Macro Runtime Scan Scope

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. Macros can only be scanned if the anti-virus software registers as an Antimalware Scan Interface (AMSI) provider on the device.

If you enable this policy setting, you can choose from the following options to determine the macro runtime scanning behavior:

- Disable for all files (not recommended): If you choose this option, no runtime scanning of enabled macros will be performed.

- Enable for low trust files: If you choose this option, runtime scanning will be enabled for all files for which macros are enabled, except for the following files:
- Files opened while macro security settings are set to "Enable All Macros"
- Files opened from a Trusted Location
- Files that are Trusted Documents
- Files that contain VBA that is digitally signed by a Trusted Publisher

- Enable for all files: If you choose this option, then low trust files are not excluded from runtime scanning.

The VBA and XLM runtimes report to an antivirus system certain high-risk code behaviors the macro is about to execute. This allows the antivirus system to indicate whether or not the macro behavior is malicious. If the behavior is determined to be malicious, the Office application closes the session and the antivirus system can quarantine the file. If the behavior is non-malicious, the macro execution proceeds.

Note: When macro runtime scanning is enabled, the runtime performance of affected VBA projects and XLM sheets may be reduced.

If you disable this policy setting, no runtime scanning of enabled macros will be performed.

If you don't configure this policy setting, "Enable for low trust files" will be the default setting.

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

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

0. Disable for all documents

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\common\security
Value Name	macroruntimescanscope
Value Type	REG_DWORD
Value	0

1. Enable for low trust documents

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\common\security
Value Name	macroruntimescanscope
Value Type	REG_DWORD
Value	1

2. Enable for all documents

Registry Hive	HKEY_CURRENT_USER
Registry Path	software\policies\microsoft\office\16.0\common\security
Value Name	macroruntimescanscope
Value Type	REG_DWORD
Value	2

office16.admx

Administrative Templates (Computers)

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

Administrative Templates (Users)

- Microsoft Access 2016
- Microsoft Excel 2016
- Microsoft Office 2016
  - AutoSave
  - Business Data
  - Collaboration Settings
  - Contact Card
  - Customizable Error Messages
  - Disable Items in User Interface
  - DLP
  - Document Information Panel
  - Downloading Framework Components
  - File Open/Save dialog box
  - First Run
  - Global Options
  - Graph settings
  - Help
  - IME (Japanese)
  - Improved Error Reporting
  - Language Preferences
  - Manage Restricted Permissions
  - Microsoft Office Document Cache
  - Microsoft Office SmartArt
  - Microsoft Save As PDF and XPS add-ins
  - Miscellaneous
  - Office 2016 Converters
  - Present Online
  - Privacy
  - Readiness Toolkit
  - Security Settings

- Digital Signatures
- Escrow Certificates
- Trust Center
- ActiveX Control Initialization
- Allow file extensions for OLE embedding
- Allow VBA to load typelib references by path from untrusted intranet locations
- Automation Security
- Block additional file extensions for OLE embedding
- Check ActiveX objects
- Check Excel RTD servers
- Check OLE objects
- Check OWC data source providers
- Control how Office handles form-based sign-in prompts
- Disable 3D Model File Formats List
- Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine
- Disable All ActiveX
- Disable all Trust Bar notifications for security issues
- Disable password to open UI
- Disable VBA for Office applications
- Disable VSTO 2003 and 2005 document-level customizations
- Enable Minimizing VBA Project Digital Signature Invalidation
- Encrypt document properties
- Encryption type for password protected Office 97-2003 files
- Encryption type for password protected Office Open XML files
- Force Runtime AV Scan
- Load Controls in Forms3
- Macro Runtime Scan Scope
- Prevent Word and Excel from loading managed code extensions
- Protect document metadata for password protected files
- Protect document metadata for rights managed Office Open XML Files
- Set minimum password length
- Set password hash format as ISO-compliant
- Set password rules domain timeout
- Set password rules level
- Suppress hyperlink warnings
- Turn off error reporting for files that fail file validation
- Turn off PDF encryption setting UI
- Use the Sensitivity feature in Office to apply and view sensitivity labels

- Server Settings
- Services

- Shared paths
- Signing
- Smart Documents (Word, Excel)
- Subscription Activation
- Telemetry Dashboard
- Tools | AutoCorrect Options... (Excel, PowerPoint and Access)
- Tools | Options | General | Service Options...
- Tools | Options | General | Web Options...
- Tools | Options | Spelling
- Web Archives
- What's New

- 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