` option to `S/MIME and Fortezza`.

Impact:

Enabling this setting and selecting "S/MIME, Exchange, and Fortezza" from the drop-down list adds support for Fortezza, a hardware based encryption standard created by the National Security Agency (NSA), a division of the United States Department of Defense. If your organization uses Fortezza, you will have to use this setting to add support for Fortezza to Outlook. The recommended SSLF configuration does not eliminate support for S/MIME, so implementing this recommendation should not affect users who need access to the S/MIME encryption and signing functionality in Outlook.

Default Value:

Not configured

1.13.2.5 (L1) Ensure 'Minimum Encryption Settings:' is set to Enabled:168 (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to set the minimum key length for an encrypted e-mail message.
If you enable this policy setting, you may set the minimum key length for an encrypted e-mail message. Outlook will display a warning dialog if the user tries to send a message using an encryption key that is below the minimum encryption key value set. The user can still choose to ignore the warning and send using the encryption key originally chosen.
If you disable or do not configure this policy setting, a dialog warning will be shown to the user if the user attempts to send a message using encryption. The user can still choose to ignore the warning and send using the encryption key originally chosen. The recommended state for this setting is: `Enabled:168`.

Rationale:

Cryptographic keys are used to encrypt and decrypt messages for transmission through unsecured channels. Key sizes are measured in bits, with larger keys generally less vulnerable to attack than smaller ones. 40-bit and 56-bit keys were common in the past, but as computers have become faster and more powerful these smaller key sizes have become vulnerable to brute-force attacks in which the attacking computer rapidly runs through every possible key combination until it successfully decrypts the message. The Advanced Encryption Standard (AES) published by the United States government requires a minimum key size of 128 bits for symmetric encryption, which offers significantly more protection against brute-force attack than smaller key sizes.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Minimum encryption settings
```

Then set the `Minimum key size (in bits)`: option to `168`.

Impact:

Users who see the minimum encryption warning display can still choose to send the message with the selected key, so enabling this setting is unlikely to cause significant disruptions.
128-bit encryption has been widely implemented for several years. Therefore, enabling this setting is unlikely to cause any usability issues for users.

Default Value:

Not configured

1.13.2.6 (L1) Ensure 'S/MIME interoperability with external clients' is set to Enabled:Handle internally (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook decodes encrypted messages itself or passes them to an external program for processing.
If you enable this policy setting, you can choose from three options for configuring external S/MIME clients:
- Handle internally. Outlook decrypts all S/MIME messages itself.
- Handle externally. Outlook hands all S/MIME messages off to the configured external program.
- Handle if possible. Outlook attempts to decrypt all S/MIME messages itself. If it cannot decrypt a message, Outlook hands the message off to the configured external program. This option is the default configuration.
If you disable or do not configure this policy setting, the behavior is the equivalent of selecting Enabled Handle if possible. The recommended state for this setting is: `Enabled:Handle internally`.

Rationale:

In some situations, administrators might wish to use an external program, such as an add-in, to handle S/MIME message decryption. If your organization works with encrypted messages that the decryption functionality in Outlook cannot handle appropriately, this setting can be used to configure Outlook to hand S/MIME messages off to an external program for decryption. If no external program has been authorized, however, misconfiguring this setting could allow unauthorized and potentially dangerous programs to handle encrypted messages, which could compromise security.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\S/MIME interoperability with external clients
```

Then set the `Behavior for handling S/MIME messages:` option to `Handle internally`.

Impact:

The recommended configuration for this setting is "Handle internally," which enforces the default configuration in Outlook and is therefore unlikely to cause usability issues for most users. If you have a designated external program that you would like to use for handling S/MIME messages, you will need to select one of the other two options from the drop-down menu.

Default Value:

Not configured

1.13.2.7 (L1) Ensure 'S/MIME receipt requests behavior' is set to Enabled:Never send S/MIME receipts (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Outlook handles S/MIME receipt requests.
If you enable this policy setting, you can choose from four options for handling S/MIME receipt requests in Outlook:
- Open message if receipt can't be sent
- Don't open message if receipt can't be sent
- Always prompt before sending receipt
- Never send S/MIME receipts
If you disable or do not configure this policy setting, when users open messages with attached receipt requests, Outlook prompts them to decide whether to send a receipt to the sender with information about the identity of the user who opened the message and the time it was opened. If Outlook cannot send the receipt, the user is still allowed to open the message. The recommended state for this setting is: `Enabled:Never send S/MIME receipts`.

Rationale:

Incoming signed or encrypted messages might include S/MIME receipt requests. S/MIME receipts provide confirmation that messages are received unaltered, and can include information about who opened the message and when it was opened.
By default, when users open messages with attached receipt requests, Outlook prompts them to decide whether to send a receipt to the sender with information about the identity of the user who opened the message and the time it was opened. If Outlook cannot send the receipt, the user is still allowed to open the message.
In some situations, allowing Outlook to automatically send receipt requests could cause sensitive information to be divulged to unauthorized people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\S/MIME receipt requests behavior
```

Then set the `Handle messages with S/MIME receipt requests in the following manner:` option to `Never send S/MIME receipts`.

Impact:

Configuring this setting to "Never send S/MIME receipts" does not affect users' ability to open and read e-mail messages. However, people who send messages with attached receipt requests to users affected by this setting will not receive the requested S/MIME receipts, which could cause confusion. Consider educating users about this setting so that they can advise e-mail correspondents to not expect any receipts they request.

Default Value:

Not configured

1.13.2.8 (L1) Ensure 'Send all signed messages as clear signed messages' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook sends signed messages as clear text signed messages.
If you enable this policy setting, the "Send clear text signed message when sending signed messages" option is selected in the E-mail Security section of the Trust Center.
If you disable or do not configure this policy setting, when users sign e-mail messages with their digital signature and send them, Outlook uses the signature's private key to encrypt the digital signature but sends the messages as clear text, unless they are encrypted separately. The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users sign e-mail messages with their digital signature and send them, Outlook uses the signature's private key to encrypt the digital signature but sends the messages as clear text, unless they are encrypted separately. If users change this functionality by clearing the Send clear text signed message when sending signed messages option in the E-mail Security section of the Trust Center, any recipients who are unable to access or use the sender's digital certificate will not be able to read the e-mail messages.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\clearsign
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Send all signed messages as clear signed messages
```

Impact:

Enabling this setting enforces the default configuration in Outlook, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not configured

1.13.2.9 (L1) Ensure 'Signature Warning' is set to Enabled:Always warn about invalid signatures (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Outlook warns users about messages with invalid digital signatures.
If you enable this policy setting, you can choose from three options for controlling how Outlook users are warned about invalid signatures:
- Let user decide if they want to be warned. This option enforces the default configuration.
- Always warn about invalid signatures.
- Never warn about invalid signatures.
If you disable or do not configure this policy setting, if users open e-mail messages that include invalid digital signatures, Outlook displays a warning dialog. Users can decide whether they want to be warned about invalid signatures in the future. The recommended state for this setting is: `Enabled:Always warn about invalid signatures`.

