Center for Internet Security®

CIS Microsoft Office Access 2013

v1.0.1 - 11-30-2016

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft Access 2013, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Access 2013 running on Windows 7. This guide was tested against Microsoft Office 2013. 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 2013 on a Microsoft Windows platform.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

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

Scored

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

Not Scored

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

Acknowledgements

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

Editor
Jordan Rakoske
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.

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 2013\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.

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 2013\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.

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. 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:

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 2013\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 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.

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.

The recommended state for this setting is: `Enabled. (Disable all Except Digitally Signed Macros)`

Rationale:

By default, when user's open files in Access that contain VBA macros, Access 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 2013\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.

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 2013\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 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.

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

Rationale:

By default, 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.

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 2013\Application
Settings\Web Options...\General\Underline hyperlinks
```

Impact:

If this setting is Enabled, Access 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.

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

Rationale:

By default, when user's 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.

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 2013\Miscellaneous\Do not prompt to convert older databases
```

Impact:

Disabling this setting enforces the default configuration in Access, 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.

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

Rationale:

By default, when users create new database files, Access saves them in the new Access 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 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 2013\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.

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.

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\modaltrustdecisiononly
```

Remediation:

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

```
User Configuration\Administrative Templates\Microsoft Access 2013\Tools |
Security\Modal Trust Decision Only
```

Impact:

Disabling this setting enforces the default configuration for Access, and so is unlikely to cause usability issues. However, this functionality has changed from previous versions of Access.

Default Value:

Not Configured

Appendix: Summary Table

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
8/07/2015	1.0.0	Initial Release
11/30/2016	1.0.1	Text and Title cleanup