

Trusted Location #1

This policy setting allows you to specify a folder as a trusted location from which to open 2016 Word, Excel, PowerPoint, Access and Visio files. Files in trusted locations bypass file validation, active content checks and Protected View. Macros and code in these files will execute without displaying warnings to the user. If you change or add a location make sure that the new location is secured, with only appropriate user permissions to add document/files.

If you enable this policy setting, you can specify a trusted location (or folder) from which the 2016 Office application can open the files which run macros without warning.

If you disable or do not configure this policy setting, the trusted location is not specified.

Supported on: At least Windows 7

Path:

Single line textbox

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\excel\security\trusted locations\location1
Value Name	path
Value Type	REG_EXPAND_SZ
Default Value	

Date:

Single line textbox

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\excel\security\trusted locations\location1
Value Name	date
Value Type	REG_SZ
Default Value	

Description:

Single line textbox

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\excel\security\trusted locations\location1
Value Name	description
Value Type	REG_SZ
Default Value	

☐ Allow sub folders:

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\excel\security\trusted locations\location1
Value Name	allowsubfolders
Value Type	REG_DWORD
Default Value	0
True Value	1
False Value	0

- Microsoft Office 2016 (Machine)
- Microsoft PowerPoint 2016 (Machine)
- Skype for Business 2016

Administrative Templates (Users)



- Microsoft Access 2016
- ▼ Microsoft Excel 2016
 - Customizable Error Messages
 - Data Recovery
 - Disable Items in User Interface
 - ▼ Excel Options
 - Advanced
 - Customize Ribbon
 - Formulas
 - General
 - Proofing
 - Save
 - ▼ Security
 - Cryptography
 - ▼ Trust Center
 - External Content
 - File Block Settings
 - Protected View
 - ▼ Trusted Locations
 - Allow Trusted Locations on the network
 - Disable all trusted locations
 - Trusted Location #1
 - Trusted Location #2
 - Trusted Location #3
 - Trusted Location #4
 - Trusted Location #5
 - Trusted Location #6
 - Trusted Location #7
 - Trusted Location #8
 - Trusted Location #9
 - Trusted Location #10
 - Trusted Location #11
 - Trusted Location #12
 - Trusted Location #13
 - Trusted Location #14
 - Trusted Location #15
 - Trusted Location #16
 - Trusted Location #17
 - Trusted Location #18
 - Trusted Location #19
 - Trusted Location #20
 - Block macros from running in Office files from the internet
 - Disable all application add-ins
 - Disable Trust Bar Notification for unsigned application add-ins and block them
 - Macro Notification Settings
 - Prevent Excel from running XLM macros
 - Require that application add-ins are signed by Trusted Publisher
 - Set maximum number of trusted documents
 - Set maximum number of trust records to preserve
 - Store macro in Personal Macro Workbook by default
 - Trust access to Visual Basic Project
 - Turn off trusted documents
 - Turn off Trusted Documents on the network
 - Force file extension to match file type
 - Perform file validation on pivot caches
 - Scan encrypted macros in Excel Open XML workbooks
 - Turn off file validation
 - WEBSERVICE Function Notification Settings

- └─ ➤ File tab
- └─ ➤ Intelligent Services
- └─ ➤ Miscellaneous
- └─ ➤ Power BI
- Microsoft Office 2016
- Microsoft OneNote 2016
- Microsoft Outlook 2016
- Microsoft PowerPoint 2016
- Microsoft Project 2016
- Microsoft Publisher 2016
- Microsoft Teams
- Microsoft Visio 2016
- Microsoft Word 2016
- Skype for Business 2016