CENTER FOR INTERNET SECURITY

CIS Microsoft Office Access 2016 Benchmark

v1.0.0 - 01-29-2016

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

CIS SECURITY BENCHMARKS TERMS OF USE

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

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

UNDER THE FOLLOWING TERMS AND CONDITIONS:

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

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

Table of Contents

Overview

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

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Access 2016 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

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

Scored

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

Not Scored

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

Acknowledgements

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

Contributor
Hardeep Mehrotara CISSP, CISA, GSEC, ISMSA

Editor
Jordan Rakoske
Edward Oechsner

Recommendations

1 User Configuration

1.1 Application Settings

This section contains settings to configure Application Settings.

1.1.1 General

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

1.1.2 International

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

1.1.3 Security

This section contains settings to configure Security Options.

1.1.3.1 Cryptography

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

1.1.3.2 Trust Center

This section contains settings to configure Trust Center.

1.1.3.2.1 Trusted Locations

This section contains settings to configure Trusted Locations.

1.1.3.2.1.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the "Allow Trusted Locations on my network (not recommended)" check box in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable or do not configure this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center. Disabling this policy setting does not delete any network locations from the Trusted Locations list. Instead, it forces the selected application to treat the locations as non-trusted and prevents users from adding new network locations to the list.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting will cause disruption for users who add network locations to the Trusted Locations list. However, it is not recommended to enable this policy setting (as the "Allow Trusted Locations on my network (not recommended)" check box itself states), so in practice it should be possible to disable this policy setting in most situations without causing significant usability issues for most users. The recommended state for this setting is: `Disabled`.

Rationale:

By default, files located in trusted locations and specified in the Trust Center are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

By default, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the Allow Trusted Locations on my network (not recommended) check box in the Trusted Locations section of the Trust Center. If a dangerous file is opened from a trusted location, it will not be subject to typical security measures and could affect users' computers or data.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\trusted
locations\allownetworklocations
```

Remediation:

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

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

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. However, this practice is discouraged (as the Allow Trusted Locations on my network (not recommended) check box itself states), so in practice it should be possible to disable this setting in most situations without causing significant usability issues for most users.

Default Value:

Not Configured

1.1.3.2.1.2 (L1) Ensure 'Disable all trusted locations' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications. 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 users' computers or data.

If you enable this policy setting, 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.

If you disable or do not configure this policy setting, all trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe. 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 users' computers or data.

By default, files located in trusted locations (those specified in the Trust Center) are assumed to be safe.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\trusted
locations\alllocationsdisabled
```

Remediation:

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

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

Impact:

If there are business-critical reasons to access some files in a more trusted environment, disabling trusted locations could cause usability problems.

Default Value:

Not Configured

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

Profile Applicability:

- Level 1

Description:

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

If you enable this policy setting, this application checks the digital signature for each add-in before loading it. If an add-in does not have a digital signature, or if the signature did not come from a trusted publisher, this application disables the add-in and notifies the user. Microsoft provides four certificates for Office, which you can add to the Trusted Publishers list. These certificates must be added to the Trusted Publishers list if you require that all add-ins be signed by a trusted publisher. The Microsoft certificates are named Mscert01.cer, Mscert02.cer, Mscert03.cer, Mscert04.cer, and can be found on the Microsoft Web site. Office 2016 stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office 2016 still reads trusted publisher certificate information from the Office trusted publisher store, but it 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 Office 2016, 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. For more information about trusted publishers, see the Office Resource Kit.

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

Rationale:

By default, Office 2016 applications do not check the digital signature on application add-ins before opening them. Disabling or not configuring this setting may allow an application to load a dangerous add-in. As a result, malicious code could become active on user computers or the network.

Audit:

1.1 Audit Procedure

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\requireaddinsig
```

Remediation:

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

```
User Configuration\Microsoft Access 2016\Application Settings\Security\Trust Center\Require that application add-ins are signed by trusted publisher
```

Impact:

Enabling 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 2016 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 2016 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 2016 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.

Default Value:

Not Configured

1.1.3.2.3 (L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed Macros) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office.

- 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.

- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.

- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Also, note that Microsoft Office stores certificates for trusted publishers in the Internet Explorer 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 you created a list of trusted publishers in a previous version of Microsoft Office and you upgrade to Office, 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. The recommended state for this setting is: `Enabled. (Disable all Except Digitally Signed Macros)`

Rationale:

By default, when users open files in Access 2016 that contain VBA macros, Access 2016 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.

Disabling or not configuring this setting may allow dangerous macros 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 group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\vbawarnings
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access 2016\Application
Settings\Security\Trust Center\VBA Macro Notification Settings
```

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.

Default Value:

Not Configured

1.1.3.2.4 (L1) Ensure Set 'Disable Trust Bar Notification for unsigned application add-ins ' is set to Enabled (Scored)

Profile Applicability:

- Level 1

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. This policy setting only applies if you enable the "Require that application add-ins are signed by Trusted Publisher" policy setting, which prevents users from changing this policy setting.

If you enable this policy setting, applications automatically disable unsigned add-ins without informing users.

If you disable this policy setting, if this 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.

If you do not configure this policy setting, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application. The recommended state for this setting is: `Enabled`.

