CIS Microsoft Intune for Office Benchmark

v1.0.0 - 11-17-2023

Terms of Use

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

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

Table of Contents

Overview

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

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

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

This document, Security Configuration Benchmark for Microsoft Office, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Office 2016, 2019, 2021 LTSC and 365 Apps for Enterprise running on Windows 11, Windows 10, Windows 8.1, and Windows Server 2016/2019/2022.

This guide was tested using Microsoft 365 Apps for Enterprise (x64) running on Windows 10/11 (x64) operating systems. Settings were deployed using Microsoft Intune (Endpoint Manager) configuration profiles. Remediation instructions are tailored to use the settings catalog profile type across all sections.

These settings apply only to specific Volume licensed editions of Office:

- Office 365 Apps for Enterprise
- Office LTSC Professional Plus 2021
- Office Standard/Professional Plus 2019
- Office Standard/Professional Plus 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 Office applications on a Windows platform. This includes Microsoft Access, Excel, Outlook, PowerPoint, Publisher, and Word.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (general use)**
  - be the starting baseline for most organizations;
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

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

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

Acknowledgements

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

Contributor
Jennifer Jarose
Haemish Edgerton

Editor
Caleb Eifert

Recommendations

1 Computer Configuration

Configuration settings in this section only apply at the device or machine level and are stored in the registry under HKEY_LOCAL_MACHINE.

Ensure these settings are configured in the `Configuration profiles` area of Microsoft Intune admin center, with Platform `Windows 10 and later` and Profile Type `Settings catalog` selected.

How the settings are distributed and assigned between uniquely named profiles is up to the organization. CIS Build Kits will follow the standard Active Directory Group Policy method by demarcating between User and Device settings with each having a respective profile. Level 1 and Level 2 settings will also have uniquely named configuration profiles. Intune profiles that contain user settings can also apply to a machine account when assigned. Respective keys and values are written to HKEY_USERS.

1.1 Administrative Templates

1.1.1 MS Security Guide

This section contains recommendations from the MS Security Guide.

1.1.1.1 (L1) Ensure 'Block Flash activation in Office documents' is set to 'Enabled: Block all activation' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the Adobe Flash control can be activated by Office documents. Note that activation blocking applies only within Office processes.

"Block all activation" prevents the Flash control from being loaded, whether directly referenced by the document or indirectly by another embedded object.

The recommended state for this setting is: `Enabled: Block all activation`.

Rationale:

Adobe Flash was discontinued in 2020. Flash content has had a long history of exploitation by malicious software developers. Blocking will ensure Office does not execute any Flash content. Enforcing the default ensures that the system was not configured in an insecure way.

Impact:

None - this enforces the default behavior of Microsoft Office.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `Block all Flash activation`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\Common\COM Compatibility\Comment
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Block all activation`.

```
Administrative Templates\MS Security Guide\Block Flash activation in Office documents
```

Default Value:

Flash content is allowed by default, equivalent to Enabled: Allow all activation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●

1.1.1.2 (L1) Ensure 'Restrict legacy JScript execution for Office' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls JScript execution per Security Zone within Internet Explorer and WebBrowser Control (WebOC) for Office applications. JScript is Microsoft's legacy dialect of the ECMAScript standard that is used in Microsoft's Internet Explorer 11 and older.

If Enabled, Office applications will not execute legacy JScript for the Internet or Restricted Sites zones and users aren't notified by the application that legacy JScript execution is restricted. Modern JScript9 will continue to function for all zones.

The recommended state for this setting is: `Enabled: Access: 69632 Excel: 69632 OneNote: 69632 Outlook: 69632 PowerPoint: 69632 Project: 69632 Publisher: 69632 Visio: 69632 Word: 69632`

Rationale:

Development on the JScript engine ended and the component was deprecated with the release of Internet Explorer 8.0 in 2009, but the engine remained in all Windows OS versions as a legacy component inside IE. Due to this, it has been exploited by a number of bad actors over the years, including nation-states.

The following CVE's are associated with JSCRIPT vulnerabilities: CVE-2018-8653, CVE-2019-1367, CVE-2019-1429, and CVE-2020-0674

Impact:

It's important to determine whether legacy JScript is being used to provide business-critical functionality before enabling this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `69632`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\internet explorer\main\featurecontrol\FEATURE_RESTRICT_LEGACY_JSCRIPT_PER_SECURITY_ZONE:<application>.exe
```

Each application binary will have a value of `69632`: `excel.exe msaccess.exe mspub.exe onenote.exe outlook.exe powerpnt.exe visio.exe winproj.exe winword.exe`

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: 69632` for each application listed.

```
Administrative Templates\MS Security Guide\Restrict legacy JScript execution
for Office
```

Default Value:

Office blocks flash content by default.

References:

1. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/disabling-legacy-scripting-engine-jscript-in-internet-explorer/ba-p/1777563

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

1.2 Microsoft Office 2016 (Machine)

This section includes recommendations for Microsoft Office.

1.2.1 Customize

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

1.2.2 Global Options

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

1.2.3 Licensing Settings

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

1.2.4 Miscellaneous

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

1.2.5 Security Settings

This section contains settings to configure Security Settings.

1.2.5.1 IE Security

This section contains settings to configure IE Security.

1.2.5.1.1 (L1) Ensure 'Add-on Management' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting manages Internet Explorer add-ons — which add-ins are always enabled, always disabled (blocked), or configurable by the user.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Internet Explorer add-ons are pieces of code that run in Internet Explorer to provide additional functionality. Rogue add-ons may contain viruses or other malicious code.

Disabling or not configuring this setting could allow malicious code or users to become active on user computers or the network. For example, a malicious user can monitor and then use keystrokes that a user types into Internet Explorer. Even legitimate add-ons may demand resources that compromise the performance of Internet Explorer and the operating systems of user computers.

Impact:

Some legitimate programs, including ones from Microsoft, use add-ons to display documents, audio, and video in Internet Explorer. The organization's policy should incorporate approved, commonly used add-ons to avoid limiting important user functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT:"Office
Application.exe"
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT:excel.exe
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications':

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Add-on
Management
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

1.2.5.1.2 (L1) Ensure 'Bind to object' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting determines whether Microsoft Internet Explorer performs its typical safety checks on Microsoft ActiveX® controls when opening URLs that are passed to it by an Office application. By default, Internet Explorer performs additional safety checks when ActiveX controls are initialized. Specifically, it prevents the control from being created if the kill bit is set in the registry. It also checks the security settings for the zone of the URL in which the control is instantiated to determine whether the control can be safely initialized. For the same behavior of the selectable applications, such as Excel and Word when they instantiate the use of Internet Explorer, the policy must be Enabled and the applications selected.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Internet Explorer performs a number of safety checks before initializing an ActiveX control. It will not initialize a control if the kill bit for the control is set in the registry, or if the security settings for the zone in which the control is located do not allow it to be initialized.

This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). A security risk could occur if potentially dangerous controls are allowed to load.

Impact:

Enabling this setting can cause some disruptions for users who open Web pages that contain potentially dangerous ActiveX controls from Office applications. However, because any affected controls are usually blocked by default when Internet Explorer opens Web pages, most users should not experience significant usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_SAFE_BINDTOOBJECT\"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Bind to Object
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

1.2.5.1.3 (L1) Ensure 'Consistent Mime Handling' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. This policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent.

For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of trustable data.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Users can use Internet Explorer to unknowingly download malicious content disguised with an incorrect filename extension or incorrectly marked in the MIME header. Once downloaded, an incorrect handler can run the file, enabling the malicious content to cause damage to the user's system or network.

Impact:

Internet Explorer uses both the extension of the filename and the MIME information to decide how to handle a file. Enabling this setting requires that information in the MIME header matches the file extension provided. Since mismatched files will be blocked by enabling this setting, ensure that any web server under organizational control is set up correctly.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING\"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Consistent Mime Handling
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

1.2.5.1.4 (L1) Ensure 'Disable user name and password' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Internet Explorer opens URLs containing user information that are passed to it by an Office application.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

The Uniform Resource Locator (URL) standard allows user authentication to be included in URL strings in the form http://username:password@example.com. A malicious user might use this URL syntax to create a hyperlink that appears to open a legitimate Web site but actually opens a deceptive (spoofed) Web site. For example, the URL http://www.microsoft.com@example.com appears to open http://www.microsoft.com but actually opens http://example.com. To protect users from such attacks, Internet Explorer usually blocks any URLs using this syntax.

This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If user names and passwords in URLs are allowed, users could be diverted to dangerous Web pages, which could pose a security risk.

Impact:

Enabling this setting can cause some disruptions for users who open URLs containing user authentication information from Office applications. Because such URLs are blocked by default when Internet Explorer opens Web pages through conventional means, however, most users should not experience significant usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE\"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Disable User
Name and Password
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.2.5.1.5 (L1) Ensure 'Information Bar' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether the Information Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Information Bar is displayed for Internet Explorer processes.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

The information bar can help users to understand when potentially malicious content has been blocked. Some users may be confused, however, by the appearance of the bar or unsure about how to respond.

Impact:

The security bar will be enabled for each of the specified applications.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SECURITYBAND\"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Information Bar
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

1.2.5.1.6 (L1) Ensure 'Local Machine Zone Lockdown Security' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows for configuration of policy settings in the zone consistent with a selected security level; for example, Low, Medium Low, Medium, or High.

When Internet Explorer opens a Web page, it places restrictions on what the page can do, based on the page's Internet Explorer security zone. There are several possible security zones, each with different sets of restrictions. The security zone for a page is determined by its location. For example, pages that are located on the Internet will normally be in the more restrictive Internet security zone. They might not be allowed to perform some operations, such as accessing the local hard drive. Pages that are located on your corporate network would normally be in the Intranet security zone, and therefore have fewer restrictions.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Local Machine zone security applies to all local files and content. This feature helps to mitigate attacks where the Local Machine zone is used as an attack vector to load malicious HTML code.

Impact:

If you enable this policy setting, the Local Machine zone security applies to all local files and content processed by the specified applications. If you disable or do not configure this policy setting, Local Machine zone security is not applied to local files or content processed by the specified applications.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Local Machine
Zone Lockdown Security
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.2.5.1.7 (L1) Ensure 'Mime Sniffing Safety Feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether Internet Explorer MIME sniffing prevents promotion of a file of one type to a more dangerous file type. For example, it does not allow script to run from a file marked as text. For Office, this setting affects any web-based content that is accessed within Office.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

MIME file-type spoofing is a potential threat to your organization. It is recommended that you ensure these files are consistently handled to help prevent malicious file downloads that may infect your network.

Impact:

When set to Enabled, MIME sniffing will not promote a file of one type to a more dangerous file type. If you disable this policy setting, MIME sniffing configures Internet Explorer processes to allow promotion of a file from one type to a more dangerous file type. For example, a text file could be promoted to an executable file, which is dangerous because any code in the supposed text file would be executed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING\"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Mime Sniffing
Safety Feature
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.2.5.1.8 (L1) Ensure 'Navigate URL' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Internet Explorer attempts to load malformed URLs that are passed to it from Office applications.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

To protect users from attacks, Internet Explorer usually does not attempt to load malformed URLs. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If Internet Explorer attempts to load a malformed URL, a security risk could occur in some cases.

Impact:

Enabling this setting does not block any legitimate URLs and is therefore unlikely to cause usability issues for any Office users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_VALIDATE_NAVIGATE_URL\"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Navigate URL
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●

1.2.5.1.9 (L1) Ensure 'Object Caching Protection' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting defines whether a reference to an object is accessible when the user navigates within the same domain or to a new domain. For Office, this applies to URLs accessed within Office applications. By default, in Internet Explorer, a reference to an object is no longer accessible when the user browses to a new domain. There is a new security context for all scriptable objects so that access to all cached objects is blocked. Additionally, access is blocked when browsing within the same domain (fully qualified domain name). A reference to an object is no longer accessible after the context has changed due to navigation.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

A malicious website may try to use object references from other domains.

Impact:

If you enable this policy setting, object reference is no longer accessible when navigating within or across domains for each specified application. If you disable or do not configure this policy setting, object reference is retained when navigating within or across domains in the Restricted Zone sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_OBJECT_CACHING:"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Object Caching Protection
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.2.5.1.10 (L1) Ensure 'Protection From Zone Elevation' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents processes running in one zone from being elevated to higher privileges in another zone. Zone elevation attacks can be severe and happen relatively frequently.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Internet Explorer places restrictions on each web page that users can use the browser to open. Web pages on a user's local computer have the fewest security restrictions and reside in the Local Machine zone, making this security zone a prime target for malicious users and code.

Disabling or not configuring this setting could allow pages in the Internet zone to navigate to pages in the Local Machine zone to then run code to elevate privileges. This could allow malicious code or users to become active on user computers or the network.

Impact:

Websites that rely on navigation to other higher privileged sites may not properly function. To allow such websites to properly function, use the settings catalog to add them to the Trusted sites zone.

NOTE: Enabling this setting also disables JavaScript navigation if no security context is present.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION:"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Protection From Zone Elevation
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.2.5.1.11 (L1) Ensure 'Restrict ActiveX Install' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables blocking of ActiveX control installation prompts for Internet Explorer processes. Users often choose to install software such as ActiveX controls that are not permitted by their organization's security policy. Such software can pose significant security and privacy risks to networks.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Microsoft ActiveX controls allow unmanaged, unprotected code to run on the user computers. ActiveX controls do not run within a protected container in the browser like other types of HTML or Microsoft Silverlight-based controls.

Disabling or not configuring this setting does not block prompts for ActiveX control installations and these prompts display to users. This could allow malicious code to become active on user computers or the network.

Impact:

Microsoft ActiveX controls allow unmanaged, unprotected code to run on the user computers. ActiveX controls do not run within a protected container in the browser like other types of HTML or Microsoft Silverlight-based controls.

Disabling or not configuring this setting does not block prompts for ActiveX control installations and these prompts display to users. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_RESTRICT_ACTIVEXINSTALL:"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Restrict
ActiveX Install
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

1.2.5.1.12 (L1) Ensure 'Restrict File Download' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting suppresses file download prompts that are not user-initiated. In certain circumstances, websites can initiate file download prompts without interaction from users. This technique can allow websites to put unauthorized files on users' hard drives if they click the wrong button and accept the download.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Disabling this setting allows websites to present file download prompts via code without the user specifically initiating the download. User preferences may also allow the download to occur without prompting or interacting with the user. Even if Internet Explorer prompts the user to accept the download, some websites abuse this functionality. Malicious websites may continually prompt users to download a file or present confusing dialog boxes to trick users into downloading or running a file.

If the download occurs and it contains malicious code, the code could become active on user computers or the network.

Impact:

User-initiated downloads can still occur, so the majority of legitimate user download interactions remain unaffected.

It is possible that some advanced users may expect their user preferences to control this behavior, and for this reason they may be confused when this preference is overridden by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD:"Office Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Restrict File Download
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

1.2.5.1.13 (L1) Ensure 'Saved from URL' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Internet Explorer evaluates URLs passed to it by Office applications for Mark of the Web (MOTW) comments.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Typically, when Internet Explorer loads a Web page from a UNC share that contains a Mark of the Web (MOTW) comment indicating the page was saved from a site on the Internet, Internet Explorer runs the page in the Internet security zone instead of the less restrictive Local Intranet security zone. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a Web page). If Internet Explorer does not evaluate the page for a MOTW, potentially dangerous code could be allowed to run.

Impact:

Enabling this setting can cause some Web pages saved on UNC shares to run in a more restrictive security zone when opened from Office applications than they would if the setting were disabled or not configured. However, a page with a MOTW indicating it was saved from an Internet site is presumed to have been designed to run in the Internet zone in the first place, so most users should not experience significant usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_UNC_SAVEDFILECHECK:"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Saved from URL
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●

1.2.5.1.14 (L1) Ensure 'Scripted Window Security Restrictions' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the Scripted Window Security Restrictions security feature, which restricts pop-up windows and prohibits scripts from displaying windows title and status bars in a way that is not visible to the user, or hides other windows title and status bars.

The recommended state for this setting is: `Enabled: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, winword.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe`.

Rationale:

Malicious websites often try to confuse or trick users into giving a site permission to perform an action allowing the site to take control of the users' computers in some manner. Disabling or not configuring this setting allows unknown websites to:

• Create browser windows that appear to be from the local operating system.

• Draw active windows that display outside of the viewable areas of the screen that can capture keyboard input.

• Overlay parent windows with their own browser windows to hide important system information, choices, or prompts.

Impact:

It is unlikely that any valid applications would use such deceptive methods to accomplish a task. For this reason, it is unlikely that organizations may encounter any major limitations due to using this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each Office application executable will have a unique value name with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_UNC_SAVEDFILECHECK:"Office
Application.exe"
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Check all applications`:

```
Microsoft Office 2016 (Machine)\Security Settings\IE Security\Scripted Window
Security Restrictions
```

Default Value:

Not Configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

1.2.6 Updates

This section contains settings to configure Updates.

1.2.6.1 (L1) Ensure 'Enable Automatic Updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the Office automatic updates are enabled or disabled for all Office products installed by using Click-to-Run.

Note: This policy has no effect on Office products installed via Windows Installer.

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

Rationale:

Security updates help prevent malicious attacks on Office applications. Timely application of Office updates helps ensure the security of devices and the applications running on the devices. Without these updates, devices and the applications running on those devices are more susceptible to security attacks.

Impact:

Office updates for Click-to-Run installations of Microsoft Office are applied in the background and have no adverse effect on users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\16.0\common\officeupdate:enableautomaticupdates
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Office 2016 (Machine)\Updates\Enable Automatic Updates
```

Default Value:

Enabled. (Office periodically checks for updates. When updates are detected, Office downloads and applies them in the background.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●

1.2.6.2 (L1) Ensure 'Hide option to enable or disable updates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if the user interface (UI) options to enable or disable Office automatic updates is visible to users. These options are found in the Product Information area of all Office applications installed via Click-to-Run. This policy setting has no effect on Office applications installed via Windows Installer.

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

Rationale:

Security updates help prevent malicious attacks on Office applications. Timely application of Office updates helps ensure the security of devices and the applications running on the devices. Without these updates, devices and the applications running on those devices are more susceptible to security attacks.

Enabling this policy setting helps prevent users from disabling automatic updates for Office.

Impact:

Office updates for Click-to-Run installations of Microsoft Office are applied in the background and have no adverse effect on users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKLM\SOFTWARE\Policies\Microsoft\office\16.0\common\officeupdate:hideenabledisableupdates
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Office 2016 (Machine)\Updates\Hide option to enable or disable updates
```

Default Value:

Disabled. (The Enable Update and Disable Updates options are visible, and users can enable or disable Office automatic updates from the UI.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●

2 User Configuration

Configuration settings in this section only apply at the user level and are stored in the registry under HKEY_USERS.

Ensure these settings are configured in the `Configuration profiles` area of Microsoft Intune admin center, with Platform `Windows 10 and later` and Profile Type `Settings catalog` selected.

How the settings are distributed and assigned between uniquely named profiles is up to the organization. CIS Build Kits will follow the standard Active Directory Group Policy method by demarcating between User and Device settings with each having a respective profile. Level 1 and Level 2 settings will also have uniquely named configuration profiles. Intune profiles that contain user settings can also apply to a machine account when assigned. Respective keys and values are written to HKEY_USERS.

2.1 Microsoft Access 2016

This section includes recommendations for Microsoft Access.

2.1.1 Application Settings

This section contains settings to configure Application Settings.

2.1.1.1 General

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

2.1.1.2 International

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

2.1.1.3 Security

This section contains settings to configure Security Options.

2.1.1.3.1 Cryptography

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

2.1.1.3.2 Trust Center

This section contains settings to configure Trust Center.

2.1.1.3.2.1 Trusted Locations

This section contains settings to configure Trusted Locations.

2.1.1.3.2.1.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether trusted locations on the network can be used. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe by the application opening the file.

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

Rationale:

Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. These custom locations added by users are ignored but not removed. Trusted locations added that specify a network location are also ignored.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security\trusted
locations:allownetworklocations
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Access 2016\Application Settings\Security\Trust Center\Trusted
Locations\Allow Trusted Locations on the network
```

Default Value:

Disabled. (Microsoft Access treats network locations as non-trusted but users can override.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.1.3.2.1.2 (L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications.

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

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

All trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2016 during setup, deployed to users using policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security\trusted
locations:alllocationsdisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Access 2016\Application Settings\Security\Trust Center\Trusted
Locations\Disable all trusted locations
```

Default Value:

Disabled. (All trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.1.3.2.2 (L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the blocking of macros from running in Office files that come from the internet.

By enabling this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Users will receive a notification that macros are blocked from running.

The exceptions when macros will be allowed to run are:

- The Office file is saved to a Trusted Location.
- The Office file was previously trusted by the user.
- Macros are digitally signed and the matching Trusted Publisher certificate is installed on the device.

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

Rationale:

Windows will mark files downloaded from the internet within an alternative NTFS data stream on the file. Files from untrusted sources can contain malicious payloads embedded in the Macros, including fileless malware, and should be handled with extra care by utilizing additional security controls.

Impact:

This enforces the default behavior and should not cause additional impact.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security:blockcontentexec
utionfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Access 2016\Application Settings\Security\Trust Center\Block macros
from running in Office files from the internet
```

Default Value:

Enabled. (Macros are blocked)

References:

1. https://learn.microsoft.com/en-us/DeployOffice/security/internet-macros-blocked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.1.1.3.2.3 (L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification.

Note: For this policy to apply the *Require that application add-ins are signed by Trusted Publisher* policy setting needs to be enabled. This will prevent users from changing the *Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them* policy setting.

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

Rationale:

Allowing unsigned application add-ins could cause the application to load dangerous add-ins and as a result, malicious code could become active on user computer and the network.

Impact:

If an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled, and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security:notbpromptunsignedaddin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Access 2016\Application Settings\Security\Trust Center\Disable
Trust Bar Notification for unsigned application add-ins and block them
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.1.1.3.2.4 (L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether add-ins for the specified Office applications must be digitally signed by a trusted publisher.

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

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Not configuring this setting may allow an application to load a dangerous add-in and as a result, malicious code could become active on a user's computer or the network.

Impact:

This setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store but does not write information to this store.

If a list of trusted publishers in a previous version of Office was created and upgrade the Office release, the trusted publisher list will still be recognized.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security:requireaddinsig
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Access 2016\Application Settings\Security\Trust Center\Require that application add-ins are signed by Trusted Publisher
```

Default Value:

Disabled. (This application does not check the digital signature on application add-ins before opening them.)

References:

1. https://learn.microsoft.com/en-us/deployoffice/security/trusted-publisher
2. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-publishers-certificate-store

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.1.1.4 Web Options...

This section contains settings to configure Web Options.

2.1.1.4.1 General

This section contains settings to configure General Options.

2.1.1.4.1.1 (L1) Ensure 'Underline hyperlinks' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether hyperlinks in Access tables, queries, forms, and reports are underlined.

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

Rationale:

Access underlines hyperlinks that appear in tables, queries, forms, and reports. If this configuration is changed, users might click on dangerous hyperlinks without realizing it, which could pose a security risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\internet:donotunderlinehyperlinks
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Access 2016\Application Settings\Web Options...\General\Underline hyperlinks
```

Default Value:

Enabled. (Access underlines all hyperlinks but users can override.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.2 Customizable Error Messages

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

2.1.3 Disable Items in User Interface

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

2.1.4 Miscellaneous

This section contains settings to configure Miscellaneous Options.

2.1.4.1 (L1) Ensure 'Default file format' is set to 'Enabled: Access 2007' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether new database files are created in the new Access format or in a format used by earlier versions of Access.

The recommended state for this setting is: `Enabled: Access 2007`

Rationale:

If a new Access file is created in an earlier format, some users may be unable to open or use the file, or they may choose a format that is less secure than the Access format.

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new Access file, and therefore it is unlikely to affect usability for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `12`:

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\settings:default file format
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Access 2007`.

```
Microsoft Access 2016\Miscellaneous\Default file format
```

Default Value:

Disabled. (Users can change override the default to an older format.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.4.2 (L1) Ensure 'Do not prompt to convert older databases' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Access prompts users to convert older databases when they are opened.

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

Rationale:

By default, when users open databases that were created in the Access 97 file format, Access prompts them to convert the database to a newer file format. Users can choose to convert the database or leave it in the older format.

If this configuration is changed, Access will leave Access 97-format databases unchanged. Access informs the user that the database is in the older format but does not provide the user with an option to convert the database. Some features introduced in more recent versions of Access will not be available, and the user will not be able to make any design changes to the database.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\settings:noconvertdialog
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Access 2016\Miscellaneous\Do not prompt to convert older databases
```

Default Value:

Disabled. (Access will prompt for conversions to a newer file format.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.5 Tools | Security

This section contains settings to configure Tools and Security Options.

2.1.5.1 (L1) Ensure 'Modal Trust Decision Only' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Access notifies users about untrusted components.

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

Rationale:

By default, when users open an untrusted Access database that contains user-programmed executable components, Access opens the database with the components disabled and displays the Message Bar with a warning that database content has been disabled. Users can inspect the contents of the database but cannot use any disabled functionality until they enable it by clicking Options on the Message Bar and selecting the appropriate action.

The default configuration can be changed so that users see a dialog box when they open an untrusted database with executable components. Users must then choose whether to enable or disable the components before working with the database. In these circumstances users frequently enable the components, even if they do not require them. Executable components can be used to launch an attack against a computer environment.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\access\security:modaltrustdecisiononly
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Access 2016\Tools | Security\Modal Trust Decision Only
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.2 Microsoft Excel 2016

This section includes recommendations for Microsoft Excel.

2.2.1 Customizable Error Messages

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

2.2.2 Data Recovery

This section contains settings to configure Data Recovery options.

2.2.2.1 (L1) Ensure 'Do not show data extraction options when opening corrupt workbooks' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Excel presents users with a list of data extraction options before beginning an Open and Repair operation when users choose to open a corrupt workbook in repair or extract mode.

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

Rationale:

By default, when users choose to open a corrupt workbook with the Open and Repair command, Excel prompts them to choose between repairing or extracting data. A corrupt Excel file may be indicative of malicious tampering. By allowing the automatic handling of corrupt spreadsheets, malicious code may be introduced to the user's computer and the network.

Impact:

This setting will prevent Excel users from choosing how workbooks are recovered, which could increase desktop support requests.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options:extractdatadisableui
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Excel 2016\Data Recovery\Do Not Show Data Extraction Options When Opening Corrupt Workbooks
```

Default Value:

Disabled. (Excel prompts to user to either extract or repair.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.3 Disable Items in User Interface

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

2.2.4 Excel Options

This section contains settings for Excel Options.