Rationale:

By default, if users open e-mail messages that include invalid digital signatures, Outlook displays a warning dialog box. Users can decide whether they want to be warned about invalid signatures in the future.
If users are not notified about invalid signatures, they might be prevented from detecting a fraudulent signature sent by a malicious person.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook
2016\Security\Cryptography\Signature Warning
```

Then set the `Signature Warning` option to `Always warn about invalid signatures`.

Impact:

Enabling this setting could cause some disruptions for Outlook users who receive a lot of messages signed with invalid signatures. These users will see a warning dialog box every time they open such a message.

Default Value:

Not configured

1.13.3 Security Form Settings

This section contains settings for configuring Security Form Settings within Outlook.

1.13.3.1 Attachment Security

This section contains settings for configuring Attachment Security within Outlook.

1.13.3.1.1 (L1) Ensure 'Allow users to demote attachments to Level 2' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook users can demote attachments to Level 2 by using a registry key, which will allow them to save files to disk and open them from that location. Outlook uses two levels of security to restrict access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.
If you enable this policy setting, users can create a list of Level 1 file types to demote to Level 2 by adding the file types to the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Security\Level1Remove.
If you disable or do not configure this policy setting, users cannot demote level 1 attachments to level 2, and the
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Security\Level1Remove registry key has no effect. The recommended state for this setting is: `Disabled`.

Rationale:

Outlook uses two levels of security to restrict access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.
By default, Outlook does not allow users to demote file types from Level 1 to Level 2. If this setting is Enabled, users can create a list of Level 1 file types to demote to Level 2 by adding the file types to the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\15.0\Security\Level1Remove
If users can demote Level 1 files to Level 2, they will be able to access potentially dangerous files after saving them to disk, which could allow malicious code to affect their computers or compromise the security of sensitive information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\allowuserstolowerattachments
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security\Allow users to demote attachments to Level 2
```

Impact:

Allowing users to demote attachments to Level 2 can pose a significant risk. Unless your users have a legitimate business need for such functionality, this setting should be disabled.

Default Value:

Not configured

1.13.3.1.2 (L1) Ensure 'Display Level 1 attachments' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook blocks potentially dangerous attachments designated Level 1. To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict access to files attached to e-mail messages or other items. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.

The recommended state for this setting is: `Disabled`.

Rationale:

To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict access to files attached to e-mail messages or other items. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.

By default, Outlook completely blocks access to Level 1 files, and requires users to save Level 2 files to disk before opening them. If this configuration is changed, users will be able to open and execute potentially dangerous attachments, which can affect their computers or compromise the confidentiality, integrity, or availability of data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\showlevel1attach
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security\Display Level 1 attachments
```

Impact:

See Attachment file types restricted by Office for the full list of file types classified Level 1 by default.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.1.3 (L1) Ensure 'Do not prompt about Level 1 attachments when closing an item' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook displays a warning before closing an item that contains an unsafe attachment that will be blocked when the item is re-opened. To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict users' access to files attached to e-mail messages or other items. Outlook completely blocks access to Level 1 files by default, and requires users to save Level 2 files to disk before opening them. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.
If you enable this policy setting, Outlook will not display a warning when users close items with Level 1 attachments, which could cause data loss.
If you disable or do not configure this policy setting, when a user closes an item to which a level 1 file has been attached, Outlook warns the user that the message contains a potentially unsafe attachment and that the user might not be able to access the attachment when opening the item later. (Such a sequence of events might occur when a user closes a draft message that they intend to resume editing at some future time.)
The recommended state for this setting is: `Disabled`.

Rationale:

To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict users' access to files attached to e-mail messages or other items. Outlook completely blocks access to Level 1 files by default, and requires users to save Level 2 files to disk before opening them. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.
By default, when a user closes an item to which a level 1 file has been attached, Outlook warns the user that the message contains a potentially unsafe attachment and that the user might not be able to access the attachment when opening the item later. (Such a sequence of events might occur when a user closes a draft message that they intend to resume editing at some future time.) If this configuration is changed, Outlook will not display the warning when the user closes the item but will still block the unsafe attachment if the user opens the message later. This functionality can cause users to lose access to important data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\dontpromptlevel1attachclose
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security\Do not prompt about Level 1 attachments when closing an item
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.1.4 (L1) Ensure 'Do not prompt about Level 1 attachments when sending an item' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook displays a warning before sending an item that contains an unsafe attachment that will be blocked when the item is opened by a recipient. To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict access to files attached to e-mail messages or other items. Outlook completely blocks access to Level 1 files by default, and requires users to save Level 2 files to disk before opening them. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.
If you enable this policy setting, Outlook will not display a warning when a user sends an item with a Level 1 attachment, which can cause users' data to be at risk.
If you disable or do not configure this policy setting, when users attempt to send an item to which a level 1 file has been attached, Outlook warns them that the message contains a potentially unsafe attachment and that the recipient might not be able to access it.
The recommended state for this setting is: `Disabled`.

Rationale:

To protect users from viruses and other harmful files, Outlook uses two levels of security, designated Level 1 and Level 2, to restrict access to files attached to e-mail messages or other items. Outlook completely blocks access to Level 1 files by default, and requires users to save Level 2 files to disk before opening them. Potentially harmful files can be classified into these two levels by file type extension, with all other file types considered safe.
By default, when users attempt to send an item to which a level 1 file has been attached, Outlook warns them that the message contains a potentially unsafe attachment and that the recipient might not be able to access it. If this configuration is changed, Outlook will not display the warning when users send such items, which can cause users to lose access to important data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\dontpromptlevel1attachsend
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security\Do not prompt about Level 1 attachments when sending an item
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.1.5 (L1) Ensure 'Remove file extensions blocked as Level 1' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls which types of attachments (determined by file extension) Outlook prevents from being delivered.

Outlook uses two levels of security to restrict users' access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, you can specify the removal of file type extensions as that Outlook classifies as Level 1--that is, to be blocked from delivery--by entering them in the text field provided separated by semicolons.

If you disable or do not configure this policy setting, Outlook classifies a number of potentially harmful file types (such as those with .exe, .reg, and .vbs extensions) as Level 1 and blocks files with those extensions from being delivered.

The recommended state for this setting is: `Disabled`.

Rationale:

Malicious code is often spread through e-mail. Some viruses have the ability to send copies of themselves to other people in the victim's Address Book or Contacts list, and such potentially harmful files can affect the computers of unwary recipients.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security
Form Settings\Attachment Security\Remove file extensions blocked as Level 1\: Removed
Extensions:
```

Impact:

Disabling this setting will cause any extensions that are already on the list will be ignored, which means that Outlook will block access to them again. This configuration could cause disruptions for users who are accustomed to sending and receiving such files.