Rationale:

By default, 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 group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\notbpromptunsignedaddin
```

Remediation:

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

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

Impact:

This setting only applies if the Office 2016 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.

Default Value:

Not Configured

1.1.4 Web Options...

This section contains settings to configure Web Options.

1.1.4.1 General

This section contains settings to configure General Options.

1.1.4.1.1 (L1) Ensure 'Underline hyperlinks' is set to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

If you enable this policy setting, Access underlines all hyperlinks in tables, queries, forms, and reports when they are created, overriding any configuration changes on the users' computers.

If you disable this policy setting, Access does not underline hyperlinks in tables, queries, forms and reports.

If you do not configure this policy setting, Access underlines hyperlinks that appear in tables, queries, forms, and reports.

Enabling this policy setting enforces the default configuration in Access, and is therefore unlikely to cause a significant usability issue for most users. If this configuration is changed, users might click on dangerous hyperlinks without realizing it, which could pose a security risk. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Access 2016 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.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\internet\donotunderlin
ehyperlinks
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access 2016\Application
Settings\Web Options...\General\Underline hyperlinks
```

Impact:

If this setting is Enabled, Access 2016 underlines all hyperlinks in tables, queries, forms, and reports when they are created, overriding any configuration changes on the users' computers.

Default Value:

Not Configured

1.2 Customizable Error Messages

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

1.3 Disable Items in User Interface

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

1.3.1 Custom

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

1.3.2 Predefined

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

1.4 Miscellaneous

This section contains settings to configure Miscellaneous Options.

1.4.1 (L1) Ensure 'Do not prompt to convert older databases' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

If you enable this policy setting, 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.

If you disable or do not configure this policy setting, 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. 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 2016 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.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\settings\noconvertdialog
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access 2016\Miscellaneous\Do not prompt to convert older databases
```

Impact:

Disabling this setting enforces the default configuration in Access 2016, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not Configured

1.4.2 (L1) Ensure 'Default file format' is set to Enabled (Access 2007) (Scored)

Profile Applicability:

- Level 1

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.

If you enable this policy setting, you can specify whether new database files are created in Access 2016 format by default or in Access 2002--2003 format. Users can still override the default and select a specific format when they save the files, but cannot set the default by themselves from the Access Options dialog.

If you disable or do not configure this policy setting, when users create new database files, Access saves them in the new Access 2016 format; however, users can change this functionality by selecting a file format from the Default file format drop down list under Access Options | Popular | Creating databases. Note: If you disable this policy setting, users can choose from three default file formats: Access 2000, Access 2002--2003, and Access 2016. You can use this policy setting to specify either the Access 2002--2003 or Access 2016 format as the default, but not the Access 2000 format. The recommended state for this setting is: `Enabled. (Access 2007)`

Rationale:

By default, when users create new database files, Access 2016 saves them in the new Access 2016 format. Users can change this functionality by clicking the Office button, clicking Access Options, and then selecting a file format from the Default file format list.

Disabling this setting allows users to choose from any of the available default file formats. If a new workbook 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 Access 2016 format.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\settings\default file format
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access
2016\Miscellaneous\Default file 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.

Default Value:

Not Configured

1.5 Tools | Security

This section contains settings to configure Tools and Security Options.

1.5.1 Workgroup Administrator...

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

1.5.2 (L1) Ensure 'Modal Trust Decision Only' is set to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

If you enable this policy setting, when users attempt to open an untrusted Access database that contains user-programmed executable components, users see a dialog box where they then must choose whether to enable or disable the components before they can work with the database.

If you disable or do not configure this policy setting, 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 recommended state for this setting is: `Disabled`.

Rationale:

By default, when users open an untrusted Access 2016 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.

Audit:

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

```
HKEY_USERS\<SID>\software\policies\microsoft\office\16.0\access\security\modaltrustdec
isiononly
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access 2016\Tools |
Security\Modal Trust Decision Only
```

Impact:

Disabling this setting enforces the default configuration for Access 2016, and so is unlikely to cause usability issues. However, this functionality has changed from previous versions of Access. In Access 2003, the default configuration presented the user with a dialog box (equivalent to how Access 2016 functions when the setting is Enabled).

Default Value:

Not Configured

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Application Settings**		
1.1.1	**General**		
1.1.2	**International**		
1.1.3	**Security**		
1.1.3.1	**Cryptography**		
1.1.3.2	**Trust Center**		
1.1.3.2.1	**Trusted Locations**		
1.1.3.2.1.1	(L1) Ensure 'Allow Trusted Locations on the network' is set to Disabled (Scored)	☐	☐
1.1.3.2.1.2	(L1) Ensure 'Disable all trusted locations' is set to Enabled (Scored)	☐	☐
1.1.3.2.2	(L1) Ensure 'Require that application add-ins are signed by Trusted Publisher' is set to Enabled (Scored)	☐	☐
1.1.3.2.3	(L1) Ensure 'VBA Macro Notification Settings' is set to Enabled (Disable all Except Digitally Signed Macros) (Scored)	☐	☐
1.1.3.2.4	(L1) Ensure Set 'Disable Trust Bar Notification for unsigned application add-ins ' is set to Enabled (Scored)	☐	☐
1.1.4	**Web Options...**		
1.1.4.1	**General**		
1.1.4.1.1	(L1) Ensure 'Underline hyperlinks' is set to Enabled (Scored)	☐	☐
1.2	**Customizable Error Messages**		
1.3	**Disable Items in User Interface**		
1.3.1	**Custom**		
1.3.2	**Predefined**		
1.4	**Miscellaneous**		
1.4.1	(L1) Ensure 'Do not prompt to convert older databases' is set to Disabled (Scored)	☐	☐
1.4.2	(L1) Ensure 'Default file format' is set to Enabled (Access 2007) (Scored)	☐	☐
1.5	**Tools | Security**		
1.5.1	**Workgroup Administrator...**		
1.5.2	(L1) Ensure 'Modal Trust Decision Only' is set to Disabled (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
1-29-16	1.0.0	Initial Release based off the Access 2013 Benchmark