2.2.4.1 Advanced

This section contains settings for Advanced settings.

2.2.4.1.1 General

2.2.4.1.1.1 (L1) Ensure 'Load Pictures from Web pages not created in Excel' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Excel loads graphics when opening Web pages that were not created in Excel.

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

Rationale:

By default, when users open Web pages in Excel, Excel loads any graphics that are included in the pages, regardless of whether they were originally created in Excel. Users can change this option in the Web Options dialog box, which is available from the Advanced section of the Excel Options dialog box.

Allowing Excel to load graphics created in other programs can make it vulnerable to possible future zero-day attacks that use graphic files as an attack vector. If such an event occurs, this setting can be used to mitigate the vulnerability.

Impact:

Excel will not load pictures from Web pages that were not created in Excel. This configuration can cause some disruptions for users who load Web pages in Excel that were created by other applications. Users who do not load Web pages in Excel will not be affected by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\internet:donotloadpictures
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Advanced\General\Load Pictures from Web Pages Not Created in Excel
```

Default Value:

Enabled. (Excel loads any graphics that are included in the pages regardless of origin.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.1.2 (L1) Ensure 'Ask to update automatic links' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Excel prompts users to update automatic links, or whether the updates occur in the background with no prompt.

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

Rationale:

When users open documents, Excel automatically updates any links to external content, such as graphics, Excel worksheets, and PowerPoint slides. If Excel is configured to automatically update links when documents are open, document content can change without the user's knowledge, which could put important information at risk.

Impact:

Users who work with Excel documents that contain external content will not be able to automatically update that content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options\binaryoptions:fupdateext_78_1
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Excel 2016\Excel Options\Advanced\Ask to Update Automatic Links
```

Default Value:

Enabled. (Excel will prompt users to update.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.2 Autocorrect Options

This section contains settings for Autocorrect Options.

2.2.4.2.1 (L1) Ensure 'Internet and network paths as hyperlinks' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether Excel automatically creates hyperlinks when users enter URL or UNC path information.

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

Rationale:

By default, when users type a string of characters that Excel recognizes as a Uniform Resource Locator (URL) or Uniform Naming Convention (UNC) path to a resource on the Internet or a local network, Excel will transform it into a hyperlink. Clicking the hyperlink opens it in the configured default Web browser or the appropriate application. This functionality can enable users to accidentally create links to dangerous or restricted resources, which could create a security risk.

Impact:

Excel users will still be able to create new hyperlinks manually, so it is unlikely to cause significant disruptions for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options:autohyperlink
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Excel 2016\Excel Options\Autocorrect Options\Internet and Network Paths as Hyperlinks
```

Default Value:

Enabled. (Excel will automatically transform matching strings to hyperlinks.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.3 Customize Ribbon

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

2.2.4.4 Formulas

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

2.2.4.5 General

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

2.2.4.6 Save

This section contains settings for Save options.

2.2.4.6.1 (L1) Ensure 'Default file format' is set to 'Enabled: Excel Workbook (.xlsx)' (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the default file format for saving workbooks in Excel.

The recommended state for this setting is: `Enabled: Excel Workbook (*.xlsx)`

Rationale:

If a new Excel file is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the default format.

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new Excel file, and therefore, it is unlikely to affect usability for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the recommended value of `51`:

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options:defaultformat
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Excel Workbook (*.xlsx)`:

```
Microsoft Excel 2016\Excel Options\Save\Default File Format
```

Default Value:

Disabled. (Excel saves new workbooks as *.xlsx but users can override this default.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.6.2 (L1) Ensure 'Disable AutoRepublish' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows administrators to disable the AutoRepublish feature in Excel. If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel saves a copy of the data to the Web page every time the user saves the workbook. By default, a message dialog displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog from appearing after every save. If the user selects "Do not show this message again", Excel will continue to automatically republish the data after every save without informing the user.

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

Rationale:

If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel saves a copy of the data to the Web page every time the user saves the workbook. If the page is on a Web server, anyone who has access to the page will be able to see the updated data after every save, which can lead to the undesired disclosure of sensitive or incorrect information.

By default, a message dialog box displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog box, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog box from appearing after every save. If the user selects "Do not show this message again," Excel will continue to automatically republish the data after every save without informing the user.

Impact:

If there is a critical business need to use the AutoRepublish feature, it might not be possible to enable this setting. However, in most situations users will be able to publish data to the Web manually.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options:disableautorepublish
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Excel 2016\Excel Options\Save\Disable AutoRepublish
```

Default Value:

Disabled. (Users can enable AutoRepublish to automatically republish workbooks.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.6.3 (L1) Ensure 'Do not show AutoRepublish warning alert' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Excel displays an alert before republishing a workbook to the World Wide Web.

AutoRepublish is a feature in Excel that allows workbooks to be automatically republished to the World Wide Web each time the workbook is saved. A number of changes might need to be made to allow the workbook to be successfully published, including the following:

- External references are converted to values.
- Hidden formulas become visible.
- The "Set precision as displayed" option, which appears beneath the "When calculating this workbook" heading in the Advanced section of the Excel Options dialog box, is no longer available.

These types of changes can mean that the version on the Web page might not be the same as the Excel file.

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

Rationale:

By default, a message dialog box appears every time the user saves a published workbook when AutoRepublish is enabled. From this dialog box, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog box from appearing after every save. If the user selects "Do not show this message again," Excel will continue to automatically republish the data after every save without informing the user.

Impact:

Configuring this setting to "Always show the alert before publishing" reinforces the default functionality in Excel and is therefore unlikely to cause usability issues for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options:disableautorepublishwarning
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Excel 2016\Excel Options\Save\Do Not Show AutoRepublish Warning Alert
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.2.4.7 Security

This section contains settings to configure Security Options.

2.2.4.7.1 Cryptography

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

2.2.4.7.2 Trust Center

This section contains settings for configuring Trust Center settings.

2.2.4.7.2.1 External Content

This section contains recommendations for External Content, such as Dynamic Data Exchange.

2.2.4.7.2.1.1 (L1) Ensure 'Always prevent untrusted Microsoft Query files from opening' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Query files (.iqy, oqy, .dqy, and .rqy) in an untrusted location are prevented from opening.

Using Microsoft Query, users can connect to external data sources, select data from those external sources, import that data into worksheets, and refresh it to keep worksheet data synchronized with the data in the external sources.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise.

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

Rationale:

Microsoft Query files that have been tampered with and placed in an untrusted location could allow an attacker to affect the confidentiality and integrity of a spreadsheet.

Impact:

Microsoft Query files in an untrusted location are prevented from opening. Users will not be able to change this setting under File > Options > Trust Center > Trust Center Settings > External Content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\external content:enableblockunsecurequeryfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\External Content\Always prevent untrusted Microsoft Query files from opening
```

Default Value:

Disabled. (Query files in an untrusted location are not prevented from opening.)

References:

1. https://support.microsoft.com/en-us/office/use-microsoft-query-to-retrieve-external-data-42a2ea18-44d9-40b3-9c38-4c62f252da2e

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.1.2 (L1) Ensure 'Don’t allow Dynamic Data Exchange (DDE) server launch in Excel' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows controls whether Dynamic Data Exchange (DDE) server launch is allowed.

The DDE protocol is a set of messages and guidelines. It sends messages between applications that share data and uses shared memory to exchange data between applications. Applications can use the DDE protocol for one-time data transfers and for continuous exchanges in which applications send updates to one another as new data becomes available.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise.

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

Rationale:

In an email attack scenario, an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file, typically by way of an enticement in an email. The attacker would have to convince the user to disable Protected Mode and click through one or more additional prompts. Email attachments are a primary method an attacker could use to spread malware.

For more information see Microsoft Security Advisory 4053440 link in the references of this recommendation.

Impact:

None - DDE Launch is disabled by default. Enforcing this policy ensures users cannot enter an unsecure state.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\external
content:disableddeserverlaunch
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\External
Content\Don't allow Dynamic Data Exchange (DDE) server launch in Excel
```

Default Value:

Enabled. (DDE launch is turned off but users can turn it on.)

References:

1. https://learn.microsoft.com/en-us/office/troubleshoot/excel/security-settings
2. https://learn.microsoft.com/en-us/windows/win32/dataxchg/about-dynamic-data-exchange
3. https://learn.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.1.3 (L1) Ensure 'Don’t allow Dynamic Data Exchange (DDE) server lookup in Excel' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows controls whether Dynamic Data Exchange (DDE) server lookup is allowed.

The DDE protocol is a set of messages and guidelines. It sends messages between applications that share data and uses shared memory to exchange data between applications. Applications can use the DDE protocol for one-time data transfers and for continuous exchanges in which applications send updates to one another as new data becomes available.

Dynamic Data Exchange Server Lookup allows Excel to find and use visible DDE servers on the network.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise.

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

Rationale:

In an email attack scenario, an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file, typically by way of an enticement in an email. The attacker would have to convince the user to disable Protected Mode and click through one or more additional prompts. Email attachments are a primary method an attacker could use to spread malware.

For more information please see Microsoft Security Advisory 4053440.

Impact:

When enabled DDE server lookup isn’t allowed, and users can’t turn on DDE server lookup in the Trust Center. A Systems Administrator would need to implement DDE under a zero trust framework.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\external
content:disableddeserverlookup
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\External
Content\Don't allow Dynamic Data Exchange (DDE) server lookup in Excel
```

Default Value:

Disabled. (DDE lookup is on)

References:

1. https://learn.microsoft.com/en-us/office/troubleshoot/excel/security-settings
2. https://learn.microsoft.com/en-us/windows/win32/dataxchg/about-dynamic-data-exchange
3. https://learn.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2 File Block Settings

This section contains File Block Settings.

In this section several policies reference a `Use Open Policy`. The actions defined by this policy are configured in the `Set default file block behavior` settings catalog setting which is included in this section of the benchmark.

2.2.4.7.2.2.1 (L1) Ensure 'dBase III /IV files' is set to 'Enable: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with dBase III /IV files format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

NOTE: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view dBase III /IV files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:dbasefiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\dBase III /IV Files
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.2 (L1) Ensure 'Dif and Sylk files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Dif and Sylk file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

DIF and SYLK are text-only file formats that are used to exchange data between different applications, such as Excel. If a vulnerability is discovered that affects these kinds of files, use this setting to protect the organization against attacks by temporarily preventing users from opening files in these formats until a security patch is available.

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Dif and Sylk files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:difandsylkfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Dif and Sylk Files
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.3 (L1) Ensure 'Excel 2 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 2 macrosheets file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 2 macrosheets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl2macros
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Excel 2 Macrosheets and Add-in Files
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.4 (L1) Ensure 'Excel 2 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 2 worksheets file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 2 worksheets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl2worksheets
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 2 Worksheets
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.5 (L1) Ensure 'Excel 3 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 3 macrosheets file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`

Rationale:

Using legacy file formats could allow malicious code to become active on user computers or the network.

Impact:

Users will not be able to open, save, or view Excel 3 macrosheets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl3macros
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Excel 3 Macrosheets and Add-in Files
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.6 (L1) Ensure 'Excel 3 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 3 worksheets file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 3 worksheets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl3worksheets
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 3 Worksheets
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.7 (L1) Ensure 'Excel 4 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 4 macrosheets and add-in file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 4 macrosheets and add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl4macros
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Excel 4 macrosheets and add-in Files
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.8 (L1) Ensure 'Excel 4 workbooks' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel 4 workbooks file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 4 workbooks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl4workbooks
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 4 Workbooks
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.9 (L1) Ensure 'Excel 4 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 4 worksheets file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 4 worksheets.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl4worksheets
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 4 Worksheets
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.10 (L1) Ensure 'Excel 95 workbooks' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel 95 workbooks.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Excel 95 workbooks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the recommended value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl95workbooks
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Excel 95 Workbooks
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.11 (L1) Ensure 'Excel 95-97 workbooks and templates' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 95-97 workbooks and templates file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on user computers or the network.

Impact:

Users will not be able to open, save, or view Excel 95-97 workbooks and templates.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl9597workbooksandtemplates
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Excel 95-97 Workbooks and Templates
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.12 (L1) Ensure 'Excel 97-2003 workbooks and templates' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Excel files with Excel 97-2003 workbooks and templates file format.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on user computers or the network.

Impact:

Users will not be able to open, save, or view Excel 97-2003 workbooks and templates.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:xl97workbooksandtemplates
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Excel 97-2003 workbooks and templates
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.13 (L1) Ensure 'Set default file block behavior' is set to 'Enabled: Blocked files are not opened' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if users can open, view, or edit Word files that are by default blocked by Microsoft Office.

The recommended state for this setting is: `Enabled: Blocked files are not opened`.

Rationale:

By default, users can open, view, or edit many file types in Word. Some file types are safer than others, as some could allow malicious code to be executed on a user computer or the network.

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in Word. Productivity could be affected if users who require access to any of these file types cannot access them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Blocked files are not opened`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\Set Default File Block Behavior
```

Default Value:

Disabled. (The behavior is the same as the *Blocked files are not opened* setting. Users will not be able to open blocked files.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.2.14 (L1) Ensure 'Web pages and Excel 2003 XML spreadsheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Web pages and Excel 2003 XML spreadsheets.

`Open/Save blocked, use open policy`: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on a user's computer or the network.

Impact:

Users will not be able to open, save, or view Web pages and Excel 2003 XML spreadsheets. In addition, the following file types will open in Protected View: `.mht .mhtml .htm .html .xml .xlmss`

While in OneNote using the function "Convert a Table to Excel" may cause OneNote to freeze until a dialogue box is confirmed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:htmland xmlssfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block
Settings\Web Pages and Excel 2003 XML Spreadsheets
```

Default Value:

Disabled. (The file type will not be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3 Protected View

This section contains Protected View Settings.

2.2.4.7.2.3.1 (L1) Ensure 'Always open untrusted database files in Protected View' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether database files (.dbf) opened from an untrusted location are always opened in Protected View.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise.

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

Rationale:

Files that originate from an untrusted location may contain malicious software. Requiring a user to open files originating from these zones forces them into a read-only mode. This reduces the chance of infection by making the user acknowledge a series of prompts before enabling editing.

Impact:

Database files opened from an untrusted location are always opened in Protected View. Users will not be able to change this setting under Trust Center Settings > Protected View.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\protectedview:enabledatabasefileprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Always open untrusted database files in Protected View
```

Default Value:

Disabled. (Database files opened from untrusted locations are not opened in Protected View.)

References:

1. https://support.microsoft.com/en-us/topic/what-is-protected-view-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3.2 (L1) Ensure 'Do not open files from the internet zone in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether files downloaded from the Internet zone open in Protected View.

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

Rationale:

Allowing users to download files from the Internet zone to open outside of Protected View could allow malicious code to become active on a user's computer or the network.

Impact:

When files open in Protected View, some functionality will be unavailable; users will be unable to edit the file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\protectedview:disableinternetfilesinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Do not open files from the internet zone in Protected View
```

Default Value:

Disabled. (Files downloaded from the internet zone open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3.3 (L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if files located in unsafe locations will open in Protected View.

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

Rationale:

Opening files located in unsafe locations that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Note: If a specified unsafe location(s) is not configured, the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

Impact:

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to safe locations in order to access them with full functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\protectedview:dis
ableunsafelocationsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Do
Not Open Files in Unsafe Locations in Protected View
```

Default Value:

Disabled. (Files located in unsafe locations open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3.4 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Enabled: Open in Protected View`.

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\filevalidation:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open in Protected View`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Set document behavior if file validation fails
```

Default Value:

Enabled. (Open in Protected View (Unchecked).)

Additional Information:

If this policy setting is disabled, Office follows the "Open files in Protected View and disallow edit" behavior.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3.5 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Unchecked: Do not allow edit (False)`.

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\filevalidation:disableeditfrompv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path `Unchecked: Do not allow edit (False)`. The value should be set to `False`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Set document behavior if file validation fails
```

Default Value:

Enabled. (Open in Protected View (Unchecked).)

Additional Information:

If this policy setting is disabled, Office follows the "Open files in Protected View and disallow edit" behavior.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.3.6 (L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if Excel files in Outlook attachments open in Protected View.

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

Rationale:

Opening files that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Impact:

Some functionality is not available when files are opened in Protected View; users will be unable to edit the file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\protectedview:disableattachmentsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View\Turn off Protected View for attachments opened from Outlook
```

Default Value:

Disabled. (Outlook attachments open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.4 Trusted Locations

This section contains Trusted Locations settings.

2.2.4.7.2.4.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether trusted locations on the network can be used. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe by the application opening the file.

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

Rationale:

Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. These custom locations added by users are ignored but not removed. Trusted locations added in policy that specify a network location are also ignored.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\trusted
locations:allownetworklocations
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Trusted
Locations\Allow Trusted Locations on the network
```

Default Value:

Disabled. (Trusted locations are not allowed, however users can check the box to allow trusted locations, and then add custom locations.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.4.2 (L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications.

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

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

All trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2016 during setup, deployed to users using policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\trusted
locations:alllocationsdisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Trusted
Locations\Disable all trusted locations
```

Default Value:

Disabled. (All trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.2.5 (L1) Ensure 'Block Excel XLL Add-ins that come from an untrusted source' is set to 'Enabled: Blocked' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

An Excel add-in is a collection of custom code and functionality that enhances Microsoft Excel's capabilities. These add-ins can be created by third-party developers or by Excel users themselves. Once installed, they become part of Excel and can be used across different workbooks.

.XLL Add-ins are native code add-ins written in C or C++ programming languages. They offer high performance and direct access to Excel's internal functions, making them suitable for complex and computationally intensive tasks.

The recommended state for this setting is: `Enabled: Blocked`.

Rationale:

Untrusted XLL files, as dynamic-link libraries (DLLs), pose a security risk in phishing campaigns, where attackers can trick users into executing seemingly harmless files containing malicious payloads. Being executables, XLL files can unwittingly run on users' systems, leading to unauthorized code execution, malware installation, and potential data breaches.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:blockxllfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Block Excel XLL Add-ins that come from an untrusted source
```

Default Value:

Disabled. (Untrusted XLL add-ins are blocked but users can override via the registry.)

References:

1. https://support.microsoft.com/en-us/topic/excel-is-blocking-untrusted-xll-add-ins-by-default-1e3752e2-1177-4444-a807-7b700266a6fb
2. https://isc.sans.edu/diary/Downloader+Disguised+as+Excel+AddIn+XLL/28052

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v7	2.8 Implement Application Whitelisting of Libraries The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			●

2.2.4.7.2.6 (L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the blocking of macros from running in Office files that come from the internet.

By enabling this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Users will receive a notification that macros are blocked from running.

The exceptions when macros will be allowed to run are:

- The Office file is saved to a Trusted Location.
- The Office file was previously trusted by the user.
- Macros are digitally signed and the matching Trusted Publisher certificate is installed on the device.

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

Rationale:

Windows will mark files downloaded from the internet within an alternative NTFS data stream on the file. Files from untrusted sources can contain malicious payloads embedded in the Macros, including fileless malware, and should be handled with extra care by utilizing additional security controls.

Impact:

This enforces the default behavior and should not cause additional impact.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:blockcontentexecu
tionfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Block macros from
running in Office files from the internet
```

Default Value:

Enabled. (Macros are blocked)

References:

1. https://learn.microsoft.com/en-us/DeployOffice/security/internet-macros-blocked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.7 (L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros or Excel 4.0 (XLM) macros are present. Multiple Office apps support VBA macros, but XLM macros are only supported by Excel.

`Disable all except digitally signed macros`: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.

The recommended state for this setting is: `Enabled: Disable all except digitally signed macros`.

Rationale:

When users open files in Excel that contain VBA macros, Excel opens the files with the macros disabled, and displays the Trust Bar with a warning that macros are present and have been disabled. Users may then enable these macros by clicking Options on the Trust Bar and selecting the option to enable them.

This can allow dangerous macros to become active on users computer or the network.

Impact:

This configuration causes documents and templates that contain unsigned macros to lose any functionality supplied by those macros. To prevent this loss of functionality, users can install the macros in a trusted location, unless the Disable all trusted locations setting is configured to Enabled, which will block them from doing so. If your organization does not use any officially sanctioned macros, consider choosing No Warnings for all macros but disable all macros for even stronger security.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:vbawarnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable all except digitally signed macros.`

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\VBA Macro
Notification Settings
```

Default Value:

Disable VBA macros with notification. Enable Excel 4.0 macros when VBA macros are enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.8 (L1) Ensure 'Prevent Excel from running XLM macros' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting will prevent Excel from running Excel 4.0 (XLM) macros. XLM macros were first added to Excel in 1992 and were disabled in Excel (Build 16.0.14427.10000) by Microsoft in 2021.

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

Rationale:

XLM is data macro format from the early nineties that was not built with security in mind. Macros can be easily exploited and are a favorite hiding place of malicious code. While newer builds of Excel disable XLM macros by default, it is an important setting to audit for a secure state in all versions of Excel.

Impact:

This enforces the default behavior. Existing XLM macros will not function and should be migrated.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:xl4macrooff
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Prevent Excel from running XLM macros
```

Default Value:

Enabled. (XLM Macros are blocked)

References:

1. https://learn.microsoft.com/en-us/DeployOffice/security/internet-macros-blocked
2. https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.9 (L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether add-ins for the specified Office applications must be digitally signed by a trusted publisher.

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

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Not configuring this setting may allow an application to load a dangerous add-in and as a result, malicious code could become active on a user's computer or the network.

Impact:

This setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users either must obtain signed versions of such add-ins or stop using them.

Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store but does not write information to this store.

If a list of trusted publishers in a previous version of Office was created and the Office release was upgraded, the trusted publisher list will still be recognized.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:requireaddinsig
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Require that
application add-ins are signed by Trusted Publisher
```

Default Value:

Disabled. (Excel does not check for digital signatures in add-ins.)

References:

1. https://learn.microsoft.com/en-us/deployoffice/security/trusted-publisher
2. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-publishers-certificate-store

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.10 (L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification.

Note: For this policy to apply the *Require that application add-ins are signed by Trusted Publisher* policy setting needs to be enabled. This will prevent users from changing the *Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them* policy setting.

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

Rationale:

Allowing unsigned application add-ins could cause the application to load dangerous add-ins and as a result, malicious code could become active on user computers and the network.

Impact:

If an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled, and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:notbpromptunsigneddaddin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Require that application add-ins are signed by Trusted Publisher (User)\Disable Trust Bar Notification for unsigned application add-ins and block them
```

Note: This setting is nested under `Require that application add-ins are signed by Trusted Publisher (User)` which needs to be enable first before disabling trust bar notifications for unsigned application add-ins.

Default Value:

Disabled. (Users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.11 (L1) Ensure 'Store macro in Personal Macro Workbook by default' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the default location for storing macros in Excel. The Record Macro dialog box includes a drop-down menu that allows users to choose whether to store the new macro in the current workbook, a new workbook, or their personal macro workbook (Personal.xlsb), a hidden workbook that opens every time Excel starts.

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

Rationale:

Excel displays the Record Macro dialog box with This Workbook already selected in the drop-down menu. If a user saves a macro in the active workbook and then distributes the workbook to others, the macro is distributed along with the workbook, which could put workbook data at risk if the macro is triggered accidentally or intentionally.

Impact:

Enabling this setting does not prevent users from selecting a different location for storing macros, so it is unlikely to cause significant usability issues for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\options\binaryoptions:fglobalsheet_37_1
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Store Macro In Personal Macro Workbook by Default
```

Default Value:

Disabled. (Macros are stored in the originating workbook.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.2.4.7.2.12 (L1) Ensure 'Trust access to Visual Basic Project' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

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

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

Impact:

None - this is the default behavior.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:accessvbom
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Trust Center\Trust Access To
Visual Basic Project
```

Default Value:

Disabled. (Client access to VBA projections is not allowed but users can override.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.3 (L1) Ensure 'Force file extension to match file type' is set to 'Enabled: Always match file type' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Excel loads file types that do not match their extension. Excel can load files with extensions that do not match the files' type. For example, if a comma-separated values (CSV) file named example.csv is renamed example.xls (or any other file extension supported by Excel 2003 and earlier only), Excel can properly load it as a CSV file.

Policy options for working with files that have non-matching extensions:

`Always match file type` - Excel does not open any files that have non-matching extensions.

The recommended state for this setting is: `Enabled: Always match file type`

Rationale:

Some attacks target specific file formats. If Excel is allowed to load files with extensions that do not match their file types, a malicious person can deceive users into loading dangerous files that have incorrect extensions.

By default, if users attempt to open files with the wrong extension, Excel opens the file and displays a warning that the file type is not what Excel expected.

Impact:

Earlier versions of Excel did not enforce file type matching. Enabling this setting and selecting `Always match file type` might cause disruptions for users who rely on the functionality of earlier versions of Excel and could interfere with the operation of tools and scripts that rely on it.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:extensionhardenin
g
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Always match file type`.