Default Value:

Not configured

1.13.3.1.6 (L1) Ensure 'Remove file extensions blocked as Level 2' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls which types of attachments (determined by file extension) must be saved to disk before users can open them. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, you can specify a list of attachment file types to classify as Level 2, which forces users to actively decide to download the attachment to view it.

If you disable or do not configure this policy setting, Outlook does not classify any file type extensions as Level 2.

Important: This policy setting only applies if the "Outlook Security Mode" policy setting under "Microsoft Outlook <version>\Security\Security Form Settings" is configured to "Use Outlook Security Group Policy." The recommended state for this setting is: `Disabled`.

Rationale:

Malicious code is often spread through e-mail. Some viruses have the ability to send copies of themselves to other people in the victim's Address Book or Contacts list, and such potentially harmful files can affect the computers of unwary recipients.

Outlook uses two levels of security to restrict users' access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.
By default, Outlook classifies a number of potentially harmful file types as Level 1. (See Attachment file types restricted by Outlook for the complete list.) Outlook does not classify any file types as Level 2 by default, so this setting is not particularly useful in isolation. Typically, if there are extensions on the Level 2 list they would have been added by using the "Add file extensions to block as Level 2" setting, through which they can be removed. The combined lists of blocked and restricted file extensions that Outlook uses are actually

built by combining various policies together. If a machine policy classifies an extension as Level 2, this setting could be used to remove the extension from the list in some situations. As with Level 1 extensions, though, removing restrictions on potentially dangerous extensions can make it easier for users to open dangerous files, which can significantly reduce security.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security\Remove file extensions blocked as Level 2\: Removed Extensions:
```

Impact:

Disabling this setting enforces the default configuration, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not configured

1.13.3.2 Custom Form Security

This section contains settings for configuring Custom Form Security within Outlook.

1.13.3.2.1 (L1) Ensure 'Allow scripts in one-off Outlook forms' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether scripts can run in Outlook forms in which the script and layout are contained within the message.
If you enable this policy setting, scripts can run in one-off Outlook forms.
If you disable or do not configure this policy setting, Outlook does not run scripts in forms in which the script and the layout are contained within the message.
Important: This policy setting only applies if the "Outlook Security Mode" policy setting under "Microsoft Outlook <version>\Security\Security Form Settings" is configured to "Use Outlook Security Group Policy." The recommended state for this setting is: `Disabled`.

Rationale:

Malicious code can be included within Outlook forms, and such code could be executed when users open the form.
By default, Outlook does not run scripts in forms in which the script and the layout are contained within the message.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\enableoneoff
formscripts
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security
Form Settings\Custom Form Security\Allow scripts in one-off Outlook forms
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and is therefore unlikely to cause significant usability issues for most users.
Allowing scripts to run in one-off Outlook forms can pose a significant risk. Unless your users have a legitimate business need for such functionality, this setting should be disabled. If your organization uses forms with scripts, consider redesigning these forms.

Default Value:

Not configured

1.13.3.2.2 (L1) Ensure 'Outlook Object Model Custom Actions Execution Prompt' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook prompts users before executing a custom action. Custom actions add functionality to Outlook that can be triggered as part of a rule. Among other possible features, custom actions can be created that reply to messages in ways that circumvent the Outlook model's programmatic send protections.
If you enable this policy setting, you can choose from four options to control how Outlook functions when a custom action is executed that uses the Outlook object model:

- Prompt User
- Automatically Approve
- Automatically Deny
- Prompt user based on computer security. This option enforces the default configuration in Outlook.

If you disable or do not configure this policy setting, when Outlook or another program initiates a custom action using the Outlook object model, users are prompted to allow or reject the action. If this configuration is changed, malicious code can use the Outlook object model to compromise sensitive information or otherwise cause data and computing resources to be at risk. This is the equivalent of choosing Enabled -- Prompt user based on computer security. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

Custom actions add functionality to Outlook that can be triggered as part of a rule. Among other possible features, custom actions can be created that reply to messages in ways that circumvent the Outlook model's programmatic send protections.
By default, when Outlook or another program initiates a custom action using the Outlook object model, users are prompted to allow or reject the action. If this configuration is changed, malicious code can use the Outlook object model to compromise sensitive information or otherwise cause data and computing resources to be at risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Custom Form Security\Set Outlook object model custom actions execution prompt\Set Outlook object model custom actions execution prompt
```

Then set the `When executing a custom action:` option to `Automatically Deny`.

Impact:

Configuring this setting to "Automatically Deny" prevents Outlook from executing any custom actions that use the Outlook object model. If your users rely on any such actions, you may have to find alternate methods for providing this functionality.

Default Value:

Not configured

1.13.3.3 Programmatic Security

This section contains settings for configuring Programmatic Security settings within Outlook.

1.13.3.3.1 Trusted Add-ins

This section contains settings for configuring Trusted Add-ins settings.

1.13.3.3.1.1 (L1) Ensure 'Configure Trusted Add-ins' to 'Disabled' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting can be used to specify a list of trusted add-ins that can be run without being restricted by the security measures in Outlook.

If you enable this policy setting, a list of trusted add-ins and hashes is made available that you can modify by adding and removing entries. The list is empty by default. To create a new entry, enter a DLL file name in the ''Value Name'' column and the hash result in the ''Value'' column.

If you disable or do not configure this policy setting, the list of trusted add-ins is empty and unused, so the recommended EC and SSLF settings do not create any usability issues. However, users who rely on add-ins that access the Outlook object model might be repeatedly prompted unless administrators enable this setting and add the add-ins to the list.

Note - You can also configure Exchange Security Form settings by enabling the ''Outlook Security Mode'' setting in User Configuration\Administrative Templates\Microsoft Outlook <version>\Security\Security Form Settings\Microsoft Outlook Security and selecting ''Use Outlook Security Group Policy'' from the drop-down list. The recommended state for this setting is: `Disabled`.

Rationale:

The Outlook object model includes entry points to access Outlook data, save data to specified locations, and send e-mail messages, all of which can be used by malicious application developers. To help protect these entry points, the Object Model Guard warns users and prompts them for confirmation when untrusted code, including add-ins, attempts to use the object model to obtain e-mail address information, store data outside of Outlook, execute certain actions, and send e-mail messages.

To reduce excessive security warnings when add-ins are used, administrators can specify a list of trusted add-ins that can access the Outlook object model silently, without raising prompts. This trusted add-in list should be treated with care, because a malicious add-in could access and forward sensitive information if added to the list.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Trusted Add-ins\Configure trusted add-ins
```

Impact:

By default, the list of trusted add-ins is empty and unused, so configuring this setting does not create any usability issues. However, users who rely on add-ins that access the Outlook object model might be repeatedly prompted unless administrators enable this setting and add the add-ins to the list.

Note You can also configure Exchange Security Form settings by enabling the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and selecting Use Outlook Security Group Policy from the drop-down list.

For more information about the Object Model Guard, see Security Behavior of the Outlook Object Model in the MSDN Outlook Developer Reference.

Default Value:

Not configured

1.13.3.3.2 (L1) Ensure 'Configure Outlook object model prompt when accessing an address book: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when an untrusted program attempts to gain access to an Address Book using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to programmatically access an Address Book using the Outlook object model:

- Prompt user - Users are prompted to approve every access attempt.

- Automatically approve - Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny - Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security - Outlook will rely on the setting in the ''Programmatic Access'' section of the Trust Center. This is the default behavior.

If you disable or do not configure this policy setting, when an untrusted application attempts to access the address book programmatically, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

If an untrusted application accesses the address book, the application could gain access to sensitive data and potentially change that data.

By default, when an untrusted application attempts to access the address book programmatically, Outlook relies on the setting configured in the "Programmatic Access"

section of the Trust Center. This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.

Note: This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt when accessing an address book
```

Then set the `Configure Outlook object model prompt when accessing an address book: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates

(ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

For more information about the Object Model Guard, see Security Behavior of the Outlook Object Model in the MSDN Outlook Developer Reference.

Default Value:

Not configured

1.13.3.3.3 (L1) Ensure 'Configure Outlook object model prompt When accessing the Formula property of a UserProperty object: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when a user designs a custom form in Outlook and attempts to bind an Address Information field to a combination or formula custom field.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to access address information using the UserProperties. Find method of the Outlook object model:

- Prompt user. The user will be prompted to approve every access attempt.

- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny. Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running.

If you disable or do not configure this policy setting, when a user tries to bind an address information field to a combination or formula custom field in a custom form, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center.The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

A custom form in Outlook could be used to gain access to sensitive address book data and potentially to change that data.

By default, when a user tries to bind an address information field to a combination or formula custom field in a custom form, Outlook relies on the setting configured in the

"Programmatic Access" section of the Trust Center. This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.

Note: This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt When accessing the Formula property of a UserProperty object
```

Then set the `Configure Outlook object model prompt When accessing the Formula property of a UserProperty object: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates

(ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

For more information about the Object Model Guard, see Security Behavior of the Outlook Object Model in the MSDN Outlook Developer Reference.

Default Value:

Not configured

1.13.3.3.4 (L1) Ensure 'Configure Outlook object model prompt when executing Save As: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when an untrusted program attempts to use the Save As command to programmatically save an item.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to use the Save As command to programmatically save an item:

- Prompt user. The user will be prompted to approve every access attempt.

- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny. Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to use the Save As command, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

If an untrusted application uses the Save As command to programmatically save an item, the application could add malicious data to a user's inbox, a public folder, or an address book.

By default, when an untrusted application attempts to use the Save As command, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.

Note: This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt when executing Save As
```

Then set the `Configure Outlook object model prompt when executing Save As: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates

(ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

For more information about the Object Model Guard, see Security Behavior of the Outlook Object Model in the MSDN Outlook Developer Reference.

Default Value:

Not configured

1.13.3.3.5 (L1) Ensure 'Configure Outlook object model prompt when reading address information: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when an untrusted program attempts to gain access to a recipient field, such as the ''To:'' field, using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to access a recipient field using the Outlook object model:

- Prompt user. The user will be prompted to approve every access attempt.

- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny. Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to access recipient fields, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

If an untrusted application accesses the recipient fields, the application could gain access to sensitive data and potentially change that data. This could result in mail being sent to the wrong party.

By default, when an untrusted application attempts to access recipient fields, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center. This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.

Note: This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt when reading address information
```

Then set the `Configure Outlook object model prompt when reading address information: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important: For this setting to apply, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft

Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.3.6 (L1) Ensure 'Configure Outlook object model prompt when responding to meeting and task requests: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when an untrusted program attempts to programmatically send e-mail in Outlook using the Response method of a task or meeting request.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to programmatically send e-mail using the Response method of a task or meeting request:

- Prompt user. The user will be prompted to approve every access attempt.

- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny. Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security. Outlook only prompts users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to respond to tasks or meeting requests programmatically, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

If an untrusted application programmatically responds to tasks or meeting requests, that application could impersonate a user response to the tasks or meeting requests with false information.

By default, when an untrusted application attempts to respond to tasks or meeting

requests programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center. This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.
Note This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt when responding to meeting and task requests\Configure Outlook object model prompt when responding to meeting and task requests
```

Then set the `Configure Outlook object model prompt when responding to meeting and task requests: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Note: For this setting to apply, you must also enable the "Outlook Security Mode" setting in

User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.3.7 (L1) Ensure 'Configure Outlook object model prompt when sending mail: Guard behavior:' is set to Enabled:Automatically Deny (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls what happens when an untrusted program attempts to send e-mail programmatically using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to send e-mail programmatically using the Outlook object model:

- Prompt user - The user will be prompted to approve every access attempt.

- Automatically approve - Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.

- Automatically deny - Outlook will automatically deny programmatic access requests from any program.

- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running.

Important: This policy setting only applies if the ''Outlook Security Mode'' policy setting under ''Microsoft Outlook <version>\Security\Security Form Settings'' is configured to ''Use Outlook Security Group Policy.''

If you disable or do not configure this policy setting, when an untrusted application attempts to send mail programmatically, Outlook relies on the setting configured in the ''Programmatic Access'' section of the Trust Center. The recommended state for this setting is: `Enabled:Automatically Deny`.

Rationale:

If an untrusted application programmatically sends e-mail, that application could send mail that includes malicious code, impersonate a user, or launch a denial-of-service attack by sending a large volume of mail to a user or group of users.