```
Microsoft Excel 2016\Excel Options\Security\Force File Extension to Match File Type
```

Default Value:

Disabled. (Excel will display a warning for unexpected formats but users can still proceed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.2.4.7.4 (L1) Ensure 'Scan encrypted macros in Excel Open XML workbooks' is set to 'Enabled: Scan encrypted macros (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether encrypted macros in Open XML documents are required to be scanned with anti-virus software before being opened.

The recommended state for this setting is: `Enabled: Scan encrypted macros (default).`

Rationale:

When an Office Open XML document is rights-managed or password protected, macros that are embedded in the document are encrypted along with the rest of the workbook's contents. Macros can contain malicious code which could cause a virus to load undetected and lead to data loss or reduced application functionality.

Impact:

None - this is the default behavior.

By default, encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:excelbypassencryptedmacroscan
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Scan encrypted macros (default).`

```
Microsoft Excel 2016\Excel Options\Security\Scan Encrypted Macros in Excel Open XML Workbooks
```

Default Value:

Scan encrypted macros. (Disabled and Not Configured are functionally equivalent.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

2.2.4.7.5 (L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the turn off the file validation feature. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

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

Rationale:

The file validation feature ensures that Office Binary Documents are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\filevalidation:enableonload
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Excel 2016\Excel Options\Security\Turn Off File Validation
```

Default Value:

Disabled. (File validation is turned on.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

2.2.4.7.6 (L1) Ensure 'WEBSERVICE Function Notification Settings' is set to 'Enabled: Disable all without notification' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Excel will warn users when WEBSERVICE functions are present.

When selecting the option "Disable all with notification" the application displays the Trust Bar for all WEBSERVICE functions. This option enforces the default configuration in Office.

The recommended state for this setting is: `Enabled: Disable all without notification`.

Rationale:

WEBSERVICE functions can be used alongside formula injection to cause users of an Excel spreadsheet to unknowingly connect to systems controlled by bad actors, or even exfiltrate data.

Impact:

Users will not be notified when a WEBSERVICE function is disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security:webservicefunctionwarnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable all without notification`.

```
Microsoft Excel 2016\Excel Options\Security\WEBSERVICE Function Notification Settings
```

Default Value:

Disabled. (WEBSERVICE functions are disabled, but can be enabled via the Trust Bar by an end user.)

References:

1. https://support.microsoft.com/en-us/office/webservice-function-0546a35a-ecc6-4739-aed7-c0b7ce1562c4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3 Microsoft Office 2016

This section contains general settings for Microsoft Office.

2.3.1 AutoSave

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.2 Business Data

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.3 Collaboration Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.4 Contact Card

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.5 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.6 Customize

This section contains settings to configure Customize settings within Office.

2.3.6.1 Shared Workspace

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.6.2 (L1) Ensure 'Disable UI extending from documents and templates' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office applications load any custom user interface (UI) code included with a document or template. Office allows developers to extend the UI with customization code that is included in a document or template.

The recommended state for this setting is: `Enabled: Disallow in Word, Excel, PowerPoint, Access, Outlook, Publisher, Project, Visio, InfoPath.`

Rationale:

The Office release allows developers to extend the UI with customization code that is included in a document or template. If the customization code is written by an inexperienced or malicious developer, it could limit the accessibility or availability of important application commands. Commands could also be added that launch macros that contain malicious code.

By default, Office applications load any UI customization code included with a document or template when opening it.

Impact:

Enabling this setting will prevent developers from using documents and templates to extend the UI, which some organizations do to increase user productivity. If the organization makes use of a modified UI, it might not be feasible to enable this setting. Sometimes only specific teams in an organization require a modified UI, and this setting could be enabled for the rest of the organization.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location. Each application will have a subkey based on the application name with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\toolbars\[Office
Application Name]:noextensibilitycustomizationfromdocument
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disallow in Word, Excel, PowerPoint, Access, Outlook, Publisher, Project, Visio, InfoPath`:

```
Microsoft Office 2016\Customize\Disable UI extending from documents and templates
```

Default Value:

Disabled. (Office applications will load any UI customization code.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.7 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.8 DLP

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.9 Document Information Panel

This section contains settings to configure Document Information Panel.

2.3.9.1 (L1) Ensure 'Document Information Panel Beaconing UI' is set to 'Enabled: Always show UI' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users see a security warning when they open custom Document Information Panels that contain a Web beaconing threat. InfoPath can be used to create custom Document Information Panels that can be attached to Excel workbooks, PowerPoint presentations, and Word documents.

The recommended state for this setting is: `Enabled: Always show UI`.

Rationale:

InfoPath can be used to create custom Document Information Panels that can be attached to Excel workbooks, PowerPoint presentations, and Word documents.

A malicious user could insert a Web beacon into an InfoPath form that is used to create a custom Document Information Panel. Web beacons can be used to contact an external server when users open the form. Information could be gathered by the form, or information entered by users could be sent to an external server and cause them to be vulnerable to additional attacks.

Impact:

Enabling this setting and selecting "Always show UI" from the drop-down menu can cause some disruptions for users who often open documents containing custom Document Information Panels.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\documentinformationpanel:
msoridcuxdocspropertypanelbeaconing
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Always show UI`:

```
Microsoft Office 2016\Document Information Panel\Document Information Panel Beaconing UI
```

Default Value:

Disabled. (Equivalent of Never show UI being set.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.10 Downloading Framework Components

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.11 File Open/Save Dialog Box

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.12 First Run

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.13 Graph Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.14 Help

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.15 IME (Japanese)

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.16 Improved Error Reporting

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.17 Language Preferences

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.18 Links

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.19 Manage Restricted Permissions

This section contains setting to configure Manage Restricted Permissions.

2.3.19.1 (L1) Ensure 'Allow users with earlier versions of Office to read with browsers...' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting will allow users with earlier versions of Office to read documents with browsers supporting Information Rights Management.

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

Rationale:

The Windows Rights Management Add-on for Internet Explorer provides a way for users who do not use the Office release to view, but not alter, files with restricted permissions. By default, IRM-enabled files are saved in a format that cannot be viewed by using the Windows Rights Management Add-on. If this setting is enabled, an embedded rights-managed HTML version of the content is saved with each IRM-enabled file, which can be viewed in Internet Explorer using the add-on. This configuration increases the size of rights-managed files, in some cases significantly.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm:includehtml
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Manage Restricted Permissions\Allow users with earlier versions of Office to read with browsers....
```

Default Value:

Disabled. (Enforce defaults.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.19.2 (L1) Ensure 'Always expand groups in Office when restricting permission for documents' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether group names automatically expand to display all the members of the group when selected in the Permissions dialog box.

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

Rationale:

By default, when users select a group name while applying Information Rights Management (IRM) permissions to Excel workbooks, InfoPath templates, Outlook e-mail messages, PowerPoint presentations, or Word documents in the Permissions dialog box, the members of the group are not displayed. This functionality can make it possible for users to unknowingly give read or change permissions to inappropriate people.

Impact:

Enabling this setting changes the way the Permissions dialog box displays names but should not create significant usability issues for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm\autoexpanddls:autoexpanddlsenable
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Manage Restricted Permissions\Always expand groups in office when restricting permission for documents
```

Default Value:

Disabled. (Members of group are not displayed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.19.3 (L1) Ensure 'Always require users to connect to verify permission' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users are required to connect to the Internet or a local network to have their licenses confirmed every time they attempt to open Excel workbooks, InfoPath forms or templates, Outlook e-mail messages, PowerPoint presentations, or Word documents that are protected by Information Rights Management (IRM). This policy is useful for logging the usage of files with restricted permissions on the server.

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

Rationale:

By default, users are not required to connect to the network to verify permissions. If users do not need their licenses confirmed when attempting to open Office documents, they might be able to access documents after their licenses have been revoked. Also, it is not possible to log the usage of files with restricted permissions if users' licenses are not confirmed.

Impact:

Enabling this setting could create problems for users who need to open rights-managed files when they are not connected to the Internet, such as mobile users. Consider surveying the organization to determine users' need for offline use of rights-managed files before enabling this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm:requireconnection
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Manage Restricted Permissions\Always require users to connect to verify permission
```

Default Value:

Disabled. (Users are not required to connect.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.19.4 (L1) Ensure 'Never allow users to specify groups when restricting permission for documents' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office users can assign permissions to distribution lists when using Information Rights Management.

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

Rationale:

By default, Office users can specify distribution lists when using Information Rights Management (IRM) to restrict access to Excel workbooks, InfoPath templates, Outlook e-mail messages, PowerPoint presentations, or Word documents. If users are not fully aware of the distribution list's membership before assigning it permission to open or modify a document, sensitive information could be at risk.

Impact:

Enabling this setting could cause some disruptions for Office users who are accustomed to specifying distribution groups when defining permissions for a document. These users will have to list users individually in the Permission dialog box to assign them permission to read or modify the document. Users who do not use Information Rights Management will not be affected by this setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm:neverallowdls
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Manage Restricted Permissions\Never Allow Users to Specify Groups When Restricting Permission for Documents
```

Default Value:

Disabled. (Users can specify dist. lists when using IRM.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

2.3.19.5 (L1) Ensure 'Prevent users from changing permissions on rights managed content' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office users can change permissions for content that is protected with Information Rights Management (IRM).

The Information Rights Management feature of Office allows individuals and administrators to specify access permissions to Word documents, Excel workbooks, PowerPoint presentations, InfoPath templates and forms, and Outlook e-mail messages. This functionality helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

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

Rationale:

The Information Rights Management feature of the Office release allows individuals and administrators to specify access permissions to Word documents, Excel workbooks, PowerPoint presentations, InfoPath templates and forms, and Outlook e-mail messages. This functionality helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

This setting can be used to prevent Office users from changing the IRM permissions of a document. If this setting is Enabled, users can open and edit documents for which they have the appropriate permissions, but they cannot create new rights-managed content, add IRM to existing documents, change existing IRM permissions, or remove IRM from documents. This configuration can prevent users from making effective use of IRM to protect documents.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm:disablecreation
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Manage Restricted Permissions\Prevent Users From Changing Permissions on Rights Managed Content
```

Default Value:

Disabled. (Users can manage IRM permissions)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

2.3.20 Microsoft Office Document Cache

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.21 Microsoft Office SmartArt

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.22 Microsoft Save as PDF and XPS add-ins

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.23 Miscellaneous

This section contains settings to configure Miscellaneous settings.

2.3.23.1 Workflow Cache

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.23.2 (L1) Ensure 'Block signing into Office' is set to 'Enabled: Org ID only' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can provide credentials to Office using either their Microsoft Account or the user ID assigned by the organization for accessing Office 365.

By selecting the `Org ID only` option, users can sign in only by using the user ID assigned by the organization for accessing Office 365.

The recommended state for this setting is: `Enabled: Org ID only`

Rationale:

If end users are allowed to connect personal Microsoft Accounts to an organization's Office applications, then confidential data could be exfiltrated to the users' personal cloud storage. Likewise, the users' personal data could more easily end up on work-related systems. By restricting Office 365 sign in to Organization ID only, users will also be forced to sign into a tenant that has managed policies and restrictions assigned to them.

Impact:

Users will be unable to connect to cloud services not maintained by the organization (such as SharePoint services in Office 365) and access the files and services provided by the cloud services.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\signin:signinoptions
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Org ID only`:

```
Microsoft Office 2016\Miscellaneous\Block Signing into Office
```

Default Value:

Enabled: Both IDs allowed

Additional Information:

This setting can be further enhanced by utilizing the CIS Microsoft 365 Benchmark to restrict sign in to specific domains, such as the organization's domain.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.23.3 (L1) Ensure 'Control Blogging' is set to 'Enabled: All Blogging Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can compose and post blog entries from Word.

The recommended state for this setting is: `Enabled: All Blogging Disabled`.

Rationale:

The blogging feature in Word enables users to compose blog entries and post them to their blogs directly from Word, without using any additional software.

By default, users can post blog entries to any compatible blogging service provider, including Windows Live Spaces, Blogger, a SharePoint or Community Server site, and others. If the organization has policies that govern the posting of blog entries, allowing users to access the blogging feature in Word might enable them to violate those policies.

Impact:

Disabling the blogging feature in Word may cause disruptions for users who use Word to compose and post blog entries. Any users who have a legitimate need to post blog entries will have to use another tool.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\common\blog:disableblog
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: All Blogging Disabled`:

```
Microsoft Office 2016\Miscellaneous\Control Blogging
```

Default Value:

Enabled-Enabled. (Users can publish blog entries to any provider.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.24 Office 2016 Converters

This section contains settings to configure Office Converters.

2.3.24.1 (L1) Ensure 'Block opening of pre-release versions of file formats new to Excel 2016 through the Compatibility Pack for Office 2016 and Excel 2016 Converter' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users with the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2016 File Formats installed can open Office Open XML files saved with pre-release versions of Excel 2016. Excel Open XML files usually have the following extensions: .xlsx, .xlsm, .xltx, .xltm, .xlam.

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

Rationale:

The Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats enables users of Microsoft Excel 2000, Microsoft Excel 2002, and Microsoft Office Excel 2003 to open files saved in the Office Open XML format used by Excel. Excel Open XML files usually have the following extensions:

- .xlsx
- .xlsm
- .xltx
- .xltm
- .xlam

By default, the Compatibility Pack does not open files that were saved in pre-release versions of the new Office Open XML format, which underwent some minor changes prior to the final release of Excel. If this configuration is changed through a registry modification or by some other mechanism, users with the Compatibility Pack installed can open files saved by some pre-release versions of Excel, but not by others, which can lead to inconsistent file opening functionality.

Impact:

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

NOTE: See Plan block file format settings in the Office Resource Kit for more information about using policy to manage and enforce file format requirements. Also, see the "File Block Technology" section in Chapter 4 of the Microsoft Office Security Guide for information about the Microsoft Office Isolated Conversion Environment (MOICE), which provides another method.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\fileblock:excel12
betafilesfromconverters
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Office 2016 Converters\Block opening of pre-release
versions of file formats new to Excel 2016 through the Compatibility Pack for
Office 2016 and Excel 2016 Converter
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.24.2 (L1) Ensure 'Block opening of pre-release versions of file formats new to PowerPoint 2016 through the Compatibility Pack for Office 2016 and PowerPoint 2016 Converter' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users with the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2016 File Formats installed can open Office Open XML files saved with pre-release versions of PowerPoint 2016. PowerPoint Open XML files usually have the following extensions: .pptx, .pptm, .potx, .potm, .ppsx, .ppsm, .ppam, .thmx, .xml.

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

Rationale:

The Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats enables users of Microsoft PowerPoint 2000, PowerPoint 2002, and Office PowerPoint 2003 to open files saved in the Office Open XML format used by PowerPoint. PowerPoint Open XML files usually have the following extensions:

- .pptx
- .pptm
- .potx
- .potm
- .ppsx
- .ppsm
- .ppam
- .thmx
- .xml

By default, the Compatibility Pack does not open files that were saved in pre-release versions of the new Office Open XML format, which underwent some minor changes prior to the final release of PowerPoint. If this configuration is changed through a registry modification or by some other mechanism, users with the Compatibility Pack installed can open files saved by some pre-release versions of PowerPoint, but not by others, which can lead to inconsistent file opening functionality.

Impact:

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

NOTE: See Plan block file format settings in the Office Resource Kit for more information about using policy to manage and enforce file format requirements. Also, see the "File Block Technology" section in Chapter 4 of the Microsoft Office Security Guide for information about the Microsoft Office Isolated Conversion Environment (MOICE), which provides another method.

NOTE#2: When enabling this policy the following setting is also set to `Enabled`:

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\File Block
Settings\PowerPoint beta converters
```

Both `PowerPoint beta converters` and the setting in this recommendation share the same registry key and value, so there is no adverse impact from this.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\fileblock:po
werpoint12betafilesfromconverters
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Office 2016 Converters\Block opening of pre-release
versions of file formats new to PowerPoint 2016 through the Compatibility
Pack for Office 2016 and PowerPoint 2016 Converter
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.25 Present Online

This section contains recommendations for the Present Online service.

2.3.25.1 Presentation Services

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.25.2 (L2) Ensure 'Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls removal of Office Presentation Service from the list of online presentation services in PowerPoint and Word. This list appears when a user selects Present Online from the Share tab in Backstage view and in the ribbon in PowerPoint.

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

Rationale:

Allowing users to utilize Office Presentation Service for PowerPoint and Word could allow for sensitive information to be sent to unauthorized parties in an unintended manner. Any information in a Word Document, or PowerPoint document could simply be sent through this service to network connected viewers. Intended or Unintended data leakage can be prevented by turning off unused services.

Impact:

Users that utilize Office Presentation Service for PowerPoint and Word will need to share their presentation another way.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\broadcast:disabledefaultservice
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Present Online\Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word
```

Default Value:

Not Configured (users can select Office Presentation Service to present their PowerPoint or Word file to other users online).

References:

1. https://support.microsoft.com/en-us/office/broadcast-your-powerpoint-presentation-online-to-a-remote-audience-25330108-518e-44be-a281-e3d85f784fee#OfficeVersion=Newer_versions

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.3.26 Readiness Toolkit

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.27 Security Settings

This section contains settings to configure Security Settings.

2.3.27.1 Digital Signatures

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.27.2 Escrow Certificates

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.27.3 Trust Center

This section contains settings to configure Trust Center.

2.3.27.3.1 Application Guard

This section is intentionally blank and exists to ensure the structure of Office benchmark is consistent.

2.3.27.3.2 Protected View

This section is intentionally blank and exists to ensure the structure of Office benchmark is consistent.

2.3.27.3.3 Trusted Catalogs

This section is intentionally blank and exists to ensure the structure of Office benchmark is consistent.

2.3.27.3.4 (L1) Ensure 'Allow mix of policy and user locations' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether trusted locations can be defined by users, the Office Customization Tool (OCT), and Intune profiles, or if they must be defined by Intune profiles alone.

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

Rationale:

When files are opened from trusted locations, all the content in the files is enabled and active. Users are not notified about any potential risks that might be contained in the files, such as unsigned macros, ActiveX controls, or links to content on the Internet.

By default, users can specify any location as a trusted location, and a computer can have a combination of user-created, OCT-created, and Group Policy-created trusted locations.

Impact:

Disabling this setting will cause some disruption for users who have defined their own trusted locations in the Trust Center. Applications will treat such locations like any other untrusted locations, which means that users will see Message Bar warnings about active content such as ActiveX controls and VBA macros when they open files, and they will have to choose whether to enable controls and macros or leave them disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security\trusted
locations:allow user locations
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Trust Center\Allow Mix of Policy and User Locations
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.4 (L1) Ensure 'ActiveX Control Initialization' is set to 'Enabled: 6' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies the Microsoft ActiveX® initialization security level for all Microsoft Office applications.

The recommended state for this setting is: `Enabled: 6`

Rationale:

Attackers can use ActiveX controls that include malicious code to attack a computer. In addition, malicious code can be used to compromise an ActiveX control and attack a computer. To indicate the safety of an ActiveX control, developers can denote them as Safe For Initialization (SFI). SFI indicates that a control is safe to open and run, and that it is not capable of causing a problem for any computer, regardless of whether it has persisted data values or not.

Impact:

This setting only increases security for ActiveX controls that are accurately marked as SFI. In situations that involve malicious or poorly designed code, an ActiveX control might be inaccurately marked as SFI.

Important: Some ActiveX controls do not respect the safe mode registry setting, and therefore might load persisted data even though this setting is configured to instruct the control to use safe mode.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `6`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\common\security:uficontrols
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: 6`

```
Microsoft Office 2016\Security Settings\ActiveX Control Initialization
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.5 (L1) Ensure 'Allow Basic Authentication prompts from network proxies' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Apps such as Word and Excel allow users to use Basic authentication to connect to resources on web servers by sending usernames and passwords with each request. These credentials are often stored on the servers, making it easier for attackers to capture them and reuse them against other endpoints or services.

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

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise, and to subscription versions of Project and Visio.

Note 2: This change doesn't affect Outlook connecting to on-premises Exchange Server using Basic authentication. This change also doesn't affect Outlook connecting to Exchange Online using Basic authentication. There is a separate effort to deprecate Basic authentication with Exchange Online. For more information, see Basic authentication deprecation in Exchange Online

Rationale:

Basic authentication is an outdated industry standard and doesn't support more robust security features, such as multifactor authentication. The threats posed by it have only increased and there are better and more effective user authentication alternatives. For example, modern authentication, which supports multifactor authentication, smart cards, and certificate-based authentication.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\identity:basicauthproxybehavior
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Allow Basic Authentication prompts
from network proxies
```

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/DeployOffice/security/basic-authentication-prompts-blocked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3.27.6 (L1) Ensure 'Allow VBA to load typelib references by path from untrusted intranet locations' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting permits VBA to load typelib references by explicit path read from the project data if that path points to an intranet location that is not explicitly in the system trusted sites list.

If this policy setting is enabled, VBA will treat intranet paths like local machine paths, and therefore VBA will attempt to search for unregistered references in intranet locations that are not local machine or in the system's trusted sites list.

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

Rationale:

The Visual Basic Application language can be abused by manipulating typelib references stored in untrusted locations. By preventing a user from overriding the default security settings this prevents a change to an unsecure state where harmful software could be more easily executed on a system.

Impact:

None - this policy enforces the default configuration.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\vba\security:allowvbaintranetreferences
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Allow VBA to load typelib references by path from untrusted intranet locations
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●

2.3.27.7 (L1) Ensure 'Automation Security' is set to 'Enabled: Disable Macros by default' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether macros can run in an Office application that is opened programmatically by another application.

Policy setting option:

`Disable macros by default` - All macros are disabled in the programmatically opened application.

The recommended state for this setting is: `Enabled: Disable Macros by default.`

Rationale:

By default, when a separate program is used to launch Microsoft Office Excel, PowerPoint, or Word programmatically, any macros can run in the programmatically opened application without being blocked. This functionality could allow an attacker to use automation to run malicious code in Excel, PowerPoint, or Word.

Impact:

"Disable macros by default" could limit functionality if an external application programmatically opens a Office application to open a document or template containing macros.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\common\security:automationsecurity
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable Macros by default`:

```
Microsoft Office 2016\Security Settings\Automation Security
```

Default Value:

Disabled. (any macros can run in the programmatically opened application without being blocked)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.3.27.8 (L1) Ensure 'Control how Office handles form-based sign-in prompts' is set to 'Enabled: Block all prompts' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office applications handle form-based sign-in prompts.

Office Forms Based Authentication [MS-OFBA] is a protocol used in Office suite applications since Microsoft Office 2007. It provides a method to authenticate to other services via HTTP over a network connection.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise, and to subscription versions of Project and Visio.

The recommended state for this setting is: `Enabled: Block all prompts`

Rationale:

Office Forms Based Authentication Protocol is legacy protocol and is disabled in Office by default. It is associated with several exploits such as credential theft and denial of service attacks.

Impact:

This enforces the default configuration of Office and will only impact users who have already permitted it in the Trust Center.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common:fbabehavior
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Block all prompts`:

```
Microsoft Office 2016\Security Settings\Control how Office handles form-based sign-in prompts
```

Default Value:

Disabled. (Form-based sign-in prompts are blocked but users can override.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.9 (L1) Ensure 'Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting restricts VBA to checking project library references only against the registry and trusted zones.

The recommended state for this setting is: `Disabled`

Rationale:

A remote code execution vulnerability exists when Microsoft Office improperly loads arbitrary type libraries. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

To exploit the vulnerability, an attacker must first convince a user to open a specially crafted Office document.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\vba\security:disablestrictvbarefssecurity
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine
```

Default Value:

Disabled.

References:

1. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0760

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.10 (L1) Ensure 'Disable all Trust Bar notifications for security issues' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office applications notify users when potentially unsafe features or content are detected, or whether such features or content are silently disabled without notification.

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

Rationale:

The Message Bar in Office applications is used to identify security issues, such as unsigned macros or potentially unsafe add-ins. When such issues are detected, the application disables the unsafe feature or content and displays the Message Bar at the top of the active window. The Message Bar informs the users about the nature of the security issue and, in some cases, provides the users with an option to enable the potentially unsafe feature or content, which could harm the user's computer.

Impact:

This setting does not modify the default configuration, and therefore is unlikely to cause any usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\trustcenter:trustbar
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Disable all Trust Bar notifications for security issues
```

Default Value:

Disabled. (The user can change this behavior by default.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.11 (L1) Ensure 'Disable password to open UI' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office users can add password encryption to documents. (Users would access this feature in Microsoft Office tab--click Info, click Protect Document, then click Encrypt with Password.)

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

Rationale:

This capability can provide an extra level of protection to documents that are already protected by access control lists or provide a means of securing documents that are not protected by file-level security.

If a document is password protected, users without the proper password will be prevented from opening the document(s).

Impact:

The recommended settings enforce the default configuration, and therefore will not affect usability. Typically, this setting should not be enabled, because doing so will prevent users from adding passwords to Office files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:disablepasswordui
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Disable password to open UI
```

Default Value:

Disabled. (Users can encrypt their 2016 Office files with passwords)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.27.12 (L1) Ensure 'Encryption mode for Information Rights Management (IRM)' is set to 'Enabled: Cipher Block Chaining (CBC)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls the encryption mode that Office uses to protect content with Information Rights Management.

- For Microsoft 365 Apps (Version 2304 or later): Cipher Block Chaining (CBC) mode is used
- For earlier Microsoft 365 Apps and Office LTSC 2021, 2019, and 2016: Electronic Codebook (ECB) mode is used

The recommended state for this setting is: `Enabled: Cipher Block Chaining (CBC).`

Rationale:

Electronic Codebook (ECB) has several weaknesses, such as the lack of diffusion, determinism, and susceptibility to pattern attacks. As a result, organizations like NIST and ISO recommend against its use.

To ensure a higher level of security, Cipher Block Chaining (CBC) can be enforced. This block cipher mode will be used to encrypt IRM content with applications like Excel, PowerPoint, Word, Visio, or Outlook, regardless of their versions.

Impact:

There is no impact or additional overhead associated with using CBC over ECB.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\drm:compatibleencryption
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Cipher Block Chaining (CBC)`:

```
Microsoft Office 2016\Security Settings\Encryption mode for Information
Rights Management (IRM)
```

Default Value:

For Microsoft 365 Apps (Version 2304 or later): Cipher Block Chaining (CBC) mode is used by default

For earlier Microsoft 365 Apps and Office LTSC 2021, 2019, and 2016: Electronic Codebook (ECB) mode is used by default

References:

1. https://support.microsoft.com/en-gb/office/restrict-access-to-documents-with-information-rights-management-in-word-94aa8ab1-465e-42d7-a323-d61f911b2d0f
2. https://csrc.nist.gov/pubs/sp/800/38/a/final

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●

2.3.27.13 (L1) Ensure 'Encryption type for password protected Office 97-2003 files' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables specification of an encryption type for password-protected Office 97-2003 files.

The recommended state for this setting is: `Enabled: Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`.

Rationale:

If unencrypted files are intercepted, sensitive information in the files can be compromised. To protect information confidentiality Microsoft Office application files can be encrypted and password protected. Only users who know the correct password will be able to decrypt such files.

Impact:

Consider the needs of the organization and users when selecting an encryption method to enforce. If working for a government agency, contracting for a government agency, or otherwise working with very sensitive information, select a method that complies with policies that govern how such information is processed. Remember to ensure that the selected cryptographic service provider is installed on the computers of all users who need to work with password-protected Office 97-2003 files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:defaultencryption12
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`:

```
Microsoft Office 2016\Security Settings\Encryption type for password
protected Office 97-2003 files
```

Default Value:

Excel, PowerPoint, and Word use Office 97/2000 Compatible encryption, a proprietary encryption method, to encrypt password-protected Office 97-2003 files.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●

2.3.27.14 (L1) Ensure 'Encryption type for password protected Office Open XML files' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows for specification of an encryption type for Office Open XML files.

The chosen encryption type must have a corresponding cryptographic service provider (CSP) installed on the computer that encrypts the file.

Note: This policy setting does not take effect unless the registry key HKEY_CURRENT_USER\Software\Microsoft\Office\16.0<office application name>\Security\Crypto\CompatMode is set to 0. By default the CompatMode registry key is set to 1.

The recommended state for this setting is: `Enabled: Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`.

Rationale:

If unencrypted files are intercepted, sensitive information in the files can be compromised. To protect information confidentiality, Office application files can be encrypted and password protected. Only users who know the correct password will be able to decrypt such files.

Impact:

Consider the needs of the organization and users when selecting an encryption method to enforce. If working for a government agency, contracting for a government agency, or otherwise working with very sensitive information, select a method that complies with policies that govern how such information is processed. Remember to ensure that the selected cryptographic service provider is installed on the computers of all users who need to work with password-protected Office Open XML files.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:openxmlencryption
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256`:

```
Microsoft Office 2016\Security Settings\Encryption type for password protected Office Open XML files
```

Default Value:

Enabled. (CSP used is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●

2.3.27.15 (L1) Ensure 'Load Controls in Forms3' is set to 'Enabled: 4' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines how ActiveX controls in UserForms should be initialized based upon whether they are Safe For Initialization (SFI) or Unsafe for Initialization (UFI).

Policy setting option options for load controls in Forms3:

`4` - For a UFI signed control, load with the default properties of the control. For an SFI signed control, load in safe mode (considered to be the safest mode).

The recommended state for this setting is: `Enabled: 4`.

Rationale:

ActiveX controls are Component Object Model (COM) objects and have unrestricted access to users' computers. ActiveX controls can access the local file system and change the registry settings of the operating system. If a malicious user repurposes an ActiveX control to take over a user's computer, the effect could be significant.

To help improve security, ActiveX developers can mark controls as Safe For Initialization (SFI), which means that the developer states that the controls are safe to open and run and not capable of causing harm to any computers. If a control is not marked SFI, the control could adversely affect a computer — or it's possible the developers did not test the control in all situations and are not sure whether their control might be compromised at some future date.

SFI controls run in safe mode, which limits their access to the computer. For example, a worksheet control can both read and write files when it is in unsafe mode, but perhaps only read from files when it is in safe mode. This functionality allows the control to be used in very powerful ways when safety wasn't important, but the control would still be safe for use in a Web page.

If a control is not marked as SFI, it is marked Unsafe For Initialization (UFI), which means that it is capable of affecting a user's computer. If UFI ActiveX controls are loaded, they are always loaded in unsafe mode.

This setting allows administrators to control how ActiveX controls in UserForms should be initialized based upon whether they are SFI or UFI.

Impact:

Disabling the policy is the equivalent to enabling it and selecting option 1, which is the default behavior and therefore unlikely to cause any unexpected usability issues.

Audit:

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

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\vba\security:loadcontrolsinforms
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: 4`:

```
Microsoft Office 2016\Security Settings\Load Controls in Forms3
```

Default Value:

Enabled: Option 1 (For a UFI or SFI signed control that supports safe and unsafe mode, load the control in unsafe mode. For an SFI signed control that only supports a safe mode configuration, load the control in safe mode.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.27.16 (L1) Ensure 'Macro Runtime Scan Scope' is set to 'Enabled: Enable for all documents' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies the behavior for both the VBA and Excel 4.0 (XLM) runtime scan features. Multiple Office apps support VBA macros, but XLM macros are only supported by Excel.

The VBA and XLM runtimes report certain high-risk code behaviors to an antivirus system before the macro executes them. This enables the antivirus system to assess whether the macro's behavior is malicious or not. If the behavior is identified as malicious, the Office application terminates the session, and the antivirus system can quarantine the file. If the behavior is deemed non-malicious, the macro execution continues.

NOTE: Macros can only be scanned if the anti-virus software registers as an Antimalware Scan Interface (AMSI) provider on the device.

NOTE#2: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise.

The recommended state for this setting is: `Enabled: Enable for all documents`

Rationale:

Macros may contain harmful functions designed to inject malicious software into a system, escalate privilege, and be a first entry point in the attack chain. By utilizing the AMSI interface on supporting anti-virus applications, defenders will increase the possibility that malicious software is identified and thwarted before it executes.

Impact:

When macro runtime scanning is enabled, the runtime performance of affected VBA projects and XLM sheets may be reduced.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:macroruntimescanscope
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Enable for all documents`:

```
Microsoft Office 2016\Security Settings\Macro Runtime Scan Scope
```

Default Value:

Not configured. (Equivalent of Enabled: Enable for low trust files)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

2.3.27.17 (L1) Ensure 'Protect document metadata for password protected files' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether metadata is encrypted when an Office Open XML file is password protected.

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

Rationale:

By default, when an Office Open XML document is protected with a password and saved, any metadata associated with the document is encrypted along with the rest of the document's contents. If this configuration is changed, potentially sensitive information such as the document author and hyperlink references could be exposed to unauthorized people.

Impact:

Enabling this setting might interfere with the functioning of tools that aggregate and display metadata information for Office Open XML files but is otherwise unlikely to cause significant usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:openxmlencryptproperty
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Security Settings\Protect document metadata for password protected files
```

Default Value:

Enabled. (Metadata associated with the document is encrypted.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●

2.3.27.18 (L1) Ensure 'Protect document metadata for rights managed Office Open XML Files' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether metadata is encrypted in Office Open XML files that are protected by Information Rights Management (IRM).

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

Rationale:

By default, when Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted. This configuration could allow potentially sensitive information such as the document author and hyperlink references to be exposed to unauthorized people.

Impact:

Enabling this setting might interfere with the functioning of tools that aggregate and display metadata information for Office Open XML files but is otherwise unlikely to cause significant usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:drmencryptproperty
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Security Settings\Protect document metadata for rights managed Office Open XML Files
```

Default Value:

Disabled. (Metadata associated with IRM restricted documents is not encrypted.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●

2.3.27.19 (L1) Ensure 'Suppress hyperlink warnings' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office applications notify users about unsafe hyperlinks. Links that Office considers unsafe include links to executable files, TIFF files, and Microsoft Document Imaging (MDI) files. Other unsafe links are those that use protocols considered to be unsafe such as javascript.

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

Rationale:

Unsafe hyperlinks are links that might pose a security risk if users click them. Clicking an unsafe link could compromise the security of sensitive information or harm the computer.

Links that Office considers unsafe include links to executable files, TIFF files, and Microsoft Document Imaging (MDI) files. Other unsafe links are those that use protocols considered to be unsafe, including msn, nntp, mms, outlook, and stssync.

By default, Office applications notify users about unsafe hyperlinks and disable them until users enable them.

Impact:

This setting does not alter the default configuration and therefore is unlikely to provide any usability concerns.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\security:disablehyperlinkwarning
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Security Settings\Suppress Hyperlink Warnings
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.28 Server Settings

This section contains settings to configure Server Settings.

2.3.28.1 SharePoint Server

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.28.2 (L1) Ensure 'Disable the Office client from polling the SharePoint Server for published links' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office applications can poll Office servers to retrieve lists of published links.

Note: This policy setting applies to Microsoft SharePoint Server specifically. It does not apply to Microsoft SharePoint Foundation.

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

Rationale:

By default, users of Office applications can see and use links to Microsoft Office SharePoint Server sites from those applications. Administrators configure published links to Office applications during initial deployment and can add or change links as part of regular operations. These links appear on the My SharePoint Sites tab of the Open, Save, and Save As dialog boxes when opening and saving documents from these applications. Links can be targeted so that they only appear to users who are members of particular audiences.

If a malicious person gains access to the list of published links, they could modify the links to point to unapproved sites, which could make sensitive data vulnerable to exposure.

Impact:

If this setting is Enabled, users will not be able to use the list of published links to open and save files directly from within Office applications, which could hinder the use of SharePoint Server for document collaboration.

Note#2: This setting applies to Microsoft Office SharePoint Server specifically. It does not apply to Windows SharePoint Services (WSS).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\portal:linkpublishingdisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Server Settings\Disable the Office client from polling the SharePoint Server for published links
```

Default Value:

Disabled. (Users of Office 2016 applications can see and use links to Microsoft SharePoint Server sites from those applications)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.29 Services

This section contains settings to configure Services.

2.3.29.1 Fax

This section configures settings to configure Fax options.

2.3.29.1.1 (L1) Ensure 'Disable Internet Fax feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can access the Internet Fax feature in Office applications.

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

Rationale:

Excel, PowerPoint, and Word users can use the Internet Fax feature to send documents to fax recipients through an Internet fax service provider. If the organization has policies that govern the time, place, or manner in which faxes are sent, this feature could help users evade those policies.

Impact:

If the Internet Fax feature is used by the organization to send faxes, enabling this setting will cause users to lose this functionality. In such situations, ensure that users who need to send faxes have some other mechanism for doing so.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\services\fax:nofax
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Services\Fax\Disable Internet Fax Feature
```

Default Value:

Disabled. (Users can use the Internet Fax feature.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.30 Shared Paths

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.31 Signing

This section contains settings for configuring Signing options.

2.3.31.1 (L1) Ensure 'Legacy format signatures' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can apply binary format digital signatures to Office 97-2003 documents.

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

Rationale:

By default, Office applications use the XML-based XMLDSIG format to attach digital signatures to documents, including Office 97-2003 binary documents. XMLDSIG signatures are not recognized by Office 2003 applications or previous versions. If an Office 2003 user opens an Excel, PowerPoint, or Word binary document with an XMLDSIG signature attached, the signature will be lost.

Impact:

Enabling this setting is not likely to cause significant usability issues for most Office users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\signatures:enablecreationofweakxpsignatures
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Signing\Legacy format signatures
```

Default Value:

Disabled. (Office applications use the XML--based XMLDSIG format to attach digital signatures to documents.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.31.2 (L1) Ensure 'Suppress external signature services menu item' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook displays the "Add Signature Services" menu item.

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

Rationale:

By default, users can select Add Signature Services (from the Signature Line drop-down menu on the Insert tab of the Ribbon in Excel, PowerPoint, and Word) to see a list of signature service providers on the Microsoft Office Web site. If the organization has policies that govern the use of external resources such as signature providers or Office Marketplace, allowing users to access the Add Signature Services menu item might enable them to violate those policies.

Impact:

Enabling this setting prevents users from adding a signature service from Microsoft Office.com but should not otherwise cause significant usability issues for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\signatures:suppressextsigningsvcs
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Signing\Suppress external signature services menu item
```

Default Value:

Disabled. (Users can select "Add Signature Services" to see a list of providers.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.32 Smart Documents (Word, Excel)

This section contains settings to configure Smart Documents.

2.3.32.1 (L1) Ensure 'Disable Smart Document's use of manifests' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Office applications can load an XML expansion pack manifest file with a Smart Document.

An XML expansion pack is the group of files that constitutes a Smart Document in Excel and Word. Packaging of one or more components provides the logic needed for a Smart Document using an XML expansion pack. These components can include any type of file, including XML schemas, Extensible Stylesheet Language Transforms (XSLTs), dynamic-link libraries (DLLs), and image files, as well as additional XML files, HTML files, Word files, Excel files, and text files.

The key component to building an XML expansion pack is creating an XML expansion pack manifest file. By creating this file, the locations of all files that make up the XML expansion pack is specified, as well as information that instructs Office how to set up the files for Smart Document. The XML expansion pack can also contain information about how to set up some files, such as how to install and register a COM object required by the XML expansion pack.

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

Rationale:

XML expansion packs can be used to initialize and load malicious code, which might affect the stability of a computer and lead to data loss.

Impact:

Enabling this setting prevents users from working with Smart Documents.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\common\smart
tag:neverloadmanifests
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Smart Documents (Word, Excel)\Disable Smart Document's
Use of Manifests
```

Default Value:

Disabled. (Office 2016 applications can load an XML expansion pack manifest file with a Smart Document.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.33 Subscription Activation

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.34 Telemetry Dashboard

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.35 Tools | AutoCorrect Options... (Excel, PowerPoint and Access)

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.36 Tools | Options | General | Service Options...

This section contains settings to configure Office options.

2.3.36.1 Conversion Service

This section contains recommendations for the Microsoft Conversion Service.

2.3.36.1.1 (L2) Ensure 'Conversion Service Options' is set to 'Enabled: Do not allow to use Microsoft Conversion Service' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls users' access to the online features of Office 2016.

The recommended state for this setting is: `Enabled: Do not allow to use Microsoft Conversion Service`

Rationale:

In a high security environment data should never be sent to 3rd parties as there could be an accidental spillage of sensitive information. Online Content, online tips and other internet connected services baked into applications (whether innocent from the software vendor's perspective or not) can allow for a covert channel to exist where information can travel through.

Impact:

Conversion services will be unavailable.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\internet:useconversionservices
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow to use Microsoft Conversion Service`:

```
Microsoft Office 2016\Tools | Options | General | Service Options...\Online Content\Conversion Service\Conversion Service Options
```

Default Value:

Disabled. (The conversion service is accessible.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.36.2 Online Content

This section contains settings to configure Online Content.

2.3.36.2.1 (L2) Ensure 'Online Content Options' is set to 'Enabled: Do not allow Office to connect to the Internet' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls users' access to the online features of Office.

Policy setting option for user access to online content and services:

`Do not allow Office to connect to the Internet` – Office applications do not connect to the Internet to access online services, or to download the latest online content from Office.com. Connected features of Office 2016 are disabled.

NOTE: This does not apply to Office 365 Apps for Enterprise but does apply to Office 2016 and 2019. Office 365 has a separate set of group policies for these controls.

The recommended state for this setting is: `Enabled: Do not allow Office to connect to the Internet`

Rationale:

In a high security environment data should never be sent to 3rd parties as there could be an accidental spillage of sensitive information. Online Content, online tips and other internet connected services baked into applications (whether innocent from the software vendor's perspective or not) can allow for a covert channel to exist where information can travel through.

Impact:

Configuring this setting to "Do not allow Office to connect to the internet" will cause disruptions for users who are accustomed to receiving content from Microsoft Office.com within Office applications. These users will still have to access Microsoft Office.com using their Web browsers to obtain this content, if permitted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\internet:useonlinecontent
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Do not allow Office to connect to the Internet`:

```
Microsoft Office 2016\Tools | Options | General | Service Options...\Online
Content\Online Content Options
```

Default Value:

Not Configured. (Office applications will be permitted to connect online.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.37 Tools | Options | General | Web Options...

This section contains settings to configure Office options.

2.3.37.1 Browsers

This section contains settings to configure Browser options.

2.3.37.2 Encoding

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.37.3 Files

This section contains settings to configure Files options.

2.3.37.3.1 (L1) Ensure 'Open Office documents as read/write while browsing' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can edit and save Office documents on Web servers that they have opened using Internet Explorer.

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

Rationale:

By default, when users browse to an Office document on a Web server using Internet Explorer, the appropriate application opens the file in read-only mode. However, if the default configuration is changed, the document is opened as read/write. Users could potentially make changes to documents and overwrite them in situations where the Web server security is not configured to prevent such changes.

Impact:

This setting enforces the Office default configuration and therefore should have minimal impact on users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\internet:opendocumentsrea
dwritewhilebrowsing
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Tools | Options | General | Web Options...\Files\Open
Office Documents as Read/Write While Browsing
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.3.37.4 General

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.3.38 Tools | Options | Spelling

This section contains settings to configure Office Options.

2.3.38.1 Proofing Data Collection

This section contains settings to configure Proofing Data Collection.

2.3.38.1.1 (L2) Ensure 'Improve Proofing Tools' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether the Help Improve Proofing Tools feature sends usage data to Microsoft. The Help Improve Proofing Tools feature collects data about use of the Proofing Tools, such as additions to the custom dictionary, and sends it to Microsoft. After about six months, the feature stops sending data to Microsoft and deletes the data collection file from the user's computer.

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

Rationale:

Although this feature does not intentionally collect personal information, some of the content that is sent could include items that were marked as spelling or grammar errors, such as proper names and account numbers. However, any numbers such as account numbers, street addresses, and phone numbers are converted to zeroes when the data is collected. Microsoft uses this information solely to improve the effectiveness of the Office Proofing Tools, not to identify users.

Impact:

The Customer Experience Improvement Program sends proofing tool data to Microsoft silently and without affecting application usage, so disabling the collection and transmission of proofing tool data is unlikely to cause usability issues for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\ptwatson:ptwoptin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Tools | Options | Spelling\Proofing Data Collection\Improve Proofing Tools
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.39 Trust Center

This section contains settings to configure Trust Center.

2.3.39.1 (L1) Ensure 'Send Office Feedback' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can provide feedback to Microsoft about their product experiences with Microsoft 365 products. Microsoft will use this feedback to improve the product for users.

Note: This policy setting only applies to subscription versions of Office, such as Microsoft 365 Apps for enterprise, and to subscription versions of Project and Visio.

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

Rationale:

Due to privacy concerns, users should not be able to send data to any third party unless approved by the System Administrators.

Impact:

If this policy setting is disabled, users will not be able to submit feedback to Microsoft.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\feedback:enabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Trust Center\Send Office Feedback
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.39.2 (L1) Ensure 'Automatically receive small updates to improve reliability' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Microsoft Office Diagnostics is enabled. Office Diagnostics enables Microsoft to diagnose system problems by periodically downloading a small file to the computer.

Rationale:

Office Diagnostics is used to improve the user experience by periodically downloading a small file to the computer with updated help information about specific problems. If Office Diagnostics is enabled, it collects information about specific errors and the IP address of the computer. When new help information is available, that help information is downloaded to the computer that experienced the related problems. Office Diagnostics does not transmit any personally identifiable information to Microsoft other than the IP address of the computer requesting the update.

By default, users can opt into receiving updates from Office Diagnostics the first time they run an Office application. If the organization has policies that govern the use of external resources such as Office Diagnostics, allowing users to opt into this feature might cause them to violate these policies.

Impact:

Disabling this setting will prevent users from receiving information and advice from Microsoft about fixing and preventing Office application errors, which could cause your support department to experience an increase in desktop support requests.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common:updatereliabilitydata
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Trust Center\Automatically Receive Small Updates to
Improve Reliability
```

Default Value:

Enabled. (Users can opt into receiving these updates at first run.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.3.39.3 (L1) Ensure 'Disable Opt-in Wizard on first run' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users see the Opt-in Wizard the first time they run a Microsoft Office application.

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

Rationale:

By default, the Opt-in Wizard displays the first time users run a Microsoft Office application, which allows them to opt into Internet-based services that will help improve their Office experience, such as Microsoft Update, the Customer Experience Improvement Program, Office Diagnostics, and Online Help. If the organization has policies that govern the use of such external resources, allowing users to opt into these services might cause them to violate the policies.

Impact:

Enabling this setting will prevent users from opting into the services listed above. This can prevent users from receiving the latest program updates, security fixes, and Help content. If this setting is enabled, consider ensuring that such updates are made available to users through alternate means.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\general:shownfirstrunoption
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Office 2016\Trust Center\Disable Opt-in Wizard on First Run
```

Default Value:

Disabled. (Opt-in Wizard will display.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.39.4 (L1) Ensure 'Enable Customer Experience Improvement Program' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can participate in the Microsoft Office Customer Experience Improvement Program to help improve Microsoft Office. When users choose to participate in the Customer Experience Improvement Program (CEIP), Office 2016 applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.

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

Rationale:

When users choose to participate in the Customer Experience Improvement Program (CEIP), Office applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.

By default, users can opt into participation in the CEIP the first time they run an Office application. If the organization has policies that govern the use of external resources such as the CEIP, allowing users to opt into the program might cause them to violate these policies.

Impact:

The Customer Experience Improvement Program sends data to Microsoft silently and without affecting application usage, so choosing Disabled will not cause usability issues for Office users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common:qmenable
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Trust Center\Enable Customer Experience Improvement Program
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.3.39.5 (L1) Ensure 'Send personal information' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether users can send personal information to Office. When users choose to send information Office applications automatically send information to Office.

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

Rationale:

Due to privacy concerns, users should not be able to send data to any third party unless approved by the System Administrators.

Impact:

If this policy setting is disabled, Office users cannot send personal information to Office.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common:sendcustomerdata
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Office 2016\Trust Center\Send personal information
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.4 Microsoft OneNote 2016

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5 Microsoft Outlook 2016

This section includes recommendations for Microsoft Outlook.

This Group Policy section is provided by the Group Policy template `outlk16.admx/adml` that is available from Microsoft using the link from the overview section of this document.

2.5.1 Account Settings

This section contains settings to configure all Outlook account settings.

2.5.1.1 E-mail

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.1.2 Exchange

The section contains settings on how outlook connects with Exchange.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents users from changing their mail folder permissions.

If this policy setting is enabled, 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.

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.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\folders:disableeditpermissions
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

2.5.1.3 Exchange ActiveSync

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.1.4 IMAP

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.1.5 Internet Calendars

This section includes setting for configuring Internet Calendars.

2.5.1.5.1 (L1) Ensure 'Automatically download attachments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook downloads files attached to 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.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\webcal:enableattachments
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Account Settings\Internet Calendars\Automatically download attachments
```

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls 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.

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 the organization has policies that govern the use of external resources such as Internet calendars, this feature might enable users to violate those policies.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\webcal:disable
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Account Settings\Internet Calendars\Do not include
Internet Calendar integration in Outlook
```

Default Value:

Disabled. (Outlook allows users to subscribe to Internet calendars.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

2.5.1.6 RSS Feeds

This section contains settings for configuring RSS Feeds within outlook.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook automatically makes an offline copy of the RSS items as HTML attachments.

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

Rationale:

Many RSS feeds use messages that contain a 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.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\rss:enablefullte
xthtml
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Default Value:

Disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\rss:synctosyscfl
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Account Settings\RSS Feeds\Synchronize Outlook RSS
Feeds with Common Feed List
```

Default Value:

Disabled. (Outlook does not automatically subscribe to RSS Feeds)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.1.6.3 (L1) Ensure 'Turn off RSS feature' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the RSS aggregation feature in Outlook. Users can subscribe to RSS feeds from within Outlook and read RSS items like e-mail messages.

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

Rationale:

If the 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.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\options\rss:disable
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Account Settings\RSS Feeds\Turn Off RSS Feature
```

Default Value:

Disabled. (Users can subscribe to RSS Feeds from within Outlook.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.1.7 SharePoint Lists

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.2 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.4 Folder Home Pages for Outlook Special Folders

This section contains settings for Folder Home Pages.

2.5.4.1 (L1) Ensure 'Do not allow Home Page URL to be set in folder Properties' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Users can set a URL to be used as the Home Page for a folder by entering the URL on the Home Page tab on the folder's Properties dialog box.

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

Rationale:

In CVE-2017-11774, a client-side Outlook attack exists that involves modifying victims' Outlook client homepages for code execution and persistence. While this has been patched by Microsoft, security researchers such as FireEye have noticed the bypassing of this patch through registry manipulation.

Implementing this recommendation alongside CIS recommendation **Ensure 'Do not allow folders in non-default stores to be set as folder home pages' is set to 'Enabled'** will help prevent the removal of protections against CVE-2017-11774.

Impact:

Users will be unable to configure this option.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\webview:disable
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Folder Home Pages for Outlook Special Folders\Do not allow Home Page URL to be set in folder Properties
```

Default Value:

Disabled. (Users can set a URL to be used as the Home Page for a folder.)

References:

1. https://www.mandiant.com/resources/blog/breaking-the-rules-tough-outlook-for-home-page-attacks
2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11774

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.5 Form Region Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.6 InfoPath Integration

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.7 Meeting Workspace

This section contains settings for configuring Meeting Workspace.

2.5.7.1 (L1) Ensure 'Disable user entries to server list' is set to 'Enabled: Publish default, disallow others' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook users can add entries to the list of SharePoint servers when establishing a meeting workspace.

Policy setting option to determine whether Outlook users can add entries to the published server list:

`Publish default, disallow others` - This option prevents users from adding servers to the default published server list.

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 the organization's information security requirements, which could cause sensitive information to be at risk.

Impact:

Users in the organization who have a legitimate need to use servers other than those in the published server list will need to obtain administrative assistance.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\meetings\profile:serverui
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Publish default, disallow others`:

```
Microsoft Outlook 2016\Meeting Workspace\Disable user entries to server list
```

Default Value:

Enabled. (Publish default, allow others.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.8 MIME to MAPI Conversion

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.9 Miscellaneous

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

2.5.9.1 Miscellaneous

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.9.2 PST Settings

This section contains settings for configuring PST Settings.