By default, when an untrusted application attempts to send mail programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center. This setting determines whether Outlook will warn users about programmatic access attempts:

- Only when antivirus software is out of date or not running (the default setting)
- Every time
- Not at all

If the "Not at all" option is selected, Outlook will silently grant programmatic access to any program that requests it, which could allow a malicious program to gain access to sensitive information.
Note: This described default functionality assumes that you have not followed the recommendation to enable the "Outlook Security Mode" Group Policy setting to ensure that Outlook security settings are configured by Group Policy. If Group Policy security settings are used for Outlook, the "Programmatic Access" section of the Trust Center is not used. In this situation, the default is to prompt users based on computer security, which is the equivalent of the "Only when antivirus software is out of date or not running" option in the Trust Center, and the user experience is not affected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Configure Outlook object model prompt when sending mail
```

Then set the `Configure Outlook object model prompt when sending mail: Guard behavior:` option to `Automatically Deny`.

Impact:

Enabling this setting and selecting Prompt user based on computer security enforces the default configuration in Outlook, and therefore is unlikely to cause usability issues for most users.

Important: If this setting is enabled, you must also enable the "Outlook Security Mode" setting in User Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Outlook <version>\Security\Security Form Settings\Microsoft Office Outlook Security and select Use Outlook Security Group Policy from the drop-down list.

Default Value:

Not configured

1.13.3.4 (L1) Ensure 'Outlook Security Mode' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls which set of security settings are enforced in Outlook.

If you enable this policy setting, you can choose from four options for enforcing Outlook security settings:

* Outlook Default Security - This option is the default configuration in Outlook. Users can configure security themselves, and Outlook ignores any security-related settings configured in Group Policy.

* Use Security Form from 'Outlook Security Settings' Public Folder - Outlook uses the settings from the security form published in the designated public folder.

* Use Security Form from 'Outlook 10 Security Settings' Public Folder - Outlook uses the settings from the security form published in the designated public folder.

* Use Outlook Security Group Policy - Outlook uses security settings from Group Policy.

Important - You must enable this policy setting if you want to apply the other Outlook security policy settings mentioned in this guide.

If you disable or do not configure this policy setting, Outlook users can configure security for themselves, and Outlook ignores any security-related settings that are configured in Group Policy.

Note - In previous versions of Outlook, when security settings were published in a form in Exchange Server public folders, users who needed these settings required the HKEY_CURRENT_USER\Software\Policies\Microsoft\Security\CheckAdminSettings registry key to be set on their computers for the settings to apply. In Outlook, the CheckAdminSettings registry key is no longer used to determine users' security settings. Instead, the Outlook Security Mode setting can be used to determine whether Outlook security should be controlled directly by Group Policy, by the security form from the Outlook Security Settings Public Folder, or by the settings on users' own computers The recommended state for this setting is: `Enabled:Use Outlook Security Group Policy`.

Rationale:

If users can configure security themselves, they might choose levels of security that leave their computers vulnerable to attack.

By default, Outlook users can configure security for themselves, and Outlook ignores any security-related settings that are configured in Group Policy.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
```

Then set the `Outlook Security Policy:` option to `Use Outlook Security Group Policy`.

Impact:

Enabling this setting prevents users from modifying their own security settings, so it might cause an increase in support calls. However, this setting is essential for ensuring that the other Outlook security settings mentioned in this baseline are applied as suggested.

Note In previous versions of Outlook, when security settings were published in a form in Exchange Server public folders, users who needed these settings required the HKEY_CURRENT_USER\Software\Policies\Microsoft\Security\CheckAdminSettings registry key to be set on their computers for the settings to apply. In Outlook, the CheckAdminSettings registry key is no longer used to determine users' security settings. Instead, the Outlook Security Mode setting can be used to determine whether Outlook security should be controlled directly by Group Policy, by the security form from the Outlook Security Settings Public Folder, or by the settings on users' own computers.

Default Value:

Not configured

1.13.4 Trust Center

This section contains settings for configuring Trust Center within Outlook.

1.13.4.1 (L1) Ensure 'Allow hyperlinks in suspected phishing e-mail messages' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether hyperlinks in suspected phishing e-mail messages in Outlook are allowed.
If you enable this policy setting, Outlook will allow hyperlinks in suspected phishing messages that are not also classified as junk e-mail.
If you disable or do not configure this policy setting, Outlook will not allow hyperlinks in suspected phishing messages, even if they are not classified as junk e-mail. The recommended state for this setting is: `Disabled`.

Rationale:

Outlooks Junk E-mail Filter evaluates each incoming message for possible spam or phishing content. Suspicious message detection is always turned on.

By default, Outlook handles suspicious messages in two ways:

- If the Junk E-mail Filter does not consider a message to be spam but does consider it to be phishing, the message is left in the Inbox but any links in the message are disabled and users cannot use the Reply and Reply All functionality. In addition, any attachments in the suspicious message are blocked.
- If the Junk E-mail Filter considers the message to be both spam and phishing, the message is automatically sent to the Junk E-mail folder. Any message sent to the Junk E-mail folder is converted to plain text format and all links are disabled. In addition, the Reply and Reply All functionality is disabled and any attachments in the message are blocked.

The InfoBar alerts users to this change in functionality. If users are certain that a message is legitimate, they can click the InfoBar and enable the links in the message.

Users can change the way Outlook handles phishing messages in the Junk E-mail Options dialog box by clearing the Disable links and other functionality in phishing messages

(Recommended) check box. If this check box is cleared, Outlook will not disable links in suspected phishing messages unless they are classified as junk e-mail, which could allow users to disclose confidential information to malicious Web sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\options\mail\junkmail
enablelinks
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Trust
Center\Allow hyperlinks in suspected phishing e-mail messages
```

Impact:

Disabling this setting enforces the default configuration in Outlook, and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.13.4.2 (L1) Ensure 'Apply macro security settings to macros, add-ins and additional actions' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether Outlook also applies the macro security settings to installed COM add-ins and additional actions.
If you enable this policy setting, the macro security settings will also be applied to add-ins and additional actions.
If you disable or do not configure this policy setting, Outlook does not use the macro security settings to determine whether to run macros, installed COM add-ins, and additional actions. The recommended state for this setting is: `Enabled`.

Rationale:

Attackers can insert malicious code into add-ins and smart tags in an attempt to affect your computing environment. By default, COM add-ins and smart tags are not subject to the same security restrictions as installed macros.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\donttrustinstalledfiles
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Trust Center\Apply macro security settings to macros, add-ins and additional actions
```

Impact:

When this setting is Enabled and a strong security level is chosen for macros, add-ins and smart tags will run under greater security restrictions. This configuration might have an impact on users that use add-ins and smart tags.

Default Value:

Not configured

1.13.4.3 (L1) Ensure 'Security Ensureting for Macros' is set to Enabled:Never warn, disable all (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the security level for macros in Outlook.
If you enable this policy setting, you can choose from four options for handling macros in Outlook:

- Always warn. This option corresponds to the "Warnings for all macros" option in the "Macro Security" section of the Outlook Trust Center. Outlook disables all macros that are not opened from a trusted location, even if the macros are signed by a trusted publisher. For each disabled macro, Outlook displays a security alert dialog box with information about the macro and its digital signature (if present), and allows users to enable the macro or leave it disabled.
- Never warn, disable all. This option corresponds to the "No warnings and disable all macros" option in the Trust Center. Outlook disables all macros that are not opened from trusted locations, and does not notify users.
- Warning for signed, disable unsigned. This option corresponds to the "Warnings for signed macros; all unsigned macros are disabled" option in the Trust Center. Outlook handles macros as follows:
    - If a macro is digitally signed by a trusted publisher, the macro can run if the user has already trusted the publisher.
    - If a macro has a valid signature from a publisher that the user has not trusted, the security alert dialog box for the macro lets the user choose whether to enable the macro for the current session, disable the macro for the current session, or to add the publisher to the Trusted Publishers list so that it will run without prompting the user in the future.
    - If a macro does not have a valid signature, Outlook disables it without prompting the user, unless it is opened from a trusted location.