2.5.9.2.1 (L1) Ensure 'PST Null Data on Delete' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether or not Outlook is forced to fully nullify deleted data in users' Personal Folder files (.pst) at the time that the data is deleted.

NOTE: This setting does not apply to (.ost) files generated when Outlook is connected to either Exchange or Exchange Online.

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

Rationale:

When a user deletes mail or other items in Outlook, the data is retained in a portion of the PST file until it is purged or overwritten. Attackers could potentially recover the data by using PST recovery tools. Nulling the data at deletion time will impede this.

Impact:

Forensics and data recovery of objects permanently removed by a user taking action to empty their Outlook trash bin will be made more difficult. These will need to be recovered by another method such as a system backup.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\PST:pstnullfreeondelete
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Miscellaneous\PST Settings\PST Null Data on Delete
```

Default Value:

Disabled. (Data remains in the PST files until it is purged or overwritten by the user.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 Securely Dispose of Data Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	●	●	●

2.5.10 Outlook Options

This section contains settings for configuring Outlook options.

2.5.10.1 Customize Ribbon

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.2 Delegates

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.3 Mail

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.4 Mail Format

This section contains settings for configuring Mail format.

2.5.10.4.1 International Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.4.2 Internet Formatting

This section contains settings for configuring Internet Formatting.

2.5.10.4.2.1 Message Format

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.4.2.2 (L1) Ensure 'Plain Text Options' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how plain text messages are formatted when they are sent from Outlook.

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

Rationale:

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.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\options\mail:message plain format mime
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Outlook Options\Mail Format\Internet Formatting\Plain text options
```

Default Value:

Disabled. (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".)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.5.10.4.3 Stationery and Fonts

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.5 Mail Setup

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.6 Other

This section contains settings for configuring Other settings within Outlook.

2.5.10.6.1 Advanced

This section contains settings for configuring Advanced settings withing Outlook.

2.5.10.6.1.1 Reminder Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting allows unblocking of folder home pages for folders in non-default stores.

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.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:nondefaultstore script
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Enabled. (Creating folder home pages for folders in non-default stores is blocked.)

References:

1. https://www.mandiant.com/resources/blog/breaking-the-rules-tough-outlook-for-home-page-attacks

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.6.2 AutoArchive

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook is the default program for e-mail, contacts, and calendar services. If this policy setting is enabled, 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.

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

Rationale:

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 the 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.

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. Enabling this setting is therefore unlikely to cause usability issues.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\general:check default client
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Enabled. (Outlook is the default, but users can change the setting.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	●	●	●

2.5.10.7 Out of Office Assistant

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8 Preferences

This section contains setting for configuring preferences within Outlook.

2.5.10.8.1 Calendar Options

This section contains settings for configuring Calendar Options within Outlook.

2.5.10.8.1.1 Free/Busy Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8.1.2 Office.com Sharing Service

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

2.5.10.8.1.2.1 (L1) Ensure 'Access to published calendars' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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

Rationale:

If this policy setting is unconfigured, 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.

When this setting is configured (enabled or disabled) 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.

Impact:

Most users do not publish their calendars to be available to every user on Office.com, so the effect will likely be minimal.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\pubcal:restrictedaccessonly
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Not configured. (Users can share their calendars with others without restrictive access.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

2.5.10.8.1.2.2 (L1) Ensure 'Prevent publishing to a DAV server' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook users can publish their calendars to a Distributed Authoring and Versioning (DAV) server.

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

Rationale:

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.

Impact:

This setting could 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\pubcal:disableda
v
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled. (Outlook users can publish calendars to servers using WebDAV.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.5.10.8.1.2.3 (L1) Ensure 'Prevent publishing to Office.com' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook users can publish their calendars to the Office.com Calendar Sharing Service.

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

Rationale:

When users publish their calendars to Office.com, it shares calendar and availability information with other people outside of the organization. If a calendar is visible to everyone on Office.com or third-party DAV servers, sensitive information contained in calendar appointments might be revealed.

Impact:

This setting could cause disruptions for Outlook users who publish their calendar data to Microsoft Office.com.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\pubcal:disableofficeonline
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled. (Users can publish and control who can view their calendar on Office.com)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

The recommended state for this setting is: `Enabled: Disables 'Full details' and 'Limited details'.`

Rationale:

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.

Impact:

This setting 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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `16384`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\options\pubcal:publishcalendardetailspolicy
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disables 'Full details' and 'Limited details'`:

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

Default Value:

Disabled. (Outlook users can share their calendars at any detail level.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.1.2.5 (L1) Ensure 'Restrict upload method' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook can automatically upload calendar updates to Office.com.

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

Rationale:

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. Allowing this could inadvertently expose data that was not meant to be shared.

Impact:

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\pubcal:singleuploadonly
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Not configured. (Outlook updates the calendars online at regular intervals unless changed by user.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.1.3 Planner Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8.1.4 Recurring Item Configuration

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8.1.5 Schedule View

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8.2 Contact Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.8.3 E-mail Options

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

2.5.10.8.3.1 (L2) Ensure 'Read e-mail as plain text' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 this policy is enabled, 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.

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

Rationale:

This option only changes the way e-mail messages are displayed; the original message is not converted to plain text format.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:readasplain
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Outlook Options\Preferences\E-mail Options\Read e-mail as plain text
```

Default Value:

Disabled. (Outlook displays e-mail messages in the format received.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.3.2 (L2) Ensure 'Read signed e-mail as plain text' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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.

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

Rationale:

This option only changes the way e-mail messages are displayed; the original message is not converted to plain text format.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:readsignedasplain
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled. (Outlook displays digitally signed e-mail messages in the format they were received in.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.4 Junk E-mail

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

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether recipients' e-mail addresses are automatically added to the user's Safe Senders List in Microsoft Outlook.

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 user's Junk E-mail folder, even if it would otherwise be considered junk.

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, administrators can choose to enable the setting for some groups of users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:junkmailtru
stoutgoingrecipients
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Default Value:

Not Configured. (Recipients of out going messages are not automatically added but this can be overridden by the user.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.4.2 (L1) Ensure 'Hide Junk Mail UI' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the Junk E-mail Filter is enabled in Outlook.

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.

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.

Impact:

This setting enforces the default and should have no impact to users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook:disableantispam
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Outlook Options\Preferences\Junk E-mail\Hide Junk Mail UI
```

Default Value:

Disabled. (The Junk E-mail filter in Outlook is enabled.)

Additional Information:

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. Use the "Junk E-mail Protection level" setting to preset a filtering level and prevent users from changing it.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.4.3 (L1) Ensure 'Trust e-mail from contacts' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook analyzes e-mail from users' Contacts when filtering junk e-mail.

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

Rationale:

E-mail addresses in users' Contacts list are treated as safe senders for purposes of filtering junk e-mail. If a trusted contact's email is hijacked or compromised, the recipient of a spam campaign may become a victim as the e-mail won't receive the same scrutiny from Outlook's junk e-mail filtering.

Impact:

When disabled, emails from certain contacts may be classified as junk mail, depending on their content. Outlook users will need to check their junk email folder more frequently to avoid missing important messages. However, this increased scrutiny can lead to a decreased level of trust in these emails.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:junkmailtrustcontacts
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Outlook Options\Preferences\Junk E-mail\Trust e-mail from contacts
```

Default Value:

Enabled. (Contacts are treated as safe senders.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.10.8.5 Search Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.9 Right-to-Left

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.10 Spelling

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.10.11 (L2) Ensure 'Internet and network paths into hyperlinks' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

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 in Outlook.

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.

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 URL or path.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the recommended value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\Outlook\options\autoformat:pgrfafo_25_1
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Outlook Options\Internet and Network Paths into Hyperlinks
```

Default Value:

Enabled. (Applicable text is automatically turned into hyperlinks.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.11 Outlook Social Connector

This section contains settings for configuring Outlook Social Connector.

2.5.11.1 (L1) Ensure 'Turn off Outlook Social Connector' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the configuration of the Outlook Social Connector. The Outlook Social Connector allows users to work in Outlook while staying up to date on the status and activities of their friends and contacts, whether they're from an organization, or from social networking sites on the Internet, like Facebook and LinkedIn.

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

Rationale:

Data may be synchronized between Outlook and the users' social media networks, like Facebook and LinkedIn.

Impact:

The Outlook Social Connector will be disabled preventing users from synchronizing data in Outlook with their social media networks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\outlook\socialconnector:runosc
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Outlook Social Connector\Turn off Outlook Social Connector
```

Default Value:

Disabled. (Outlook Social connector is turned on.)

References:

1. https://docs.microsoft.com/en-us/outlook/troubleshoot/deployment/how-to-manage-outlook-social-connector-via-group-policy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.12 Outlook Today Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.13 Search Folders

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.14 Security

This section contains settings for configuring Security options.

2.5.14.1 Automatic Picture Download Settings

This section contains settings for configuring Automatic Picture Download Settings.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook automatically downloads external content in e-mails from senders in the Safe Senders List or Safe Recipients List.

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

Rationale:

Malicious 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.

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.

Impact:

Outlook will not automatically download external content for messages sent by people listed in user's Safe Senders Lists or Safe Recipients Lists. This will cause users to have to download content for each message individually.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:unblockspec
ificsenders
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Default Value:

Enabled. (Downloads are permitted when users receive e-mail from people listed in the user's Safe Senders List or Safe Recipients List.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.1.2 (L1) Ensure 'Block Trusted Zones' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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

Rationale:

Malicious 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.

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.

Impact:

Outlook will not automatically download external content for messages sent by people listed in user's Safe Senders Lists or Safe Recipients Lists. This will cause users to have to download content for each message individually.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:trustedzone
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Automatic Picture Download Settings\Block Trusted Zones
```

Default Value:

Disabled. (Outlook automatically downloads content from Web sites in the Trusted sites zone in Internet Explorer.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Note: 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 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.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:blockextcontent
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Enabled. (Outlook does not download external content unsafe content.)

Additional Information:

Note: 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook automatically downloads content from safe zones when displaying messages.

Note: This policy setting is *backwards*. Despite the name, *disabling* this 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.

Impact:

Users with e-mail messages that include content from safe zones will be required to download content for each message individually.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:unblocksafezone
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Default Value:

Enabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.2 Cryptography

This section contains settings for configuring Cryptography within Outlook.

2.5.14.2.1 Signature Status Dialog Box

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

2.5.14.2.1.1 (L1) Ensure 'Attachment Secure Temporary Folder' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows administrators to specify a folder path for the Secure Temporary Files rather than using the one that is randomly generated by Outlook.

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

Rationale:

Setting a designated specific path and folder to use as the Secure Temporary Files folder is not recommended because 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.

Impact:

None - This enforces the default.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location which should be **absent,** or **no** registry value defined.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:outlooksecuretempfolder
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Cryptography\Signature Status dialog box\Attachment Secure Temporary Folder
```

Default Value:

Disabled. (Outlook will assign the Secure Temporary Files folder a different random name for each user.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.2.1.2 (L1) Ensure 'Missing CRLs' is set to 'Enabled: Error' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

The recommended state for this setting is: `Enabled: Error`.

Rationale:

If a CRL is missing or unavailable, Outlook cannot determine whether a certificate has been revoked. An improperly issued certificate or one that has been compromised might be used to gain access to data.

Impact:

Users will be prevented from using certificates when the appropriate CRL is not available to verify them. This could increase desktop support requests.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:sigstatusnocrl
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Error`.

```
Microsoft Outlook 2016\Security\Cryptography\Signature Status dialog box\Missing CRLs
```

Default Value:

Disabled. (Warning displayed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.2.1.3 (L1) Ensure 'Missing Root Certificates' is set to 'Enabled: Error' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Outlook functions when a root certificate is missing. Outlook will display either an error or warning based on the status of the root certificate.

The recommended state for this setting is: `Enabled: Error`.

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.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:sigstatusnotrustdecision
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Error`:

```
Microsoft Outlook 2016\Security\Cryptography\Signature Status dialog box\Missing root certificates
```

Default Value:

Enabled: Error (Users will see an error when a root certificate is missing.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the configuration of 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.

Note: 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`.

Note: The title of the Group Policy text is slightly misleading. `Promote Level 2 errors as errors, not warnings` should actually read `Promote Level 2 errors as warnings, not errors` which would align more closely with the description of the various states Enable/Disable.

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.

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

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promoteerrorsas warnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Default Value:

Disabled. (Level 2 errors will be treated as errors.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.2.2 (L1) Ensure 'Do not display 'Publish to GAL' button' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook users can publish e-mail certificates to the Global Address List (GAL). The GAL contains information for all email users, distribution groups, and Exchange resources.

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

Rationale:

Only Administrators should be able to perform tasks such as publishing digital certificates to the GAL.

Impact:

Only Administrators will be able to publish a new or updated certificate to the GAL.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:publishtogaldisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Cryptography\Do not display 'Publish to GAL' button
```

Default Value:

Disabled. (Outlook users can publish their e-mail certificates to the GAL through the "E-mail Security" section of the Trust Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting controls whether Outlook users are allowed to send e-mail messages after they see an encryption warning dialog.

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

Rationale:

If users send messages after seeing an encryption error, it is likely that recipients will not be able to read the e-mail message.

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:disablecontinueencryption
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.2.4 (L1) Ensure 'Message Formats' is set to 'Enabled: S/MIME' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

The recommended state for this setting is: `Enabled: S/MIME`.

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 content. It is therefore important to have a mechanism for signing messages and providing end-to-end encryption.

Impact:

None - This is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:msgformats
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: S/MIME`:

```
Microsoft Outlook 2016\Security\Cryptography\Message Formats
```

Default Value:

Disabled. (S/MIME is used to encrypt and sign.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook decodes encrypted messages itself or passes them to an external program for processing.

If the option `Handle internally` is selected, Outlook decrypts all S/MIME messages itself.

The recommended state for this setting is: `Enabled: Handle internally`

Rationale:

This setting could allow unauthorized and potentially dangerous programs to handle encrypted messages outside of the organization, which could compromise security.

Impact:

The recommended configuration for this setting is `Handle internally`, which enforces the default configuration in Outlook and is unlikely to cause usability issues for most users.

In some situations, administrators might wish to use an external program, such as an add-in, to handle S/MIME message decryption. If a designated external program needed to handle S/MIME messages, an exception to this recommendation must be made.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:externalsmime
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Handle internally`:

```
Microsoft Outlook 2016\Security\Cryptography\S/MIME interoperability with
external clients
```

Default Value:

Enabled (Handle if possible.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.3 Security Form Settings

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

2.5.14.3.1 Attachment Security

This section contains settings for configuring Attachment Security within Outlook.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:dontpromptlevel1attachclose
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.))

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:dontpromptlevel1attachsend
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

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

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

2.5.14.3.2 Custom Form Security

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.14.3.3 Programmatic Security

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.5.14.3.4 (L1) Ensure 'Outlook Security Mode' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting enables the use of a custom set of security settings that are enforced in Outlook. This must be enabled if other Outlook security policy settings mentioned in this guide are to be applied.

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

Rationale:

Users should not be able to configure security themselves. Choosing the lowest levels of security can lead to systems being vulnerable to attack.

Note: This setting is essential for ensuring that the other Outlook security settings mentioned in this baseline are applied as suggested.

Impact:

Enabling this setting prevents users from modifying their own security settings, so it might cause an increase in support calls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:adminsecuritymode
```

Note: This setting shares the same registry key and value as the `Outlook Security Policy` recommendation later in this section. This is because the setting was split into two when Microsoft migrated it from Group Policy to an Intune settings catalog profile. The value of `Enabled` does not have a unique key/value associated with it in the registry, however for assessment purposes it will remain as a separate recommendation.

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
```

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures the use of third-party ActiveX controls in Outlook. This setting can can be configured 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 untrusted third-party controls, the risk of malware infecting the computer increases.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\outlook\16.0\outlook\security:allowactivexoneoffforms
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Load only Outlook Controls`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Allow Active X One Off Forms
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

(Third-party ActiveX controls are not allowed to run in one-off forms in Outlook.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether hyperlinks in suspected phishing e-mail messages in Outlook are allowed.

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.

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

Rationale:

Outlooks Junk E-mail Filter evaluates each incoming message for possible spam or phishing content. Allowing this functionality could stop users from clicking on malicious emails.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:junkmailena
blelinks
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Allow hyperlinks in suspected phishing e-mail messages
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Outlook will not allow hyperlinks in suspected phishing messages, even if they are not classified as junk e-mail.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.7 Deploy and Maintain Email Server Anti-Malware Protections Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether scripts can run in Outlook forms in which the script and layout are contained within the message.

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

Rationale:

Malicious code can be included within Outlook forms and can be executed when users open the form.

Impact:

None - this is the default behavior. Unless users have a legitimate business need for such functionality, this setting should be disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:enableoneofformscripts
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Allow scripts in one-off Outlook forms
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Outlook does not run scripts in forms in which the script and the layout are contained within the message.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.5.14.3.8 (L1) Ensure 'Allow users to demote attachments to Level 2' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Note: If this policy 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\16.0\Outlook\Security\Level1Remov
e
```

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

Rationale:

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 infect their system or compromise the security of sensitive information.

Impact:

Users will not be able to demote a Level 1 file to a Level 2 file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:allowuserstolow
erattachments
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Allow users to demote attachments to Level 2
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Users cannot demote level 1 attachments to level 2.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

2.5.14.3.9 (L1) Ensure 'Authentication with Exchange server' is set to 'Enabled: Kerberos Password Authentication' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls which authentication method Outlook uses to authenticate with an on-premises 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.

Policy setting options for controlling how Outlook authenticates with Microsoft Exchange Server:

`Kerberos Password Authentication` - Outlook attempts to authenticate using the Kerberos protocol only.

Warning: When configuring on Outlook clients that connect to Exchange Online (365), this setting must be set to `Disabled` or left unconfigured.

The recommended state for this setting is: `Enabled: Kerberos Password Authentication`.

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.

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.

Warning: Testing of this setting is necessary before deployment as it could cause interruptions in service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `16`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:authenticationsservice
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Kerberos/NTLM Password Authentication`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Authentication with Exchange Server
```

Warning: When configuring on Outlook clients that connect to Exchange Online (365), this setting must be set to `Disabled` or left unconfigured.
Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Kerberos/NTLM Password Authentication (Outlook will attempt to use Kerberos then NTLM.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●

2.5.14.3.10 (L1) Ensure 'Configure Outlook object model prompt when accessing an address book' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls what happens when an untrusted program attempts to gain access to an Address Book using the Outlook object model. The Outlook object model includes entry points to access Outlook data, save data to specified locations, and send emails.

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

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 or exfiltrate that data.

Impact:

Untrusted programs will not be able to gain access to the Address Book using the Outlook object model.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoomaddres
sinformationaccess
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt when accessing an address book
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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. The Outlook object model includes entry points to access Outlook data, save data to specified locations, and send emails.

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

The recommended state for this setting is: `Enabled: Automatically Deny`.

Rationale:

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

Impact:

Users will not be able to control what happens when a custom form in Outlook is created and will not be able to bind an Address Information field to a combination or formula custom field.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoommeetingtaskrequestresponse
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt When accessing the Formula property
of a UserProperty object
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.14.3.12 (L1) Ensure 'Configure Outlook object model prompt when executing Save As' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

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.

Impact:

Untrusted programs will not be able to use the Save As command to programmatically save an item.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoomsaveas
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt when executing Save As
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.14.3.13 (L1) Ensure 'Configure Outlook object model prompt when reading address information' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

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.

Impact:

Untrusted programs will not be able to gain access to a recipient field, such as the *To:* field, using the Outlook object model.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoomaddressinformationaccess
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt when reading address information
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (When an untrusted application attempts to access recipient fields, Outlook relies on the setting configured in the *Programmatic Access* section of the Trust Center.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.14.3.14 (L1) Ensure 'Configure Outlook object model prompt when responding to meeting and task requests' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

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's response to tasks or meeting requests with false information.

Impact:

Untrusted programs will not be able to programmatically send an e-mail in Outlook using the Response method of a task or meeting request.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoommeetin
gtaskrequestresponse
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt when responding to meeting and task
requests
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

2.5.14.3.15 (L1) Ensure 'Display Level 1 attachments' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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:

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.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:showlevel1attach
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Display Level 1 attachments
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Outlook completely blocks access to Level 1 files, and requires users to save Level 2 files to disk before opening them.)

References:

1. https://support.microsoft.com/en-us/office/blocked-attachments-in-outlook-434752e1-02d3-4e90-9124-8b81e49a8519

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

2.5.14.3.16 (L1) Ensure 'Configure Outlook object model prompt when sending mail' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

When the option `Automatically deny` is selected, Outlook will automatically deny programmatic access requests from any program.

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, impersonates a user, or launches a denial-of-service attack by sending a large volume of mail to a user or group of users.

Impact:

An untrusted program will not be able to send e-mail programmatically using the Outlook object model.

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. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoomsend
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Configure Outlook object model prompt when sending mail
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

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

When an untrusted application attempts to send mail programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook executes scripts that are associated with custom forms or folder home pages for public folders. By enabling this policy setting, Outlook cannot execute any scripts associated with public folders, overriding any configuration changes on users' computers.

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.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:publicfolderscr
ipt
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Do not allow Outlook object model scripts to run for public folders
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Enabled. (Outlook will not run any scripts associated with public folders but users can override.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook executes scripts associated with custom forms or folder home pages for shared folders. If this policy setting is enabled, Outlook cannot execute any scripts associated with shared folders, overriding any configuration changes on users' computers.

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. 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.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:sharedfolderscript
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Do not allow Outlook object model scripts to run for shared folders
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Enabled. (Outlook cannot execute any scripts associated with shared folders.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.5.14.3.19 (L1) Ensure 'Enable RPC encryption' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook uses remote procedure call (RPC) encryption to communicate with Microsoft Exchange servers.

If this policy setting is enabled, 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.

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 encrypted. If this policy is disabled, an end user may modify this setting creating an opportunity for malicious eavesdropping of network traffic between Outlook client and the Exchange server.

Impact:

This is the default behavior and would only impact unsupported versions of Outlook.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\rpc:enablerpcencryption
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Enable RPC encryption
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

RPC Encryption is used by default but can be overridden by per-profile settings.

References:

1. https://learn.microsoft.com/en-us/exchange/troubleshoot/client-connectivity/outlook-connection-issue-caused-by-rpc-encryption-requirement

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.5.14.3.20 (L1) Ensure 'Include Internet in Safe Zones for Automatic Picture Download' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether pictures and external content in HTML e-mail messages from untrusted senders on the Internet are downloaded without Outlook users explicitly choosing to do so.

When Disabled, Outlook does not consider the Internet a safe zone, which means that 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.

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

Rationale:

E-mails sourced from the internet can contain malicious content or phishing links. This security control prevents the content in e-mail messages from automatically reaching the end user, as well as preventing the changing of this setting to an insecure state.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:internet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Include Internet in Safe Zones for Automatic Picture Download
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Outlook does not consider the internet a safe zone.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.3.21 (L1) Ensure 'Junk E-mail protection level' is set to 'Enabled: High' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls your Junk E-mail protection level.

By selecting the `High` option, 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.

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.

Impact:

Users may experience more false positives when this is set to **High**, requiring them to check their Junk e-mail folder more often.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\mail:junkmailprotection
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: High`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Junk E-mail protection level
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Enabled: Low (Users can change their junk e-mail options.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.3.22 (L1) Ensure 'Minimum encryption settings' is set to 'Enabled: 256' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the configuration of the minimum cryptographic key length for encrypting e-mail messages.

The recommended state for this setting is: `Enabled: 256`.

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.

Impact:

Users who see the minimum encryption warning display can still choose to send the message with the selected key, so little to no impact is expected.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `256`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:minenckey
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: 256`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Minimum encryption settings
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.5.14.3.23 (L1) Ensure 'Outlook Security Policy' is set to 'Use Outlook Security Group Policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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

When the option `Use Outlook Security Group Policy` is selected, Outlook uses security settings from Intune configuration profiles.

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 user's 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 user's own computers.

The recommended state for this setting is: `Use Outlook Security Group Policy.`

Rationale:

Users should not be able to configure security themselves. Choosing the lowest levels of security can lead to systems being vulnerable to attack.

Note: This setting is essential for ensuring that the other Outlook security settings mentioned in this baseline are applied as suggested.

Impact:

Enabling this setting prevents users from modifying their own security settings, so it might cause an increase in support calls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:adminsecuritymode
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Outlook Security Policy
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.3.24 (L1) Ensure 'Prevent users from customizing attachment security settings' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting prevents users from overriding the set of attachments blocked by Outlook.

Note: Outlook also checks the *Level1Remove* registry key (which could allow the user to save the file to disk) when this setting is specified.

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

Rationale:

If users can change the security settings for attachments, they could choose a less secure value and increase the risk of being infected and spreading malware.

Impact:

Users will not be able to customize the attachment security settings and legitimate attachments might be blocked.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook:disallowattachmentcustomization
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Prevent users from customizing attachment security settings
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Users will be allowed to override the set of attachments blocked by Outlook.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 user's 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.

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

Rationale:

Malicious code is often spread through e-mail. Some viruses can 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.