This option is the default configuration in Outlook.

- No security check. This option corresponds to the "No security check for macros (Not recommended)" option in the Trust Center. Outlook runs all macros without prompting users. This configuration makes users' computers vulnerable to potentially malicious code and is not recommended.

If you disable or do not configure this policy setting, the behavior is the equivalent of Enabled -- Warning for signed, disable unsigned. The recommended state for this setting is: `Enabled:Never warn, disable all`.

Rationale:

To protect users from dangerous code, the Outlook default configuration disables all macros that are not trusted, including unsigned macros, macros with expired or invalid signatures, and macros with valid signatures from publishers who are not on users' Trusted Publishers lists. The default configuration also allows macros that are signed by trusted publishers to run automatically without notifying users, which could allow dangerous code to run.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Trust Center\Security setting for macros
```

Then set the `Security Level` option to `Never warn, disable all`.

Impact:

Configuring this setting to "Never warn, disable all" will cause Outlook users to lose the benefits of any functionality provided by macros. Users who wish to benefit from macros can install the macros in a trusted location, unless Disable all trusted locations is set to Enabled.

Default Value:

Not configured

1.13.5 (L1) Ensure 'Allow Active X One Off Forms' is set to Enabled:Load only Outlook Controls (Scored)

Profile Applicability:

- Level 1

Description:

By default, third-party ActiveX controls are not allowed to run in one-off forms in Outlook. You can change this behavior so that Safe Controls (Microsoft Forms 2.0 controls and the Outlook Recipient and Body controls) are allowed in one-off forms, or so that all ActiveX controls are allowed to run. The recommended state for this setting is: `Enabled:Load only Outlook Controls`.

Rationale:

If additional types of Active X controls are allowed, particularly un-trusted third-party controls, the risk of malware infecting the computer increases.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Allow Active X One Off Forms
```

Then set the `Allow Active X One Off Forms` option to `Load only Outlook Controls`.

Impact:

This setting enforces the default configuration and therefore should not have any effect on usability.

Default Value:

Not configured

1.13.6 (L1) Ensure 'Configure Add-In Trust Level' is set to Enabled:Trust all loaded and installed COM addins (Scored)

Profile Applicability:

- Level 1

Description:

All installed trusted COM addins can be trusted. Exchange Settings for the addins still override if present and this option is selected. The recommended state for this setting is: `Enabled:Trust all loaded and installed COM addins`.

Rationale:

Under normal circumstances the installed COM add-ins are applications that have been approved and intentionally deployed by the organization and therefore they should not pose a security threat. However, if malware has infected systems its possible that the malware will use the COM add-in feature to perform unauthorized actions.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Configure Add-In Trust Level
```

Then set the `Configure Add-In Trust Level` option to `Trust all loaded and installed COM addins`.

Impact:

This setting enforces the default configuration, and therefore is unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.13.7 (L1) Ensure 'Disable 'Remember password' for Internet e-mail accounts' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

Use this option to hide your user's ability to cache passwords locally in the computer's registry. When configured, this policy will hide the 'Remember Password' checkbox and not allow users to have Outlook remember their password.
Note that POP3, IMAP, and HTTP e-mail accounts are all considered Internet e-mail accounts in Outlook. E-mail account options are listed on the Server Type dialog box when users choose 'New' under Tools | Account Settings. The recommended state for this setting is: `Enabled`.

Rationale:

An attacker who is able to access the user's profile may be able to acquire these cached passwords, they could then use this information to compromise the user's email accounts and other systems that use the same credentials.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\enableremembe
rpwd
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Disable
'Remember password' for Internet e-mail accounts
```

Impact:

Enabling this setting can cause users to be frustrated because they will have to repeatedly enter their email account passwords for any email services that do not accept their Windows credentials. For Exchange servers that are members of the same Active Directory domain enabling this setting should not cause users to be prompted for their credentials

since Exchange will accept their domain credentials, but for Exchange servers in untrusted domains and other types of email accounts the users might be forced to reenter their password frequently.

Default Value:

Not configured

1.13.8 (L1) Ensure 'Do not automatically sign replies' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to specify whether replies will be automatically signed.
If you enable this policy setting, the option to respond automatically to a signed message with a signed response will be overridden, and an unsigned response will be the default reply to a signed message.
If you disable or do not configure this policy setting, a signed response will be the default reply to a signed message. The recommended state for this setting is: `Enabled`.

Rationale:

If digital signatures are automatically applied to all outbound messages its likely that some recipients will be unable to verify the signatures. This is due to the fact that most organizations will deploy digital certificates to users from their own internal Certification Authority (CA), which external users cannot access. Recipients of signed messages who are unable to confirm the validity of those signatures may feel unsafe viewing legitimate messages.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\security\nosignonreply
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Do not automatically sign replies
```

Impact:

This setting enforces the default configuration, and therefore is unlikely to cause significant usability issues for most users.

Default Value:

Not configured

1.13.9 (L1) Ensure 'Prevent users from customizing attachment security settings' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents users from overriding the set of attachments blocked by Outlook.
If you enable this policy setting users will be prevented from overriding the set of attachments blocked by Outlook. Outlook also checks the "Level1Remove" registry key when this setting is specified.
If you disable or do not configure this policy setting, users will be allowed to override the set of attachments blocked by Outlook. The recommended state for this setting is: `Enabled`.

Rationale:

If users are able to change the security settings for attachments, they could choose less secure values and increase the risk of unintentionally spreading malware.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\outlook\disallowattachmentcustomization
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Prevent users from customizing attachment security settings
```

Impact:

Enabling this setting cause some users to be frustrated that they cannot customize the attachment security settings, but in most environments this should not be a significant issue.

Default Value:

Not configured

1.13.10 (L1) Ensure "Prompt User To Choose Security Settings If Default settings Fail' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

Check to prompt the user to choose security settings if default settings fail; uncheck to automatically select. The recommended state for this setting is: `Disabled`.