Impact:

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting will have **no registry value** (the key will not exist) if it is set to `Disabled`:

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:fileextensionsr
emovelevel1
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode
> Remove file extensions blocked as Level 1
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

References:

1. https://support.microsoft.com/en-us/office/blocked-attachments-in-outlook-434752e1-02d3-4e90-9124-8b81e49a8519

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

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

Rationale:

Malicious code is often spread through e-mail. Some viruses can 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 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 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.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting will have **no registry value** (the key will not exist) if it is set to `Disabled`:

```
HKEY_USERS\[USER SID]\Software\Policies\Microsoft\Office\16.0\Outlook\Security:fileextensionsremovelevel2
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Remove file extensions blocked as Level 2
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (Outlook does not classify any file type extensions as Level 2.)

References:

1. https://support.microsoft.com/en-us/office/blocked-attachments-in-outlook-434752e1-02d3-4e90-9124-8b81e49a8519

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Outlook retrieves Certificate Revocation Lists (CRLs) to verify the validity of certificates. CRLs are lists of digital certificates that have been revoked by their controlling Certificate Authority (CAs), typically because the certificates were issued improperly, or their associated private keys were compromised.

The recommended state for this setting is: `Enabled: When online always retrieve the CRL`.

Rationale:

Outlook may improperly trust a revoked certificate, which could put the system and data at risk.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:usecrlchasing
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: When online always retrieve the CRL`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Retrieving CRLs (Certificate Revocation Lists)
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.3.28 (L1) Ensure 'Security setting for macros' is set to 'Enabled: Warn for signed, disable unsigned' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the security level for macros in Outlook. Macros are a single instruction that expands automatically into a set of instructions to perform a particular task.

Available Policy Options:

`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.

`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.

The recommended state for this setting is: `Enabled: Warn for signed, disable unsigned`.

Rationale:

To protect users from dangerous code, the disabling of 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 is recommended to help against would allow dangerous code to run.

Impact:

None - this is enforcing the default behavior. Unsigned macros will be disabled.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:level
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Warn for signed, disable unsigned`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Security setting for macros
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (The behavior is the equivalent of Enabled -- Warning for signed, disable unsigned.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.5.14.3.29 (L1) Ensure 'Set Outlook object model custom actions execution prompt' is set to 'Enabled: Automatically Deny' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

The recommended state for this setting is: `Enabled: Automatically Deny`.

Rationale:

Malicious code can use the Outlook object model to compromise sensitive information or otherwise cause data and computing resources to be at risk.

Impact:

Configuring this setting to `Automatically Deny` prevents Outlook from executing any custom actions that use the Outlook object model. Users will not be able to utilize this function.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:promptoomcustomaction
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Automatically Deny`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Set Outlook object model custom actions execution prompt
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled: (When Outlook or another program initiates a custom action using the Outlook object model, users are prompted to allow or reject the action.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Outlook warns users about messages with invalid digital signatures.

The recommended state for this setting is: `Enabled: Always warn about invalid signatures`.

Rationale:

If users are not notified about invalid signatures, it might prevent the user from detecting a fraudulent signature sent by a malicious user.

Impact:

None - This is the default behavior.

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location and has the value of `1`:

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:warnaboutinvalid
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Always warn about invalid signatures`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Signature Warning
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Disabled. (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.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether e-mail messages dragged from Outlook to the file system are saved in Unicode or ANSI format.

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

Rationale:

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.

Impact:

ANSI file encoding may limit the overall size a .msg file can reach, although a single mail item should not be of concern.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\options\general:msgformat
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Security Form Settings\Outlook Security Mode > Use Unicode format when dragging e-mail message to file system
```

Important: For this setting to apply, the *Outlook Security Mode* setting must be enabled in *Microsoft Outlook 2016\Security\Security Form Settings* with Use Outlook Security Group Policy selected, as set in this benchmark.

Default Value:

Enabled. (Outlook uses Unicode character encoding.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.4 Trust Center

This section contains settings for configuring Trust Center within Outlook.

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether Outlook also applies the macro security settings to 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.

Impact:

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.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:donttrustinstalledfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

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

Default Value:

Disabled. (Outlook does not use the macro security settings to determine whether to run macros, installed COM add-ins, and additional actions.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting hides the 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: 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 cached passwords. Cached passwords could then be used to compromise the user's email account(s) and other systems that use the same credentials.

Impact:

Users will have to enter their email account passwords for any email services that do not accept their Windows credentials.

Note: 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.

Note #2: For Exchange servers in **untrusted domains** and other types of email accounts, users might be forced to reenter their password frequently.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:enablerememberpwd
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Outlook 2016\Security\Disable 'Remember password' for Internet e-mail accounts
```

Default Value:

Disabled. (Passwords can be remembered.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.6 (L1) Ensure 'Do not automatically sign replies' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting specifies whether replies will be automatically (digitally) signed.

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

Rationale:

Disabling this setting and allowing automatic digital signatures will ensure the original sender of a signed message also receives a signed one in return. Breaking the integrity in this trust relationship may cause the other party to disregard the sender's message, causing information and trust to be lost.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:nosignonreply
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Do not automatically sign replies
```

Default Value:

Disabled. (A signed response will be the default reply to a signed message.)

References:

1. https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.14.7 (L1) Ensure 'Prompt user to choose security settings if default settings fail' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures whether users are prompted to choose Outlook security settings if the default settings fail to apply.

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

Rationale:

Allowing users to select their own security settings results in inconsistent enforcement in the organization and the likelihood of non-secure settings being applied.

Impact:

Enabling this setting will prevent a prompt from appearing when the default security settings fail and users will not be able to choose security settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\outlook\security:forcedefaultprofile
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft Outlook 2016\Security\Prompt user to choose security settings if default settings fail
```

Default Value:

Not Configured.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6 Microsoft PowerPoint 2016

This section includes recommendations for Microsoft PowerPoint.

This Group Policy section is provided by the Group Policy template `ppt16.admx/adml` that is available from Microsoft using the link from the overview section of this document.

2.6.1 Collaboration Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.2 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.4 File Tab

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.5 Miscellaneous

This section contains Miscellaneous settings.

2.6.5.1 Server Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.5.2 (L2) Ensure 'Disable Slide Update' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting controls whether users can link slides in a presentation with their counterparts in a PowerPoint Slide Library.

PowerPoint users can share and reuse slide content by storing individual slide files in a centrally located Slide Library on a server running Office SharePoint Server. Using the Slide Update feature, users can associate a slide in a presentation on a user's computer with the original slide that resides in the Slide Library on the server.

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

Rationale:

Updating a slide in a presentation from an external source like a Slide Library can cause important information to be exposed or lost. An attacker could modify the data in the slide library, affecting the integrity of all slide presentations that depend upon that library.

Impact:

Enabling this setting prevents PowerPoint from checking Slide Libraries for slide updates.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\slide
libraries:disableslideupdate
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft PowerPoint 2016\Miscellaneous\Disable Slide Update
```

Default Value:

Disabled. (Slide updates are allowed.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.6.6 PowerPoint Options

2.6.6.1 Advanced

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.6.2 Customize Ribbon

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.6.3 General

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.6.4 Proofing

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.6.5 Save

This section contains Save settings.

*2.6.6.5.1 (L1) Ensure 'Default file format' is set to 'Enabled: PowerPoint Presentation (*pptx)' (Automated)*

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting governs the default format for new presentation files that users create.

The recommended state for this setting is: `Enabled: PowerPoint Presentation (*pptx).`

Rationale:

If a new PowerPoint file is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the PowerPoint format.

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new PowerPoint file, therefore it is unlikely to affect usability for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `27`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\options:defaultformat
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: PowerPoint Presentation (*pptx)`:

```
Microsoft PowerPoint 2016\PowerPoint Options\Save\Default file format
```

Default Value:

Disabled. (PowerPoint Presentation is the default option.)

Additional Information:

By default, when users create new PowerPoint files, PowerPoint saves them in the new *.pptx file format. Users can change this functionality by clicking the Office button, clicking PowerPoint Options, and then selecting a file format from the Default file format list.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6 Security

This sections contains settings for Security Options.

2.6.6.6.1 Cryptography

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.6.6.6.2 Trust Center

This section contains settings for Trust Center.

2.6.6.6.2.1 File Block Settings

This section contains File Block Settings.

2.6.6.6.2.1.1 (L1) Ensure 'PowerPoint 97-2003 presentations, shows, templates and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save PowerPoint files with PowerPoint 97-2003 presentations, shows, templates and add-in files.

Note: *Use Open Policy* action is defined by the *Set default file block behavior* group policy setting which is included in this benchmark.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

Using legacy file formats could allow malicious code to become active on user computers or the network.

Impact:

Users will not be able to open, save, or view files of the specified format.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\excel\powerpoint\security\fileblock:binaryfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\File Block Settings\PowerPoint 97-2003 presentations, shows, templates and add-in files
```

Default Value:

Disabled. (File type is not blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.1.2 (L1) Ensure 'Set default file block behavior' to 'Enabled: Blocked files are not opened' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if users can open, view, or edit Word files that are by default blocked by Microsoft Office.

The recommended state for this setting is: `Enabled: Blocked files are not opened`.

Rationale:

By default, users can open, view, or edit a large number of file types in Word. Some file types are safer than others, as some could allow malicious code to execute on a user computer or the network.

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in Word. Productivity could be affected if users who require access to any of these file types cannot access them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\Office\16.0\powerpoint\security\fileblock:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Blocked files are not opened`:

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\File Block Settings\Set Default File Block Behavior
```

Default Value:

Disabled. (The behavior is the same as the *Blocked files are not opened* setting. Users will not be able to open blocked files.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.2 Protected View

This section contains settings for Protected View options.

2.6.6.6.2.2.1 (L1) Ensure 'Do not open files from the Internet zone in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether files downloaded from the Internet zone open in Protected View.

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

Rationale:

Allowing users to download files from the Internet zone to open outside of Protected View could allow malicious code to become active on a user's computer or the network.

Impact:

When files open in Protected View, some functionality will be unavailable and productivity in your organization could be affected. When this is undesirable, users will have to add sites to their trusted sites list, thus allowing the files to be opened in normal view with all functionality available.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\protectedview:disableinternetfilesinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View\Do not open files from the Internet zone in Protected View
```

Default Value:

Disabled. (Files downloaded from the Internet zone open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.2.2 (L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if files located in unsafe locations will open in Protected View.

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

Rationale:

Opening files located in unsafe locations that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Note: If a specified unsafe location(s) is not configured, the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

Impact:

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to save locations in order to access them with full functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\protectedview:disableunsafelocationsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View\Do not open files in unsafe locations in Protected View
```

Default Value:

Disabled. (Files located in unsafe locations open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.2.3 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Enabled: Open in Protected View`.

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\filevalidation:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open in Protected View`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View\Set Document Behavior if File Validation Fails
```

Default Value:

Enabled: Open in Protected View (Checked allow edit)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.2.4 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Unchecked: Do not allow edit (False).`

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\filevalidation:disableeditfrompv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Unchecked: Do not allow edit (False).`

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View\Set Document Behavior if File Validation Fails
```

Default Value:

Enabled: Open in Protected View (Checked allow edit)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.2.5 (L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if PowerPoint files in Outlook attachments open in Protected View.

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

Rationale:

Opening files that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Impact:

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to save locations in order to access them with full functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\protectedview:disableattachmentsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Protected View\Turn off Protected View for attachments opened from Outlook
```

Default Value:

Disabled. (Outlook attachments open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.3 Trusted Locations

This section contains settings for Trusted Locations.

2.6.6.6.2.3.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether trusted locations on the network can be used. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe by the application opening the file.

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

Rationale:

Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. These custom locations added by users are ignored but not removed. Trusted locations added in Group Policy that specify a network location are also ignored.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\trusted
locations:allownetworklocations
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Trusted
Locations\Allow Trusted Locations on the network
```

Default Value:

Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.3.2 (L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications.

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

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

All trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2016 during setup, deployed to users using Group Policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\trusted
locations:alllocationsdisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Trusted
Locations\Disable all trusted locations
```

Default Value:

Disabled. (All trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.4 (L1) Ensure 'Block macros from running in Office files from the Internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Windows Attachment Execution Service places a marker in the file's alternate data stream to indicate it came from the Internet zone. If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Users will receive a notification that macros are blocked from running.

The exceptions when macros will be allowed to run are:

- The Office file is saved to a Trusted Location.
- The Office file was previously trusted by the user.
- Macros are digitally signed and the matching Trusted Publisher certificate is installed on the device.

The recommended state for this setting is: `Enabled`

Rationale:

Macros can contain malicious code or instructions that can compromise the system on which they are run. Blocking macros on files marked as originating from the internet ensures known, unknown, and obfuscated code are contained by this measure from being ran accidentally by the end user.

Impact:

As this measure is enforcing the default, there is little or no impact.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\policies\microsoft\office\16.0\powerpoint\security:blockcontentexecutionfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Block
macros from running in Office files from the Internet
```

Default Value:

Enabled. (Macros on files marked from the internet are blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.6.6.6.2.5 (L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether add-ins for this application must be digitally signed by a trusted publisher.

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

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Not configuring this setting may allow an application to load dangerous add-ins and as a result, malicious code could become active on endpoints or the network.

Impact:

This setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:requireaddinsig
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Require that application add-ins are aigned by Trusted Publisher
```

Default Value:

Disabled. (This application does not check the digital signature on application add-ins before opening them.)

Additional Information:

Office stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store, but does not write information to this store.

Therefore, if you created a list of trusted publishers in a previous version of Office and you upgrade to the Office release, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.6.6.6.2.6 (L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification.

Note: For this policy to apply, the *Require that application add-ins are signed by Trusted Publisher* policy setting needs to be enabled. This will prevent users from changing the *Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them* policy setting.

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

Rationale:

Allowing unsigned application add-ins could cause the application to load dangerous add-ins and as a result, malicious code could become active on endpoints and the network.

Impact:

If an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled, and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:notbpromptunsignedaddin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Require
that application add-ins are signed by Trusted Publisher\Disable Trust Bar
Notification for Unsigned Application Add-ins and Block Them
```

Default Value:

Disabled. (Users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.)

Additional Information:

This setting only applies if the Office application is configured to require that all add-ins are signed by a trusted publisher. By default, users can configure this requirement themselves in the Add-ins category of the Trust Center for the application. To enforce this requirement, you must enable the Require that application add-ins are signed by Trusted Publisher setting in Group Policy, which prevents users from changing the setting themselves.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.6.6.6.2.7 (L1) Ensure 'Trust Access to Visual Basic Project' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

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

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

Impact:

None - this is the default behavior.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:accessvbom
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\Trust Access to Visual Basic Project
```

Default Value:

Disabled. (Automation clients do not have programmatic access to VBA projects. Users can enable this by selecting the *Trust access to the VBA project object model* in the *Macro Settings* section of the Trust Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.2.8 (L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

The recommended state for this setting is: `Enabled: Disable all except digitally signed macros`.

Rationale:

By default, when a user opens a file that contains VBA macros, the macros are disabled, and a warning is displayed on the Trust Bar that the macro has been disabled. Users may then enable these macros by clicking options on the Trust Bar and selecting to enable the macro which could execute malicious code and cause a virus to load undetected.

Note: Microsoft Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Microsoft Office still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store.

Therefore, if a list of trusted publishers is created in a previous version of Microsoft Office and is upgraded, the trusted publisher list will still be recognized. However, any trusted publisher certificates that are added to the list will be stored in the trusted publisher store.

Impact:

This configuration causes documents and templates that contain unsigned macros to lose all functionality supplied by the macro. To prevent this loss of functionality, users can install the macro in a trusted location, unless the *Disable all trusted locations* setting is configured to `Enabled`, which will not allow the user to add to the trusted location.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:vbawarnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable all except digitally signed macros`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Trust Center\VBA Macro
Notification Settings
```

Default Value:

Enabled: Disable all with notification (Trust Bar displays warning but users can Enable Content regardless of macro signatures.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.3 (L1) Ensure 'Make hidden markup visible' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether hidden markup is visible when users open PowerPoint files in standard or HTML format.

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

Rationale:

If a file is saved with hidden markup, users might inadvertently distribute sensitive comments or information outside of their trusted circle without realizing that this information is still present in the document.

Impact:

In most cases, markup is intended to be visible to users. Markup does not display in presentation mode in PowerPoint, even if it is visible in design mode, so it is likely that this setting will have a minimal impact on usability.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\options:markupopensave
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Make hidden markup visible
```

Default Value:

Enabled

Additional Information:

PowerPoint presentations that are saved in standard or HTML format can contain a flag indicating whether markup (comments or ink annotations) in the presentation should be visible when the presentation is open. By default, PowerPoint ignores this flag when opening a file, and always displays any markup present in the file. In addition, when saving a file, PowerPoint sets the flag to display markup when the presentation is next opened.

If this default configuration is changed, PowerPoint sets the flag according to the state of the Show Markup option on the Review tab of the Ribbon when it saves presentations in standard or HTML format. In addition, PowerPoint enables or disables the Show Markup option according to the way the flag is set when it opens files, which means that a presentation saved with hidden markup is opened with the markup still hidden.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.4 (L1) Ensure 'Run Programs' is set to 'Enabled: disable (don't run any programs)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the prompting and activation behavior for the *Run Programs* option for action buttons in PowerPoint.

By choosing the `Disable (don't run any programs)` option, if users click an action button with the *Run Programs* action assigned to it, nothing will happen.

The recommended state for this setting is: `Enabled: Disable (don't run any programs)`

Rationale:

Action buttons can be used to launch external programs from PowerPoint presentations. If a malicious user adds an action button to a presentation that launches a dangerous program, it could affect the security of a user's computer and data.

Impact:

Users who wish to create or use presentations that launch external programs when action buttons are clicked will not be able to do so. These users will have to launch any external programs manually at the appropriate times when delivering presentations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:runprograms
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: disable (don't run any programs).`

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Run Programs
```

Default Value:

Disabled. (If users click an action with the "Run Programs" action assigned to it, nothing will happen. This behavior is the same as Enabled -- Disable (don't run any programs).)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.6.6.6.5 (L1) Ensure 'Scan encrypted macros in PowerPoint Open XML presentations' is set to 'Enabled: Scan encrypted macros' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether encrypted macros in Open XML documents are required to be scanned with antivirus software before being opened.

The recommended state for this setting is: `Enabled: Scan encrypted macros`.

Rationale:

When an Office Open XML document is rights-managed or password protected, macros that are embedded in the document are encrypted along with the rest of the workbook's contents. Macros can contain malicious code which could cause a virus to load undetected and lead to data loss or reduced application functionality.

Impact:

None - this is the default behavior.

By default, encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:powerpointbypassencryptedmacroscan
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Scan encrypted macros`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Scan encrypted macros in PowerPoint Open XML presentations
```

Default Value:

Enabled. (Encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

2.6.6.6.6 (L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the file validation feature. Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

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

Rationale:

The file validation feature ensures that Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security\filevalidation:enableonload
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Turn off file validation
```

Default Value:

Disabled. (File validation feature is on.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

2.6.6.6.7 (L1) Ensure 'Unblock automatic download of linked images' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether PowerPoint automatically downloads links from external sources.

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

Rationale:

When users insert images into PowerPoint presentations, they can select *Link to File* instead of *Insert*. If a user selects *Link to File*, the image is represented by a link to a file on disk instead of being embedded in the presentation file itself.

By default, when PowerPoint opens a presentation, it does not display any linked images saved on a different computer unless the presentation itself is saved in a trusted location (as configured in the Trust Center). If this configuration is changed, PowerPoint will load any images that were saved in remote locations, which presents a security risk.

Impact:

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

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security:downloadimages
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`:

```
Microsoft PowerPoint 2016\PowerPoint Options\Security\Unblock automatic
download of linked images
```

Default Value:

Disabled. (When PowerPoint opens a presentation, it does not display any linked images saved on a different computer unless the presentation itself is saved in a trusted location (as configured in the Trust Center).)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.7 Microsoft Project 2016

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.8 Microsoft Publisher 2016

This section includes recommendations for Microsoft Publisher.

This Group Policy section is provided by the Group Policy template `pub16.admx/adml` that is available from Microsoft using the link from the overview section of this document.

2.8.1 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.8.2 Miscellaneous

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.8.3 Publisher Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.8.4 Security

This section contains security related recommendations for Publisher.

2.8.4.1 Trust Center

This section contains recommendations for the Trust Center of Microsoft Publisher.

2.8.4.1.1 (L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows the blocking of macros from running in Office files that come from the internet.

By enabling this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Users will receive a notification that macros are blocked from running.

The exceptions when macros will be allowed to run are:

- The Office file is saved to a Trusted Location.
- The Office file was previously trusted by the user.
- Macros are digitally signed and the matching Trusted Publisher certificate is installed on the device.

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

Rationale:

Windows will mark files downloaded from the internet within an alternative NTFS data stream on the file. Files from untrusted sources can contain malicious payloads embedded in the Macros, including fileless malware, and should be handled with extra care by utilizing additional security controls.

Impact:

This enforces the default behavior and should not cause additional impact.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\publisher\security:blockcontentexecutionfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`:

```
Microsoft Publisher 2016\Security\Trust Center\Block macros from running in Office files from the internet
```

Default Value:

Enabled. (Macros are blocked)

References:

1. https://learn.microsoft.com/en-us/DeployOffice/security/internet-macros-blocked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.9 Implement Application Whitelisting of Scripts The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			●

2.8.4.1.2 (L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether add-ins for the specified Office applications must be digitally signed by a trusted publisher.

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

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Not configuring this setting may allow an application to load a dangerous add-in and as a result, malicious code could become active on a user's computer or the network.

Impact:

This setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store but does not write information to this store.

If a list of trusted publishers in a previous version of Office was created and the Office release is upgraded, the trusted publisher list will still be recognized. However, any trusted publisher certificates that were added to the list will be stored in the Internet Explorer trusted publisher store.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\publisher\security:requireaddinsig
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Publisher 2016\Security\Trust Center\Require that application add-ins are signed by Trusted Publisher
```

Default Value:

Disabled. (This application does not check the digital signature on application add-ins before opening them. If a dangerous add-in is loaded, it could harm users' computers or compromise data security.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.8.4.1.3 (L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disables such add-ins without notification.

Note: For this policy to apply, the *Require that application add-ins are signed by Trusted Publisher* policy setting needs to be enabled. This will prevent users from changing the *Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them* policy setting.

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

Rationale:

Allowing unsigned application add-ins could cause the application to load dangerous add-ins and as a result, malicious code could become active endpoints and the network.

Impact:

If an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\publisher\security:notbpromptunsignedaddin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Publisher 2016\Security\Trust Center\Require that application add-ins are signed by Trusted Publisher\Disable Trust Bar Notification for unsigned application add-ins and block them
```

Default Value:

Disabled. (Users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.8.4.1.4 (L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

The recommended state for this setting is: `Enabled: Disable all except digitally signed macros`.

Rationale:

By default, when a user opens a file that contains VBA macros, the macros are disabled, and a warning is displayed on the Trust Bar that the macro has been disabled. Users may then enable these macros by clicking options on the Trust Bar and selecting to enable the macro which could execute malicious code and cause a virus to load undetected.

Note: Microsoft Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Microsoft Office still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store.

Therefore, if a list of trusted publishers is created in a previous version of Microsoft Office and is upgraded, the trusted publisher list will still be recognized. However, any trusted publisher certificates that are added to the list will be stored in the trusted publisher store.

Impact:

This configuration causes documents and templates that contain unsigned macros to lose all functionality supplied by the macro. To prevent this loss of functionality, users can install the macro in a trusted location, unless the *Disable all trusted locations* setting is configured to `Enabled`, which will not allow the user to add to the trusted location.

Warning: With the `Disable all except digitally signed macros` option selected, users will not be able to open unsigned Access databases.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\publisher\security:vbawarnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable all except digitally signed macros`.

```
Microsoft Publisher 2016\Security\Trust Center\VBA Macro Notification Settings
```

Default Value:

Enabled: Disable all with notification (Trust Bar displays warning but users can Enable Content regardless of macro signatures.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.8.4.2 (L1) Ensure 'Publisher Automation Security Level' is set to 'Enabled: By UI (prompted)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether macros opened programmatically by another application can run in Publisher and how those macros will run.

The recommended state for this setting is: `By UI (prompted)`.

Note: With the above macro functionality configuration selected, macro behavior will be determined by the setting *VBA Macro Notification Settings* in the Trust Center.

Rationale:

Users may enable macros which could execute malicious code and cause a virus to load undetected.

Impact:

This configuration causes documents and templates that contain unsigned macros to lose all functionality supplied by the macro. To prevent this loss of functionality, users can install the macro in a trusted location, unless the *Disable all trusted locations* setting is configured to *Enabled*, which will not allow the user to add to the trusted location.

Warning: With the *Disable all except digitally signed macros* option selected, users will not be able to open unsigned Access databases.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\common\security:automationsecuritypublisher
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: By UI (prompted)`:

```
Microsoft Publisher 2016\Security\Publisher Automation Security Level
```

Default Value:

Disabled. (Publisher will use the default Macro setting in Trust Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.9 Microsoft Teams

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.10 Microsoft Visio 2016

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11 Microsoft Word 2016

This section includes recommendations for Microsoft Word.

This Group Policy section is provided by the Group Policy template `word16.admx/adml` that is available from Microsoft using the link from the overview section of this document.

2.11.1 Collaboration Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.2 Customizable Error Messages

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.3 Disable Items in User Interface

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.4 File Tab

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.5 Japanese Find

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.6 Miscellaneous

This section contains settings to configure Miscellaneous settings within Word

2.11.6.1 Server Settings

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.6.2 (L2) Ensure 'Use online translation dictionaries' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting determines if online dictionaries are used for the translation of text through the Research pane.

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

Rationale:

Data should not be shared with third party vendors in an enterprise managed environment. Enabling this service could potentially allow sensitive information to be sent to a third party for translation.

Impact:

Users will not be able to translate text through the Research pane by using the online dictionaries.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\common\research\translation:useonline
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Miscellaneous\Use online translation dictionaries
```

Default Value:

Enabled. (The online dictionaries can be used to translate text through the Research pane.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.11.7 Review Tab

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8 Word Options

This section contains settings to configure Word options.

2.11.8.1 Advanced

This section contains settings to configure Advance Word options.

2.11.8.1.1 E-Mail Options

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8.1.2 (L1) Ensure 'Update automatic links at Open' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting configures the check/uncheck box in the corresponding UI option for updating automatic links when a document is opened.

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

Rationale:

When a user opens a document, Word automatically updates any links to external content, such as graphics, Excel worksheets, and PowerPoint slides. If Word is configured to automatically update links when documents are open, document content can change without the user's knowledge or introduce unsafe links.

Impact:

Users who work with Word documents that contain external content will not be able to automatically update that content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\options:dontupdatelinks
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Advanced\Update automatic links at Open
```

Default Value:

Not Configured.

Additional Information:

To disable automatic updating, the user can click the Office Button, click Word Options, click Advanced, scroll to the General section, and then clear the Update automatic links at open check box.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.2 Customized Ribbon

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8.3 Display

This section contains settings to configure Word Display Settings

2.11.8.3.1 (L1) Ensure 'Hidden text' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether text that is formatted as hidden displays in Microsoft Word.

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

Rationale:

By default, Word does not display text formatted as hidden unless Show/Hide ¶ is selected or Word is configured to show hidden text in the Display section of the Word Options dialog box. If a document that contains hidden text is distributed, sensitive information in the document could be at risk.

Impact:

Displaying hidden text can change the way a document flows as well as make it difficult to judge the number of pages in a document where Word will insert automatic page breaks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\options:showhiddentext
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Display\Hidden text
```

Default Value:

Disabled. (Word does not display text formatted as hidden unless "Show/Hide ¶" is selected or Word is configured to show hidden text in the "Display" section of the "Word Options" dialog.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.4 General

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8.5 Proofing

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8.6 Save

This section contains Word save options.

2.11.8.6.1 (L1) Ensure 'Default file format' is set to 'Enabled: Word Document (.docx)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines the default file format for saving files in Word.

Note: This policy setting is often set in combination with the *Save As Open XML in Compatibility Mode* policy setting.

The recommended state for this setting is: `Enabled: Word Document (.docx).`

Rationale:

If a new Word file is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the default format.

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new Word file, therefore it is unlikely to affect usability for most users.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `null`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\options:defaultformat
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Word Document (.docx).`

```
Microsoft Word 2016\Word Options\Save\Default file format
```

Default Value:

Disabled. (Word defaults to save new files in the Office Open XML forma .docx)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7 Security

This section contains settings to configure Security Options.

2.11.8.7.1 Cryptography

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

2.11.8.7.2 Trust Center

This section contains settings to configure Trust Center within Word.

2.11.8.7.2.1 File Block Settings

This Section contains settings for configuring File Block settings.

2.11.8.7.2.1.1 (L1) Ensure 'Set default file block behavior' is set to 'Enabled: Blocked files are not opened' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if users can open, view, or edit Word files that are by default blocked by Microsoft Office.

The recommended state for this setting is: `Enabled: Blocked files are not opened`.

Rationale:

By default, users can open, view, or edit a large number of file types in Word. Some file types are safer than others, as some could allow malicious code to execute on a user computer or the network.

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in Word. Productivity could be affected if users who require access to any of these file types cannot access them.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Blocked files are not opened`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Set Default File Block Behavior
```

Default Value:

Disabled. (The behavior is the same as the *Blocked files are not opened* setting. Users will not be able to open blocked files.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.2 (L1) Ensure 'Word 2 and earlier binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 2 and earlier binary documents and templates.

By choosing the `Open/Save blocked, use open policy`, both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the *default file block behavior* key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 2 and earlier binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word2files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 2 and Earlier Binary Documents and Templates
```

Default Value:

Disabled. (The file type will be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.3 (L1) Ensure 'Word 2000 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 2000 binary documents and templates.

By choosing the `Open/Save blocked, use open policy` both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 2000 binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word2000 files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 2000 binary documents and templates
```

Default Value:

Disabled. (The file type will not be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.4 (L1) Ensure 'Word 2003 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 2003 binary documents and templates.

By choosing the `Open/Save blocked, use open policy` both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 2003 binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word2003 files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 2003 binary documents and templates
```

Default Value:

Disabled. (The file type will not be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.5 (L1) Ensure 'Word 2007 and later binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 2007 and later binary documents and templates.

By choosing the `Open/Save blocked, use open policy` both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 2007 and later binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word2007 files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 2007 and later binary documents and templates
```

Default Value:

Disabled. (The file type will not be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.6 (L1) Ensure 'Word 6.0 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 6.0 binary documents and templates.

By choosing the `Open/Save blocked, use open policy`, both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 6.0 binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word60files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 6.0 Binary Documents and Templates
```

Default Value:

Disabled. (The file type will be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.7 (L1) Ensure 'Word 95 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 95 binary documents and templates.

By choosing the `Open/Save blocked, use open policy`, both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 95 binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word95files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 95 Binary Documents and Templates
```

Default Value:

Disabled. (The file type will be blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.8 (L1) Ensure 'Word 97 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word 97 binary documents and templates.

By choosing the `Open/Save blocked, use open policy` both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word 97 binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:word97files
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word 97 Binary Documents and Templates
```

Default Value:

Disabled. (The file type will not be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.1.9 (L1) Ensure 'Word XP binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether users can open, view, edit, or save Word XP binary documents and templates.

By choosing the `Open/Save blocked, use open policy` both the opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.

The recommended state for this setting is: `Enabled: Open/Save blocked, use open policy`.

Rationale:

By default, users can open, view, or edit this type of document in Word. This could allow malicious code to become active on a user computer or the network.

Impact:

Word XP binary documents and templates will not open in Microsoft Word.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `2`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\fileblock:wordxpfiles
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open/Save blocked, use open policy`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\File Block Settings\Word XP binary documents and templates
```

Default Value:

Disabled. (The file type will not be blocked.)

References:

1. http://technet.microsoft.com/en-us/library/cc179230.aspx

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.2 Protected View

This section contains settings to configure Protected view options.

2.11.8.7.2.2.1 (L1) Ensure 'Do not open files from the internet zone in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines whether files downloaded from the Internet zone open in Protected View.

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

Rationale:

Allowing users to download files from the Internet zone to open outside of Protected View could allow malicious code to become active on a user's computer or the network.

Impact:

When files open in Protected View, some functionality will be unavailable. Users will be unable to edit the file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\protectedview:disableinternetfilesinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Protected View\Do Not Open Files From The Internet Zone in Protected View
```

Default Value:

Disabled. (Files downloaded from the Internet zone open in Protected View.)

References:

1. https://support.microsoft.com/en-us/office/what-is-protected-view-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.2.2 (L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if files located in unsafe locations will open in Protected View.

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

Rationale:

Opening files located in unsafe locations that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Note: If a specified unsafe location(s) is not configured, the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

Impact:

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to safe locations in order to access them with full functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\protectedview:disa
bleunsafelocationsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Protected View\Do Not
Open Files in Unsafe Locations in Protected View
```

Default Value:

Disabled. (Files located in unsafe locations open in Protected View.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.2.3 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Enabled: Open in Protected View`.

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\filevalidation:openinprotectedview
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Open in Protected View`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Protected View\Document Behavior if File Validation Fails
```

Default Value:

Enabled. (Open in Protected View (Unchecked).)

Additional Information:

If this policy setting is disabled, Office follows the "Open files in Protected View and disallow edit" behavior.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.2.4 (L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit` (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how Office handles documents when they fail file validation.

Office File Validation is a feature that performs security checks on files. If Office File Validation detects a problem with a file, the file cannot be opened.

The recommended state for this setting is: `Unchecked: Do not allow edit (false).`

Rationale:

Files that have failed file validation outside of Protected View could allow malicious code to execute on the system or the network.

Impact:

Files that are blocked by the validation fail rule will not open on a user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\filevalidation:dis
ableeditfrompv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Unchecked: Do not allow edit (false).`

```
Microsoft Word 2016\Word Options\Security\Trust Center\Protected
View\Document Behavior if File Validation Fails
```

Default Value:

Enabled. (Open in Protected View (Unchecked).)

Additional Information:

If this policy setting is disabled, Office follows the "Open files in Protected View and disallow edit" behavior.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.2.5 (L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting determines if Word files in Outlook attachments open in Protected View.

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

Rationale:

Opening files that do not require Protected View could lead to malicious code executing on a user's computer or the network.

Impact:

Some functionality is not available when files are opened in Protected View. Users will be unable to edit documents.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\protectedview:disableattachmentsinpv
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Protected View\Turn Off Protected View for Attachments Opened From Outlook
```

Default Value:

Disabled. (Outlook attachments open in Protected View.)

References:

1. https://support.microsoft.com/en-us/office/what-is-protected-view-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653
2. https://learn.microsoft.com/en-us/outlook/troubleshoot/security/office-document-attachments-open-in-protected-view

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.3 Trusted Locations

This section contains settings to configure Trusted Locations.

2.11.8.7.2.3.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether trusted locations on the network can be used. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe by the application opening the file.

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

Rationale:

Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. These custom locations added by users are ignored but not removed. Trusted locations added in Group Policy that specify a network location are also ignored.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\trusted
locations:allownetworklocations
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Trusted
Locations\Allow Trusted Locations on the Network
```

Default Value:

Enabled. (Users can specify trusted locations.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.3.2 (L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications.

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

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Impact:

All trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2016 during setup, deployed to users using Group Policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\trusted
locations:alllocationsdisabled
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Trusted
Locations\Disable All Trusted Locations
```

Default Value:

Disabled. (All trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.4 (L1) Ensure 'Block macros from running in Office files from the Internet' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Windows Attachment Execution Service places a marker in the file's alternate data stream to indicate it came from the Internet zone. If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Users will receive a notification that macros are blocked from running.

The exceptions when macros will be allowed to run are:

- The Office file is saved to a Trusted Location.
- The Office file was previously trusted by the user.
- Macros are digitally signed and the matching Trusted Publisher certificate is installed on the device.

The recommended state for this setting is: `Enabled`

Rationale:

Macros can contain malicious code or instructions that can compromise the system on which they are run. Blocking macros on files marked as originating from the internet ensures known, unknown, and obfuscated code is contained by this measure from being ran accidentally by the end user.

Impact:

As this measure is enforcing the default, there is little or no impact.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\policies\microsoft\office\16.0\word\security:blockcontentexecutionfrominternet
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Block macros from
running in Office files from the Internet
```

Default Value:

Enabled. (Macros on files marked from the internet are blocked.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.11.8.7.2.5 (L1) Ensure 'Dynamic Data Exchange' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls the ability to use Dynamic Data Exchange (DDE) in Word.

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

Rationale:

In an email attack scenario, an attacker could leverage the DDE protocol by sending a specially crafted file to the user and then convincing the user to open the file, typically by way of an enticement in an email. The attacker would have to convince the user to disable Protected Mode and click through one or more additional prompts. Email attachments are a primary method an attacker could use to spread malware.

For more information, see Microsoft Security Advisory 4053440 link in the references of this recommendation.

Impact:

None - DDE is disabled by default in Word. Enforcing this policy ensures users cannot enter an unsecure state.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting will have **no registry value** (the key will not exist) if it is set to `Disabled`:

```
HKEY_USERS\[USER SID]\SOFTWARE\policies\microsoft\office\16.0\word\security:allowdde
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Dynamic Data Exchange
```

Default Value:

Disabled. (DDE is Disabled.)

References:

1. https://learn.microsoft.com/en-us/windows/win32/dataxchg/about-dynamic-data-exchange
2. https://learn.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

2.11.8.7.2.6 (L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether add-ins for the specified Office applications must be digitally signed by a trusted publisher.

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

Rationale:

By default, Office applications do not check the digital signature on application add-ins before opening them. Not configuring this setting may allow an application to load a dangerous add-in and as a result, malicious code could become active on a user's computer or the network.

Impact:

This setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office still reads trusted publisher certificate information from the Office trusted publisher store but does not write information to this store.

If a list of trusted publishers in a previous version of Office was created and the Office release was upgraded, the trusted publisher list will still be recognized. However, any trusted publisher certificates that were added to the list will be stored in the Internet Explorer trusted publisher store.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security:requireaddinsig
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Require that
application add-ins are signed by Trusted Publisher
```

Default Value:

Disabled. (This application does not check the digital signature on application add-ins before opening them. If a dangerous add-in is loaded, it could harm users' computers or compromise data security.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.11.8.7.2.7 (L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disables such add-ins without notification.

Note: For this policy to apply, the *Require that application add-ins are signed by Trusted Publisher* policy setting needs to be enabled. This will prevent users from changing the *Disable Trust Bar Notification for unsigned application add-ins and block them* policy setting.

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

Rationale:

Allowing unsigned application add-ins could cause the application to load dangerous add-ins and as a result, malicious code could become active on endpoints and the network.

Impact:

If an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security:notbpromptunsignedaddin
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Require that
application add-ins are signed by Trusted Publisher\Disable Trust Bar
Notification for unsigned application add-ins and block them
```

Default Value:

Disabled. (Users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.11.8.7.2.8 (L1) Ensure 'Scan encrypted macros in Word Open XML Documents' to 'Enabled: Scan encrypted macros (default)' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether encrypted macros in Open XML documents are required to be scanned with antivirus software before being opened.

The recommended state for this setting is: `Enabled: Scan encrypted macros (default).`

Rationale:

When an Office Open XML document is rights-managed or password protected, macros that are embedded in the document are encrypted along with the rest of the workbook's contents. Macros can contain malicious code which could cause a virus to load undetected and lead to data loss or reduced application functionality.

Impact:

None - this is the default behavior.

By default, encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security:wordbypassencrypteddmacroscan
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Scan encrypted macros (default).`

```
Microsoft Word 2016\Word Options\Security\Trust Center\Scan encrypted macros in Word Open XML Documents
```

Default Value:

Enabled: Scan encrypted macros

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

2.11.8.7.2.9 (L1) Ensure 'Trust access to Visual Basic Project' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

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

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

Impact:

None - this is the default behavior.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `0`.

```
HKEY_USERS\[USER
SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security:accessvbom
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\Trust access to Visual Basic Project
```

Default Value:

Disabled. (Automation clients do not have programmatic access to VBA projects. Users can enable this by selecting the *Trust access to the VBA project object model* in the *Macro Settings* section of the Trust Center.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.2.10 (L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

The recommended state for this setting is: `Enabled: Disable all except digitally signed macros`.

Rationale:

By default, when a user opens a file that contains VBA macros, the macros are disabled, and a warning is displayed on the Trust Bar that the macro has been disabled. Users may then enable these macros by clicking options on the Trust Bar and selecting to enable the macro which could execute malicious code and cause a virus to load undetected.

Note: Microsoft Office stores certificates for trusted publishers in the trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Microsoft Office still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store.

Therefore, if a list of trusted publishers is created in a previous version of Microsoft Office and is upgraded, the trusted publisher list will still be recognized. However, any trusted publisher certificates that are added to the list will be stored in the trusted publisher store.

Impact:

This configuration causes documents and templates that contain unsigned macros to lose all functionality supplied by the macro. To prevent this loss of functionality, users can install the macro in a trusted location, unless the *Disable all trusted locations* setting is configured to `Enabled`, which will not allow the user to add to the trusted location.

Warning: With the `Disable all except digitally signed macros` option selected, users will not be able to open unsigned Access databases.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `3`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security:vbawarnings
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled: Disable all except digitally signed macros`.

```
Microsoft Word 2016\Word Options\Security\Trust Center\VBA Macro Notification Settings
```

Default Value:

Enabled: Disable all with notification (Trust Bar displays warning but users can Enable Content regardless of macro signatures.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

2.11.8.7.3 (L1) Ensure 'Make hidden markup visible' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting controls whether hidden markup is visible when users open Word documents in standard or HTML format.

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

Rationale:

If a file is saved with hidden markup, users might inadvertently distribute sensitive comments or information outside of their trusted circle without realizing that this information is still present in the document.

Impact:

In most cases, markup is intended to be visible to users. Markup does not display in presentation mode in Word, even if it is visible in design mode, so it is likely that this setting will have a minimal impact on usability.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\options:showmarkupopensave
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Enabled`.

```
Microsoft Word 2016\Word Options\Security\Make hidden markup visible
```

Default Value:

Not Configured.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.11.8.7.4 (L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting allows you to turn off the file validation feature. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

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

Rationale:

The file validation feature ensures that Office Binary Documents are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Impact:

None - this is the default behavior.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This setting is backed by the following registry location with a value of `1`.

```
HKEY_USERS\[USER SID]\SOFTWARE\Policies\Microsoft\office\16.0\word\security\filevalidation:enableonload
```

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled`.