Rationale:

Users may not have the necessary knowledge to make the best choices regarding Outlook security settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\Policies\Microsoft\Office\16.0\Outlook\security\forcedefault
profile
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft Outlook 2016\Security\Prompt
User To Choose Security Settings If Default Settings Fail
```

Impact:

Enabling this setting will prevent a prompt from appearing when the default security settings fail. This should rarely be an issue since the settings are unlikely to fail in the first place.

Default Value:

Not Configured

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Account Settings**		
1.1.1	**E-mail**		
1.1.2	**Exchange**		
1.1.2.1	**Cached Exchange Mode**		
1.1.2.2	**Offline Address Book**		
1.1.2.3	(L1) Ensure 'Authentication with Exchange server.' is set to 'Enabled:Kerberos/NTLM Password Authentication' (Scored)	☐	☐
1.1.2.4	(L1) Ensure 'Automatically configure profile based on Active Directory Primary SMTP address' is set to Enabled (Scored)	☐	☐
1.1.2.5	(L1) Ensure 'Do not allow users to change permissions on folders' is set to Enabled (Scored)	☐	☐
1.1.2.6	(L1) Ensure 'Enable RPC encryption' is set to Enabled (Scored)	☐	☐
1.1.3	**Exchange ActiveSync**		
1.1.4	**IMAP**		
1.1.5	**Internet Calendars**		
1.1.5.1	(L1) Ensure 'Automatically download attachments' is set to Disabled (Scored)	☐	☐
1.1.5.2	(L1) Ensure 'Do not include Internet Calendar integration in Outlook' is set to Enabled (Scored)	☐	☐
1.1.6	**RSS Feeds**		
1.1.6.1	(L1) Ensure 'Download full text of articles as HTML attachments' is set to Disabled (Scored)	☐	☐
1.1.6.2	(L1) Ensure 'Synchronize Outlook RSS Feeds with Common Feed List' is set to Disabled (Scored)	☐	☐
1.1.6.3	(L1) Ensure 'Turn Off RSS Feature' is set to Enabled (Scored)	☐	☐
1.1.7	**SharePoint Lists**		
1.2	**Customizable Error Messages**		
1.3	**Disable Items in User Interface**		
1.3.1	**Custom**		
1.3.2	**Predefined**		
1.4	**Form Region Settings**		
1.5	**InfoPath Integration**		
1.6	**Meeting Workspace**		
1.6.1	(L1) Ensure 'Check to disable users from adding entries to server list' is set to Enabled:Publish default, disallow others	☐	☐

	(Scored)		
1.7	**MIME to MAPI Conversion**		
1.8	**Miscellaneous**		
1.8.1	**Miscellaneous**		
1.8.2	**PST Settings**		
1.8.2.1	(L1) Ensure 'PST Null Data On Delete' is set to Enabled (Scored)	☐	☐
1.9	**Outlook Options**		
1.9.1	**Customize Ribbon**		
1.9.2	**Delegates**		
1.9.3	**Mail**		
1.9.3.1	**Compose Messages**		
1.9.4	**Mail Format**		
1.9.4.1	**International Options**		
1.9.4.2	**Internet Formatting**		
1.9.4.2.1	**Message Format**		
1.9.4.2.2	(L1) Ensure ' Outlook Rich Text Options' is set to Enabled (Scored)	☐	☐
1.9.4.2.3	(L1) Ensure 'Plain Text Options' is set to Disabled (Scored)	☐	☐
1.9.4.3	**Stationery and Fonts**		
1.9.4.4	(L1) Ensure 'Do not allow signatures for e-mail messages' to 'Disabled' (Scored)	☐	☐
1.9.5	**Mail Setup**		
1.9.6	**Other**		
1.9.6.1	**Advanced**		
1.9.6.1.1	**Reminder Options**		
1.9.6.1.2	(L1) Ensure 'Do not allow folders in non-default stores to be set as folder home pages' is set to Enabled (Scored)	☐	☐
1.9.6.1.3	(L1) Ensure 'Do not allow Outlook object model scripts to run for public folders' is set to Enabled (Scored)	☐	☐
1.9.6.1.4	(L1) Ensure 'Do not allow Outlook object model scripts to run for shared folders' is set to Enabled (Scored)	☐	☐
1.9.6.1.5	(L1) Ensure 'Use Unicode format when dragging e-mail message to file system' is set to Disabled (Scored)	☐	☐
1.9.6.2	**AutoArchive**		
1.9.6.3	(L1) Ensure 'Make Outlook the default program for E-mail, Contacts, and Calendar' is set to Enabled (Scored)	☐	☐
1.9.7	**Out of Office Assistant**		
1.9.8	**Preferences**		
1.9.8.1	**Calendar Options**		
1.9.8.1.1	**Free/Busy Options**		
1.9.8.1.2	**Office.com Sharing Service**		
1.9.8.1.2.1	(L1) Ensure 'Access to published calendars' is set to Enabled	☐	☐

	(Scored)		
1.9.8.1.2.2	(L1) Ensure 'Prevent publishing to a DAV server' is set to Enabled (Scored)	☐	☐
1.9.8.1.2.3	(L1) Ensure 'Prevent publishing to Office.com' is set to Enabled (Scored)	☐	☐
1.9.8.1.2.4	(L1) Ensure 'Restrict level of calendar details users can publish' is set to Enabled:Disables 'Full details' and 'Limited details' (Scored)	☐	☐
1.9.8.1.2.5	(L1) Ensure 'Restrict upload method' is set to Enabled (Scored)	☐	☐
1.9.8.1.3	**Planner Options**		
1.9.8.1.4	**Recurring Item Configuration**		
1.9.8.1.5	**Schedule View**		
1.9.8.2	**Contact Options**		
1.9.8.3	**E-mail Options**		
1.9.8.3.1	**Advanced E-mail Options**		
1.9.8.3.1.1	**Desktop Alert**		
1.9.8.3.2	**Tracking Options**		
1.9.8.3.3	(L1) Ensure 'Read e-mail as plain text' is set to Enabled (Scored)	☐	☐
1.9.8.3.4	(L1) Ensure 'Read signed e-mail as plain text' is set to Enabled (Scored)	☐	☐
1.9.8.4	**Junk E-mail**		
1.9.8.4.1	(L1) Ensure 'Add e-mail recipients to users' Safe Senders Lists' is set to Disabled (Scored)	☐	☐
1.9.8.4.2	(L1) Ensure 'Hide Junk Mail UI' is set to Disabled (Scored)	☐	☐
1.9.8.4.3	(L1) Ensure 'Junk E-mail protection level: Select level:' is set to Enabled:High (Scored)	☐	☐
1.9.8.4.4	(L1) Ensure 'Trust e-mail from contacts' is set to Enabled (Scored)	☐	☐
1.9.8.5	**Search Options**		
1.9.9	**Right-to-Left**		
1.9.10	**Spelling**		
1.9.11	(L1) Ensure 'Internet and Network Paths into Hyperlinks' is set to Disabled (Scored)	☐	☐
1.10	**Outlook Social Connector**		
1.10.1	(L1) Ensure 'Do Not Download Photos from Active Directory' is set to Enabled (Scored)	☐	☐
1.10.2	(L1) Ensure 'Turn Off Outlook Social Connector" is set to Enabled (Not Scored)	☐	☐
1.11	**Outlook Today Settings**		
1.12	**Search Folders**		
1.13	**Security**		

1.13.1	**Automatic Picture Download Settings**		
1.13.1.1	(L1) Ensure 'Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists' is set to Disabled (Scored)	☐	☐
1.13.1.2	(L1) Ensure 'Block Trusted Zones' is set to Enabled (Scored)	☐	☐
1.13.1.3	(L1) Ensure 'Display pictures and external content in HTML e-mail' is set to Enabled (Scored)	☐	☐
1.13.1.4	(L1) Ensure 'Do not permit download of content from safe zones' is set to Disabled (Scored)	☐	☐
1.13.2	**Cryptography**		
1.13.2.1	**Signature Status Dialog Box**		
1.13.2.1.1	(L1) Ensure 'Attachment Secure Temporary Folder' is set to Disabled (Scored)	☐	☐
1.13.2.1.2	(L1) Ensure 'Missing CRLs' is set to Enabled:Error (Scored)	☐	☐
1.13.2.1.3	(L1) Ensure 'Missing Root Certificates' is set to Enabled:Warning (Scored)	☐	☐
1.13.2.1.4	(L1) Ensure 'Promote Level 2 errors as errors, not warnings' is set to Disabled (Scored)	☐	☐
1.13.2.1.5	(L1) Ensure 'Retrieving CRLs (Certificate Revocation Lists)' is set to Enabled:When online always retrieve the CRL (Scored)	☐	☐
1.13.2.2	(L1) Ensure 'Do not display 'Publish to GAL' button' is set to Enabled (Scored)	☐	☐
1.13.2.3	(L1) Ensure 'Do not provide Continue option on Encryption warning dialog boxes' is set to Enabled (Scored)	☐	☐
1.13.2.4	(L1) Ensure 'Message Formats' is set to Enabled:S/MIME and Fortezza (Scored)	☐	☐
1.13.2.5	(L1) Ensure 'Minimum Encryption Settings:' is set to Enabled:168 (Scored)	☐	☐
1.13.2.6	(L1) Ensure 'S/MIME interoperability with external clients' is set to Enabled:Handle internally (Scored)	☐	☐
1.13.2.7	(L1) Ensure 'S/MIME receipt requests behavior' is set to Enabled:Never send S/MIME receipts (Scored)	☐	☐
1.13.2.8	(L1) Ensure 'Send all signed messages as clear signed messages' is set to Enabled (Scored)	☐	☐
1.13.2.9	(L1) Ensure 'Signature Warning' is set to Enabled:Always warn about invalid signatures (Scored)	☐	☐
1.13.3	**Security Form Settings**		
1.13.3.1	**Attachment Security**		
1.13.3.1.1	(L1) Ensure 'Allow users to demote attachments to Level 2' is set to Disabled (Scored)	☐	☐
1.13.3.1.2	(L1) Ensure 'Display Level 1 attachments' is set to Disabled (Scored)	☐	☐
1.13.3.1.3	(L1) Ensure 'Do not prompt about Level 1 attachments when closing an item' is set to Disabled (Scored)	☐	☐

1.13.3.1.4	(L1) Ensure 'Do not prompt about Level 1 attachments when sending an item' is set to Disabled (Scored)	☐	☐
1.13.3.1.5	(L1) Ensure 'Remove file extensions blocked as Level 1' is set to Disabled (Scored)	☐	☐
1.13.3.1.6	(L1) Ensure 'Remove file extensions blocked as Level 2' is set to Disabled (Scored)	☐	☐
1.13.3.2	**Custom Form Security**		
1.13.3.2.1	(L1) Ensure 'Allow scripts in one-off Outlook forms' is set to Disabled (Scored)	☐	☐
1.13.3.2.2	(L1) Ensure 'Outlook Object Model Custom Actions Execution Prompt' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3	**Programmatic Security**		
1.13.3.3.1	**Trusted Add-ins**		
1.13.3.3.1.1	(L1) Ensure 'Configure Trusted Add-ins' to 'Disabled' (Not Scored)	☐	☐
1.13.3.3.2	(L1) Ensure 'Configure Outlook object model prompt when accessing an address book: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3.3	(L1) Ensure 'Configure Outlook object model prompt When accessing the Formula property of a UserProperty object: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3.4	(L1) Ensure 'Configure Outlook object model prompt when executing Save As: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3.5	(L1) Ensure 'Configure Outlook object model prompt when reading address information: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3.6	(L1) Ensure 'Configure Outlook object model prompt when responding to meeting and task requests: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.3.7	(L1) Ensure 'Configure Outlook object model prompt when sending mail: Guard behavior:' is set to Enabled:Automatically Deny (Scored)	☐	☐
1.13.3.4	(L1) Ensure 'Outlook Security Mode' is set to Enabled (Scored)	☐	☐
1.13.4	**Trust Center**		
1.13.4.1	(L1) Ensure 'Allow hyperlinks in suspected phishing e-mail messages' is set to Disabled (Scored)	☐	☐
1.13.4.2	(L1) Ensure 'Apply macro security settings to macros, add-ins and additional actions' is set to Enabled (Scored)	☐	☐
1.13.4.3	(L1) Ensure 'Security Ensureting for Macros' is set to Enabled:Never warn, disable all (Scored)	☐	☐
1.13.5	(L1) Ensure 'Allow Active X One Off Forms' is set to	☐	☐

	Enabled:Load only Outlook Controls (Scored)		
1.13.6	(L1) Ensure 'Configure Add-In Trust Level' is set to Enabled:Trust all loaded and installed COM addins (Scored)	☐	☐
1.13.7	(L1) Ensure 'Disable 'Remember password' for Internet e-mail accounts' is set to Enabled (Scored)	☐	☐
1.13.8	(L1) Ensure 'Do not automatically sign replies' is set to Enabled (Scored)	☐	☐
1.13.9	(L1) Ensure 'Prevent users from customizing attachment security settings' is set to Enabled (Scored)	☐	☐
1.13.10	(L1) Ensure "Prompt User To Choose Security Settings If Default settings Fail' is set to Disabled (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
06-27-2013	1.0.0	Initial Release
09-30-2016	1.1.0	Removed 1.9.4.2.1.1 (L1) Ensure 'Message Format' is set to Enabled:Plain Text Ticket #18
09-30-2016	1.1.0	Modified 1.1.2.3 - 'Authentication with Exchange Server' setting breaks authentication with Office 365 Ticket #19
09-30-2016	1.1.0	Modified Titles and Structure to conform with CIS Standard.