```
Microsoft Word 2016\Word Options\Security\Turn off file validation
```

Default Value:

Disabled. (File validation will be turned on.)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

2.12 Skype for Business 2016

This section is intentionally blank and exists to ensure the structure of the Microsoft Office benchmark is consistent.

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Computer Configuration**		
1.1	**Administrative Templates**		
1.1.1	**MS Security Guide**		
1.1.1.1	(L1) Ensure 'Block Flash activation in Office documents' is set to 'Enabled: Block all activation' (Automated)	☐	☐
1.1.1.2	(L1) Ensure 'Restrict legacy JScript execution for Office' is set to 'Enabled' (Automated)	☐	☐
1.2	**Microsoft Office 2016 (Machine)**		
1.2.1	**Customize**		
1.2.2	**Global Options**		
1.2.3	**Licensing Settings**		
1.2.4	**Miscellaneous**		
1.2.5	**Security Settings**		
1.2.5.1	**IE Security**		
1.2.5.1.1	(L1) Ensure 'Add-on Management' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.2	(L1) Ensure 'Bind to object' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.3	(L1) Ensure 'Consistent Mime Handling' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.4	(L1) Ensure 'Disable user name and password' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.2.5.1.5	(L1) Ensure 'Information Bar' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.6	(L1) Ensure 'Local Machine Zone Lockdown Security' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.7	(L1) Ensure 'Mime Sniffing Safety Feature' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.8	(L1) Ensure 'Navigate URL' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.9	(L1) Ensure 'Object Caching Protection' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.10	(L1) Ensure 'Protection From Zone Elevation' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.11	(L1) Ensure 'Restrict ActiveX Install' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.12	(L1) Ensure 'Restrict File Download' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.13	(L1) Ensure 'Saved from URL' is set to 'Enabled' (Automated)	☐	☐
1.2.5.1.14	(L1) Ensure 'Scripted Window Security Restrictions' is set to 'Enabled' (Automated)	☐	☐
1.2.6	**Updates**		
1.2.6.1	(L1) Ensure 'Enable Automatic Updates' is set to 'Enabled' (Automated)	☐	☐
1.2.6.2	(L1) Ensure 'Hide option to enable or disable updates' is set to 'Enabled' (Automated)	☐	☐
2	**User Configuration**		
2.1	**Microsoft Access 2016**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.1	**Application Settings**		
2.1.1.1	**General**		
2.1.1.2	**International**		
2.1.1.3	**Security**		
2.1.1.3.1	**Cryptography**		
2.1.1.3.2	**Trust Center**		
2.1.1.3.2.1	**Trusted Locations**		
2.1.1.3.2.1.1	(L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)	☐	☐
2.1.1.3.2.1.2	(L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)	☐	☐
2.1.1.3.2.2	(L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)	☐	☐
2.1.1.3.2.3	(L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)	☐	☐
2.1.1.3.2.4	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)	☐	☐
2.1.1.4	**Web Options...**		
2.1.1.4.1	**General**		
2.1.1.4.1.1	(L1) Ensure 'Underline hyperlinks' is set to 'Enabled' (Automated)	☐	☐
2.1.2	**Customizable Error Messages**		
2.1.3	**Disable Items in User Interface**		
2.1.4	**Miscellaneous**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.4.1	(L1) Ensure 'Default file format' is set to 'Enabled: Access 2007' (Automated)	☐	☐
2.1.4.2	(L1) Ensure 'Do not prompt to convert older databases' is set to 'Disabled' (Automated)	☐	☐
2.1.5	**Tools | Security**		
2.1.5.1	(L1) Ensure 'Modal Trust Decision Only' is set to 'Disabled' (Automated)	☐	☐
2.2	**Microsoft Excel 2016**		
2.2.1	**Customizable Error Messages**		
2.2.2	**Data Recovery**		
2.2.2.1	(L1) Ensure 'Do not show data extraction options when opening corrupt workbooks' is set to 'Enabled' (Automated)	☐	☐
2.2.3	**Disable Items in User Interface**		
2.2.4	**Excel Options**		
2.2.4.1	**Advanced**		
2.2.4.1.1	**General**		
2.2.4.1.1.1	(L1) Ensure 'Load Pictures from Web pages not created in Excel' is set to 'Disabled' (Automated)	☐	☐
2.2.4.1.2	(L1) Ensure 'Ask to update automatic links' is set to 'Enabled' (Automated)	☐	☐
2.2.4.2	**Autocorrect Options**		
2.2.4.2.1	(L1) Ensure 'Internet and network paths as hyperlinks' is set to 'Disabled' (Automated)	☐	☐
2.2.4.3	**Customize Ribbon**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4.4	**Formulas**		
2.2.4.5	**General**		
2.2.4.6	**Save**		
2.2.4.6.1	(L1) Ensure 'Default file format' is set to 'Enabled: Excel Workbook (*.xlsx)' (Automated)	☐	☐
2.2.4.6.2	(L1) Ensure 'Disable AutoRepublish' is set to 'Enabled' (Automated)	☐	☐
2.2.4.6.3	(L1) Ensure 'Do not show AutoRepublish warning alert' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7	**Security**		
2.2.4.7.1	**Cryptography**		
2.2.4.7.2	**Trust Center**		
2.2.4.7.2.1	**External Content**		
2.2.4.7.2.1.1	(L1) Ensure 'Always prevent untrusted Microsoft Query files from opening' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.1.2	(L1) Ensure 'Don’t allow Dynamic Data Exchange (DDE) server launch in Excel' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.1.3	(L1) Ensure 'Don’t allow Dynamic Data Exchange (DDE) server lookup in Excel' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.2	**File Block Settings**		
2.2.4.7.2.2.1	(L1) Ensure 'dBase III /IV files' is set to 'Enable: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.2	(L1) Ensure 'Dif and Sylk files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4.7.2.2.3	(L1) Ensure 'Excel 2 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.4	(L1) Ensure 'Excel 2 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.5	(L1) Ensure 'Excel 3 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.6	(L1) Ensure 'Excel 3 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.7	(L1) Ensure 'Excel 4 macrosheets and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.8	(L1) Ensure 'Excel 4 workbooks' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.9	(L1) Ensure 'Excel 4 worksheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.2.4.7.2.2.10	(L1) Ensure 'Excel 95 workbooks' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)	☐	☐
2.2.4.7.2.2.11	(L1) Ensure 'Excel 95-97 workbooks and templates' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)	☐	☐
2.2.4.7.2.2.12	(L1) Ensure 'Excel 97-2003 workbooks and templates' is set to 'Enabled: Open/Save Blocked, Use Open Policy' (Automated)	☐	☐
2.2.4.7.2.2.13	(L1) Ensure 'Set default file block behavior' is set to 'Enabled: Blocked files are not opened' (Automated)	☐	☐
2.2.4.7.2.2.14	(L1) Ensure 'Web pages and Excel 2003 XML spreadsheets' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4.7.2.3	**Protected View**		
2.2.4.7.2.3.1	(L1) Ensure 'Always open untrusted database files in Protected View' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.3.2	(L1) Ensure 'Do not open files from the internet zone in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.2.3.3	(L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.2.3.4	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)	☐	☐
2.2.4.7.2.3.5	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit' (Automated)	☐	☐
2.2.4.7.2.3.6	(L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.2.4	**Trusted Locations**		
2.2.4.7.2.4.1	(L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.2.4.2	(L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.5	(L1) Ensure 'Block Excel XLL Add-ins that come from an untrusted source' is set to 'Enabled: Blocked' (Automated)	☐	☐
2.2.4.7.2.6	(L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.7	(L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)	☐	☐
2.2.4.7.2.8	(L1) Ensure 'Prevent Excel from running XLM macros' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4.7.2.9	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.10	(L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.11	(L1) Ensure 'Store macro in Personal Macro Workbook by default' is set to 'Enabled' (Automated)	☐	☐
2.2.4.7.2.12	(L1) Ensure 'Trust access to Visual Basic Project' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.3	(L1) Ensure 'Force file extension to match file type' is set to 'Enabled: Always match file type' (Automated)	☐	☐
2.2.4.7.4	(L1) Ensure 'Scan encrypted macros in Excel Open XML workbooks' is set to 'Enabled: Scan encrypted macros (default)' (Automated)	☐	☐
2.2.4.7.5	(L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)	☐	☐
2.2.4.7.6	(L1) Ensure 'WEBSERVICE Function Notification Settings' is set to 'Enabled: Disable all without notification' (Automated)	☐	☐
2.3	**Microsoft Office 2016**		
2.3.1	**AutoSave**		
2.3.2	**Business Data**		
2.3.3	**Collaboration Settings**		
2.3.4	**Contact Card**		
2.3.5	**Customizable Error Messages**		
2.3.6	**Customize**		
2.3.6.1	**Shared Workspace**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.6.2	(L1) Ensure 'Disable UI extending from documents and templates' is set to 'Enabled' (Automated)	☐	☐
2.3.7	**Disable Items in User Interface**		
2.3.8	**DLP**		
2.3.9	**Document Information Panel**		
2.3.9.1	(L1) Ensure 'Document Information Panel Beaconing UI' is set to 'Enabled: Always show UI' (Automated)	☐	☐
2.3.10	**Downloading Framework Components**		
2.3.11	**File Open/Save Dialog Box**		
2.3.12	**First Run**		
2.3.13	**Graph Settings**		
2.3.14	**Help**		
2.3.15	**IME (Japanese)**		
2.3.16	**Improved Error Reporting**		
2.3.17	**Language Preferences**		
2.3.18	**Links**		
2.3.19	**Manage Restricted Permissions**		
2.3.19.1	(L1) Ensure 'Allow users with earlier versions of Office to read with browsers...' is set to 'Disabled' (Automated)	☐	☐
2.3.19.2	(L1) Ensure 'Always expand groups in Office when restricting permission for documents' is set to 'Enabled' (Automated)	☐	☐
2.3.19.3	(L1) Ensure 'Always require users to connect to verify permission' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.19.4	(L1) Ensure 'Never allow users to specify groups when restricting permission for documents' is set to 'Enabled' (Automated)	☐	☐
2.3.19.5	(L1) Ensure 'Prevent users from changing permissions on rights managed content' is set to 'Disabled' (Automated)	☐	☐
2.3.20	**Microsoft Office Document Cache**		
2.3.21	**Microsoft Office SmartArt**		
2.3.22	**Microsoft Save as PDF and XPS add-ins**		
2.3.23	**Miscellaneous**		
2.3.23.1	**Workflow Cache**		
2.3.23.2	(L1) Ensure 'Block signing into Office' is set to 'Enabled: Org ID only' (Automated)	☐	☐
2.3.23.3	(L1) Ensure 'Control Blogging' is set to 'Enabled: All Blogging Disabled' (Automated)	☐	☐
2.3.24	**Office 2016 Converters**		
2.3.24.1	(L1) Ensure 'Block opening of pre-release versions of file formats new to Excel 2016 through the Compatibility Pack for Office 2016 and Excel 2016 Converter' is set to 'Enabled' (Automated)	☐	☐
2.3.24.2	(L1) Ensure 'Block opening of pre-release versions of file formats new to PowerPoint 2016 through the Compatibility Pack for Office 2016 and PowerPoint 2016 Converter' is set to 'Enabled' (Automated)	☐	☐
2.3.25	**Present Online**		
2.3.25.1	**Presentation Services**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.25.2	(L2) Ensure 'Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word' is set to 'Enabled' (Automated)	☐	☐
2.3.26	**Readiness Toolkit**		
2.3.27	**Security Settings**		
2.3.27.1	**Digital Signatures**		
2.3.27.2	**Escrow Certificates**		
2.3.27.3	**Trust Center**		
2.3.27.3.1	**Application Guard**		
2.3.27.3.2	**Protected View**		
2.3.27.3.3	**Trusted Catalogs**		
2.3.27.3.4	(L1) Ensure 'Allow mix of policy and user locations' is set to 'Disabled' (Automated)	☐	☐
2.3.27.4	(L1) Ensure 'ActiveX Control Initialization' is set to 'Enabled: 6' (Automated)	☐	☐
2.3.27.5	(L1) Ensure 'Allow Basic Authentication prompts from network proxies' is set to 'Disabled' (Automated)	☐	☐
2.3.27.6	(L1) Ensure 'Allow VBA to load typelib references by path from untrusted intranet locations' is set to 'Disabled' (Automated)	☐	☐
2.3.27.7	(L1) Ensure 'Automation Security' is set to 'Enabled: Disable Macros by default' (Automated)	☐	☐
2.3.27.8	(L1) Ensure 'Control how Office handles form-based sign-in prompts' is set to 'Enabled: Block all prompts' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.27.9	(L1) Ensure 'Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine' is set to 'Disabled' (Automated)	☐	☐
2.3.27.10	(L1) Ensure 'Disable all Trust Bar notifications for security issues' is set to 'Disabled' (Automated)	☐	☐
2.3.27.11	(L1) Ensure 'Disable password to open UI' is set to 'Disabled' (Automated)	☐	☐
2.3.27.12	(L1) Ensure 'Encryption mode for Information Rights Management (IRM)' is set to 'Enabled: Cipher Block Chaining (CBC)' (Automated)	☐	☐
2.3.27.13	(L1) Ensure 'Encryption type for password protected Office 97-2003 files' is set to 'Enabled' (Automated)	☐	☐
2.3.27.14	(L1) Ensure 'Encryption type for password protected Office Open XML files' is set to 'Enabled' (Automated)	☐	☐
2.3.27.15	(L1) Ensure 'Load Controls in Forms3' is set to 'Enabled: 4' (Automated)	☐	☐
2.3.27.16	(L1) Ensure 'Macro Runtime Scan Scope' is set to 'Enabled: Enable for all documents' (Automated)	☐	☐
2.3.27.17	(L1) Ensure 'Protect document metadata for password protected files' is set to 'Enabled' (Automated)	☐	☐
2.3.27.18	(L1) Ensure 'Protect document metadata for rights managed Office Open XML Files' is set to 'Enabled' (Automated)	☐	☐
2.3.27.19	(L1) Ensure 'Suppress hyperlink warnings' is set to 'Disabled' (Automated)	☐	☐
2.3.28	**Server Settings**		
2.3.28.1	**SharePoint Server**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.28.2	(L1) Ensure 'Disable the Office client from polling the SharePoint Server for published links' is set to 'Enabled' (Automated)	☐	☐
2.3.29	**Services**		
2.3.29.1	**Fax**		
2.3.29.1.1	(L1) Ensure 'Disable Internet Fax feature' is set to 'Enabled' (Automated)	☐	☐
2.3.30	**Shared Paths**		
2.3.31	**Signing**		
2.3.31.1	(L1) Ensure 'Legacy format signatures' is set to 'Disabled' (Automated)	☐	☐
2.3.31.2	(L1) Ensure 'Suppress external signature services menu item' is set to 'Enabled' (Automated)	☐	☐
2.3.32	**Smart Documents (Word, Excel)**		
2.3.32.1	(L1) Ensure 'Disable Smart Document's use of manifests' is set to 'Enabled' (Automated)	☐	☐
2.3.33	**Subscription Activation**		
2.3.34	**Telemetry Dashboard**		
2.3.35	**Tools | AutoCorrect Options... (Excel, PowerPoint and Access)**		
2.3.36	**Tools | Options | General | Service Options...**		
2.3.36.1	**Conversion Service**		
2.3.36.1.1	(L2) Ensure 'Conversion Service Options' is set to 'Enabled: Do not allow to use Microsoft Conversion Service' (Automated)	☐	☐
2.3.36.2	**Online Content**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.36.2.1	(L2) Ensure 'Online Content Options' is set to 'Enabled: Do not allow Office to connect to the Internet' (Automated)	☐	☐
2.3.37	**Tools | Options | General | Web Options...**		
2.3.37.1	**Browsers**		
2.3.37.2	**Encoding**		
2.3.37.3	**Files**		
2.3.37.3.1	(L1) Ensure 'Open Office documents as read/write while browsing' is set to 'Disabled' (Automated)	☐	☐
2.3.37.4	**General**		
2.3.38	**Tools | Options | Spelling**		
2.3.38.1	**Proofing Data Collection**		
2.3.38.1.1	(L2) Ensure 'Improve Proofing Tools' is set to 'Disabled' (Automated)	☐	☐
2.3.39	**Trust Center**		
2.3.39.1	(L1) Ensure 'Send Office Feedback' is set to 'Disabled' (Automated)	☐	☐
2.3.39.2	(L1) Ensure 'Automatically receive small updates to improve reliability' is set to 'Disabled' (Automated)	☐	☐
2.3.39.3	(L1) Ensure 'Disable Opt-in Wizard on first run' is set to 'Enabled' (Automated)	☐	☐
2.3.39.4	(L1) Ensure 'Enable Customer Experience Improvement Program' is set to 'Disabled' (Automated)	☐	☐
2.3.39.5	(L1) Ensure 'Send personal information' is set to 'Disabled' (Automated)	☐	☐
2.4	**Microsoft OneNote 2016**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5	**Microsoft Outlook 2016**		
2.5.1	**Account Settings**		
2.5.1.1	**E-mail**		
2.5.1.2	**Exchange**		
2.5.1.2.1	(L1) Ensure 'Do not allow users to change permissions on folders' is set to 'Enabled' (Automated)	☐	☐
2.5.1.3	**Exchange ActiveSync**		
2.5.1.4	**IMAP**		
2.5.1.5	**Internet Calendars**		
2.5.1.5.1	(L1) Ensure 'Automatically download attachments' is set to 'Disabled' (Automated)	☐	☐
2.5.1.5.2	(L1) Ensure 'Do not include Internet Calendar integration in Outlook' is set to 'Enabled' (Automated)	☐	☐
2.5.1.6	**RSS Feeds**		
2.5.1.6.1	(L1) Ensure 'Download full text of articles as HTML attachments' is set to 'Disabled' (Automated)	☐	☐
2.5.1.6.2	(L1) Ensure 'Synchronize Outlook RSS Feeds with Common Feed List' is set to 'Disabled' (Automated)	☐	☐
2.5.1.6.3	(L1) Ensure 'Turn off RSS feature' is set to 'Enabled' (Automated)	☐	☐
2.5.1.7	**SharePoint Lists**		
2.5.2	**Customizable Error Messages**		
2.5.3	**Disable Items in User Interface**		
2.5.4	**Folder Home Pages for Outlook Special Folders**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.4.1	(L1) Ensure 'Do not allow Home Page URL to be set in folder Properties' is set to 'Enabled' (Automated)	☐	☐
2.5.5	**Form Region Settings**		
2.5.6	**InfoPath Integration**		
2.5.7	**Meeting Workspace**		
2.5.7.1	(L1) Ensure 'Disable user entries to server list' is set to 'Enabled: Publish default, disallow others' (Automated)	☐	☐
2.5.8	**MIME to MAPI Conversion**		
2.5.9	**Miscellaneous**		
2.5.9.1	**Miscellaneous**		
2.5.9.2	**PST Settings**		
2.5.9.2.1	(L1) Ensure 'PST Null Data on Delete' is set to 'Enabled' (Automated)	☐	☐
2.5.10	**Outlook Options**		
2.5.10.1	**Customize Ribbon**		
2.5.10.2	**Delegates**		
2.5.10.3	**Mail**		
2.5.10.4	**Mail Format**		
2.5.10.4.1	**International Options**		
2.5.10.4.2	**Internet Formatting**		
2.5.10.4.2.1	**Message Format**		
2.5.10.4.2.2	(L1) Ensure 'Plain Text Options' is set to 'Disabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.10.4.3	**Stationery and Fonts**		
2.5.10.5	**Mail Setup**		
2.5.10.6	**Other**		
2.5.10.6.1	**Advanced**		
2.5.10.6.1.1	**Reminder Options**		
2.5.10.6.1.2	(L1) Ensure 'Do not allow folders in non-default stores to be set as folder home pages' is set to 'Enabled' (Automated)	☐	☐
2.5.10.6.2	**AutoArchive**		
2.5.10.6.3	(L1) Ensure 'Make Outlook the default program for E-mail, Contacts, and Calendar' is set to 'Enabled' (Automated)	☐	☐
2.5.10.7	**Out of Office Assistant**		
2.5.10.8	**Preferences**		
2.5.10.8.1	**Calendar Options**		
2.5.10.8.1.1	**Free/Busy Options**		
2.5.10.8.1.2	**Office.com Sharing Service**		
2.5.10.8.1.2.1	(L1) Ensure 'Access to published calendars' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.1.2.2	(L1) Ensure 'Prevent publishing to a DAV server' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.1.2.3	(L1) Ensure 'Prevent publishing to Office.com' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.1.2.4	(L1) Ensure 'Restrict level of calendar details users can publish' is set to 'Enabled: Disables Full details and Limited details' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.10.8.1.2.5	(L1) Ensure 'Restrict upload method' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.1.3	**Planner Options**		
2.5.10.8.1.4	**Recurring Item Configuration**		
2.5.10.8.1.5	**Schedule View**		
2.5.10.8.2	**Contact Options**		
2.5.10.8.3	**E-mail Options**		
2.5.10.8.3.1	(L2) Ensure 'Read e-mail as plain text' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.3.2	(L2) Ensure 'Read signed e-mail as plain text' is set to 'Enabled' (Automated)	☐	☐
2.5.10.8.4	**Junk E-mail**		
2.5.10.8.4.1	(L1) Ensure 'Add e-mail recipients to users' Safe Senders Lists' is set to 'Disabled' (Automated)	☐	☐
2.5.10.8.4.2	(L1) Ensure 'Hide Junk Mail UI' is set to 'Disabled' (Automated)	☐	☐
2.5.10.8.4.3	(L1) Ensure 'Trust e-mail from contacts' is set to 'Disabled' (Automated)	☐	☐
2.5.10.8.5	**Search Options**		
2.5.10.9	**Right-to-Left**		
2.5.10.10	**Spelling**		
2.5.10.11	(L2) Ensure 'Internet and network paths into hyperlinks' is set to 'Disabled' (Automated)	☐	☐
2.5.11	**Outlook Social Connector**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.11.1	(L1) Ensure 'Turn off Outlook Social Connector' is set to 'Enabled' (Automated)	☐	☐
2.5.12	**Outlook Today Settings**		
2.5.13	**Search Folders**		
2.5.14	**Security**		
2.5.14.1	**Automatic Picture Download Settings**		
2.5.14.1.1	(L1) Ensure 'Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists' is set to 'Disabled' (Automated)	☐	☐
2.5.14.1.2	(L1) Ensure 'Block Trusted Zones' is set to 'Enabled' (Automated)	☐	☐
2.5.14.1.3	(L1) Ensure 'Display pictures and external content in HTML e-mail' is set to 'Enabled' (Automated)	☐	☐
2.5.14.1.4	(L1) Ensure 'Do not permit download of content from safe zones' is set to 'Disabled' (Automated)	☐	☐
2.5.14.2	**Cryptography**		
2.5.14.2.1	**Signature Status Dialog Box**		
2.5.14.2.1.1	(L1) Ensure 'Attachment Secure Temporary Folder' is set to 'Disabled' (Automated)	☐	☐
2.5.14.2.1.2	(L1) Ensure 'Missing CRLs' is set to 'Enabled: Error' (Automated)	☐	☐
2.5.14.2.1.3	(L1) Ensure 'Missing Root Certificates' is set to 'Enabled: Error' (Automated)	☐	☐
2.5.14.2.1.4	(L1) Ensure 'Promote Level 2 errors as errors, not warnings' is set to 'Disabled' (Automated)	☐	☐
2.5.14.2.2	(L1) Ensure 'Do not display 'Publish to GAL' button' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.14.2.3	(L1) Ensure 'Do not provide Continue option on Encryption warning dialog boxes' is set to 'Enabled' (Automated)	☐	☐
2.5.14.2.4	(L1) Ensure 'Message Formats' is set to 'Enabled: S/MIME' (Automated)	☐	☐
2.5.14.2.5	(L1) Ensure 'S/MIME interoperability with external clients:' is set to 'Enabled: Handle internally' (Automated)	☐	☐
2.5.14.3	**Security Form Settings**		
2.5.14.3.1	**Attachment Security**		
2.5.14.3.1.1	(L1) Ensure 'Do not prompt about Level 1 attachments when closing an item' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.1.2	(L1) Ensure 'Do not prompt about Level 1 attachments when sending an item' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.2	**Custom Form Security**		
2.5.14.3.3	**Programmatic Security**		
2.5.14.3.4	(L1) Ensure 'Outlook Security Mode' is set to 'Enabled' (Automated)	☐	☐
2.5.14.3.5	(L1) Ensure 'Allow Active X One Off Forms' is set to 'Enabled: Load only Outlook Controls' (Automated)	☐	☐
2.5.14.3.6	(L1) Ensure 'Allow hyperlinks in suspected phishing e-mail messages' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.7	(L1) Ensure 'Allow scripts in one-off Outlook forms' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.8	(L1) Ensure 'Allow users to demote attachments to Level 2' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.9	(L1) Ensure 'Authentication with Exchange server' is set to 'Enabled: Kerberos Password Authentication' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.14.3.10	(L1) Ensure 'Configure Outlook object model prompt when accessing an address book' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.11	(L1) Ensure 'Configure Outlook object model prompt When accessing the Formula property of a UserProperty object' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.12	(L1) Ensure 'Configure Outlook object model prompt when executing Save As' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.13	(L1) Ensure 'Configure Outlook object model prompt when reading address information' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.14	(L1) Ensure 'Configure Outlook object model prompt when responding to meeting and task requests' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.15	(L1) Ensure 'Display Level 1 attachments' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.16	(L1) Ensure 'Configure Outlook object model prompt when sending mail' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.17	(L1) Ensure 'Do not allow Outlook object model scripts to run for public folders' is set to 'Enabled' (Automated)	☐	☐
2.5.14.3.18	(L1) Ensure 'Do not allow Outlook object model scripts to run for shared folders' is set to 'Enabled' (Automated)	☐	☐
2.5.14.3.19	(L1) Ensure 'Enable RPC encryption' is set to 'Enabled' (Automated)	☐	☐
2.5.14.3.20	(L1) Ensure 'Include Internet in Safe Zones for Automatic Picture Download' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.21	(L1) Ensure 'Junk E-mail protection level' is set to 'Enabled: High' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.14.3.22	(L1) Ensure 'Minimum encryption settings' is set to 'Enabled: 256' (Automated)	☐	☐
2.5.14.3.23	(L1) Ensure 'Outlook Security Policy' is set to 'Use Outlook Security Group Policy' (Automated)	☐	☐
2.5.14.3.24	(L1) Ensure 'Prevent users from customizing attachment security settings' is set to 'Enabled' (Automated)	☐	☐
2.5.14.3.25	(L1) Ensure 'Remove file extensions blocked as Level 1' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.26	(L1) Ensure 'Remove file extensions blocked as Level 2' is set to 'Disabled' (Automated)	☐	☐
2.5.14.3.27	(L1) Ensure 'Retrieving CRLs (Certificate Revocation Lists)' is set to 'Enabled: When online always retrieve the CRL' (Automated)	☐	☐
2.5.14.3.28	(L1) Ensure 'Security setting for macros' is set to 'Enabled: Warn for signed, disable unsigned' (Automated)	☐	☐
2.5.14.3.29	(L1) Ensure 'Set Outlook object model custom actions execution prompt' is set to 'Enabled: Automatically Deny' (Automated)	☐	☐
2.5.14.3.30	(L1) Ensure 'Signature Warning' is set to 'Enabled: Always warn about invalid signatures' (Automated)	☐	☐
2.5.14.3.31	(L1) Ensure 'Use Unicode format when dragging e-mail message to file system' is set to 'Disabled' (Automated)	☐	☐
2.5.14.4	**Trust Center**		
2.5.14.4.1	(L1) Ensure 'Apply macro security settings to macros, add-ins and additional actions' is set to 'Enabled' (Automated)	☐	☐
2.5.14.5	(L1) Ensure 'Disable 'Remember password' for Internet e-mail accounts' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.14.6	(L1) Ensure 'Do not automatically sign replies' is set to 'Disabled' (Automated)	☐	☐
2.5.14.7	(L1) Ensure 'Prompt user to choose security settings if default settings fail' is set to 'Disabled' (Automated)	☐	☐
2.6	**Microsoft PowerPoint 2016**		
2.6.1	**Collaboration Settings**		
2.6.2	**Customizable Error Messages**		
2.6.3	**Disable Items in User Interface**		
2.6.4	**File Tab**		
2.6.5	**Miscellaneous**		
2.6.5.1	**Server Settings**		
2.6.5.2	(L2) Ensure 'Disable Slide Update' is set to 'Enabled' (Automated)	☐	☐
2.6.6	**PowerPoint Options**		
2.6.6.1	**Advanced**		
2.6.6.2	**Customize Ribbon**		
2.6.6.3	**General**		
2.6.6.4	**Proofing**		
2.6.6.5	**Save**		
2.6.6.5.1	(L1) Ensure 'Default file format' is set to 'Enabled: PowerPoint Presentation (*pptx)' (Automated)	☐	☐
2.6.6.6	**Security**		
2.6.6.6.1	**Cryptography**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6.6.6.2	**Trust Center**		
2.6.6.6.2.1	**File Block Settings**		
2.6.6.6.2.1.1	(L1) Ensure 'PowerPoint 97-2003 presentations, shows, templates and add-in files' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.6.6.6.2.1.2	(L1) Ensure 'Set default file block behavior' to 'Enabled: Blocked files are not opened' (Automated)	☐	☐
2.6.6.6.2.2	**Protected View**		
2.6.6.6.2.2.1	(L1) Ensure 'Do not open files from the Internet zone in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.2.2.2	(L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.2.2.3	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)	☐	☐
2.6.6.6.2.2.4	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit' (Automated)	☐	☐
2.6.6.6.2.2.5	(L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.2.3	**Trusted Locations**		
2.6.6.6.2.3.1	(L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.2.3.2	(L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)	☐	☐
2.6.6.6.2.4	(L1) Ensure 'Block macros from running in Office files from the Internet' is set to 'Enabled' (Automated)	☐	☐
2.6.6.6.2.5	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.6.6.6.2.6	(L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)	☐	☐
2.6.6.6.2.7	(L1) Ensure 'Trust Access to Visual Basic Project' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.2.8	(L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)	☐	☐
2.6.6.6.3	(L1) Ensure 'Make hidden markup visible' is set to 'Enabled' (Automated)	☐	☐
2.6.6.6.4	(L1) Ensure 'Run Programs' is set to 'Enabled: disable (don't run any programs)' (Automated)	☐	☐
2.6.6.6.5	(L1) Ensure 'Scan encrypted macros in PowerPoint Open XML presentations' is set to 'Enabled: Scan encrypted macros' (Automated)	☐	☐
2.6.6.6.6	(L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)	☐	☐
2.6.6.6.7	(L1) Ensure 'Unblock automatic download of linked images' is set to 'Disabled' (Automated)	☐	☐
2.7	**Microsoft Project 2016**		
2.8	**Microsoft Publisher 2016**		
2.8.1	**Disable Items in User Interface**		
2.8.2	**Miscellaneous**		
2.8.3	**Publisher Options**		
2.8.4	**Security**		
2.8.4.1	**Trust Center**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.8.4.1.1	(L1) Ensure 'Block macros from running in Office files from the internet' is set to 'Enabled' (Automated)	☐	☐
2.8.4.1.2	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' to 'Enabled' (Automated)	☐	☐
2.8.4.1.3	(L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)	☐	☐
2.8.4.1.4	(L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)	☐	☐
2.8.4.2	(L1) Ensure 'Publisher Automation Security Level' is set to 'Enabled: By UI (prompted)' (Automated)	☐	☐
2.9	**Microsoft Teams**		
2.10	**Microsoft Visio 2016**		
2.11	**Microsoft Word 2016**		
2.11.1	**Collaboration Settings**		
2.11.2	**Customizable Error Messages**		
2.11.3	**Disable Items in User Interface**		
2.11.4	**File Tab**		
2.11.5	**Japanese Find**		
2.11.6	**Miscellaneous**		
2.11.6.1	**Server Settings**		
2.11.6.2	(L2) Ensure 'Use online translation dictionaries' is set to 'Disabled' (Automated)	☐	☐
2.11.7	**Review Tab**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.11.8	**Word Options**		
2.11.8.1	**Advanced**		
2.11.8.1.1	**E-Mail Options**		
2.11.8.1.2	(L1) Ensure 'Update automatic links at Open' is set to 'Disabled' (Automated)	☐	☐
2.11.8.2	**Customized Ribbon**		
2.11.8.3	**Display**		
2.11.8.3.1	(L1) Ensure 'Hidden text' is set to 'Enabled' (Automated)	☐	☐
2.11.8.4	**General**		
2.11.8.5	**Proofing**		
2.11.8.6	**Save**		
2.11.8.6.1	(L1) Ensure 'Default file format' is set to 'Enabled: Word Document (.docx)' (Automated)	☐	☐
2.11.8.7	**Security**		
2.11.8.7.1	**Cryptography**		
2.11.8.7.2	**Trust Center**		
2.11.8.7.2.1	**File Block Settings**		
2.11.8.7.2.1.1	(L1) Ensure 'Set default file block behavior' is set to 'Enabled: Blocked files are not opened' (Automated)	☐	☐
2.11.8.7.2.1.2	(L1) Ensure 'Word 2 and earlier binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.3	(L1) Ensure 'Word 2000 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.11.8.7.2.1.4	(L1) Ensure 'Word 2003 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.5	(L1) Ensure 'Word 2007 and later binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.6	(L1) Ensure 'Word 6.0 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.7	(L1) Ensure 'Word 95 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.8	(L1) Ensure 'Word 97 binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.1.9	(L1) Ensure 'Word XP binary documents and templates' is set to 'Enabled: Open/Save blocked, use open policy' (Automated)	☐	☐
2.11.8.7.2.2	**Protected View**		
2.11.8.7.2.2.1	(L1) Ensure 'Do not open files from the internet zone in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.2.2	(L1) Ensure 'Do not open files in unsafe locations in Protected View' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.2.3	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Enabled: Open in Protected View' (Automated)	☐	☐
2.11.8.7.2.2.4	(L1) Ensure 'Set document behavior if file validation fails' is set to 'Unchecked: Do not allow edit` (Automated)	☐	☐
2.11.8.7.2.2.5	(L1) Ensure 'Turn off Protected View for attachments opened from Outlook' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.3	**Trusted Locations**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.11.8.7.2.3.1	(L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.3.2	(L2) Ensure 'Disable all trusted locations' is set to 'Enabled' (Automated)	☐	☐
2.11.8.7.2.4	(L1) Ensure 'Block macros from running in Office files from the Internet' is set to 'Enabled' (Automated)	☐	☐
2.11.8.7.2.5	(L1) Ensure 'Dynamic Data Exchange' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.6	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to 'Enabled' (Automated)	☐	☐
2.11.8.7.2.7	(L1) Ensure 'Disable Trust Bar Notification for unsigned application add-ins and block them' is set to 'Enabled' (Automated)	☐	☐
2.11.8.7.2.8	(L1) Ensure 'Scan encrypted macros in Word Open XML Documents' to 'Enabled: Scan encrypted macros (default)' (Automated)	☐	☐
2.11.8.7.2.9	(L1) Ensure 'Trust access to Visual Basic Project' is set to 'Disabled' (Automated)	☐	☐
2.11.8.7.2.10	(L1) Ensure 'VBA Macro Notification Settings' is set to 'Enabled: Disable all except digitally signed macros' (Automated)	☐	☐
2.11.8.7.3	(L1) Ensure 'Make hidden markup visible' is set to 'Enabled' (Automated)	☐	☐
2.11.8.7.4	(L1) Ensure 'Turn off file validation' is set to 'Disabled' (Automated)	☐	☐
2.12	**Skype for Business 2016**		

Appendix: Change History

Date	Version	Changes for this version
11/17/2023	1.0.0	Initial release