SECMON1

Information Security Guideline

Configuring Macro Settings

THIS PAGE INTENTIONALLY LEFT BLANK

Disabling or limiting Microsoft Office macros can aid in preventing malicious code from entering your organisation's network. Compromised macros can often evade basic email content filtering and application whitelisting.

While macros can greatly improve productivity, they can also make your systems vulnerable, especially if they are out-of-date or downloaded from the Internet.

All macros created by users or third parties should be reviewed before being approved for use within the organisation. By understanding the business requirements for the use of macros, and applying the necessary mitigation strategies, organisations can effectively manage the risk of allowing them in their IT environment.

Note: The best approach is to block macros from the Internet and only allow vetted macros either in "trusted locations" with limited write access or digitally signed with a trusted certificate.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what Microsoft Office Macros are and why it is an essential security measure to configure or even disable them.

In this document, we are going to provide some basic macro configuration steps to assist in strengthening your security, as well as providing you with some interesting and important links where you can educate yourself further on this topic and identify other options available to you.

Implementation Guidance

Microsoft Office has a new security feature that blocks macros from the Internet. When configuring this feature, also configure the Microsoft Windows Attachment Manager to prevent users from removing zone information, which is used as a way of getting around the block.

For organisations with a business requirement to run Microsoft Office macros, configure Microsoft Office on a per-user and per-application basis to only run macros vetted as trustworthy and preferably placed in 'trusted location' directories typical users can't write to.

Enforce the macro security configuration settings via Group Policy to prevent users from changing them to run a malicious or otherwise unapproved macro.

Further information

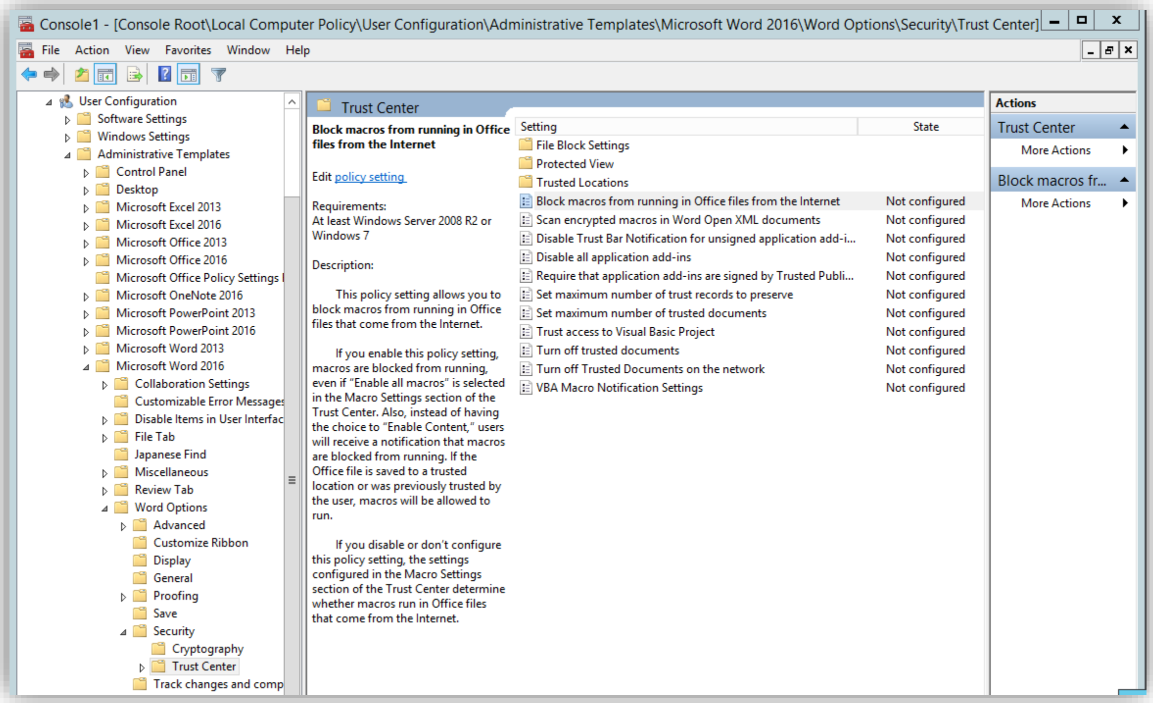
Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

More information on Macro-based malware and the Macro-disable feature in Office 2016 is available here.

How-To Guide

Using Group Policy for Enforcing the Macro Block or Configuring Macro Use in Windows Server 2008

1. Either press the Windows logo key +R to open the **RUN** dialog box or click **Start**, click **All Programs**, click **Accessories**, then click **Run**.
2. Type **gpmc.msc** in the text box, and then click **OK** or press **ENTER**. This opens the **Group Policy Management Console/Editor**
3. In the **Group Policy Management Editor**, go to **User Configuration**
4. Click **Administrative Templates** > **Microsoft Word 2016** > **Word Options** > **Security** > **Trust Center**
5. Open the **Block macros from running in Office files from the Internet** setting to configure and enable it



Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

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. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

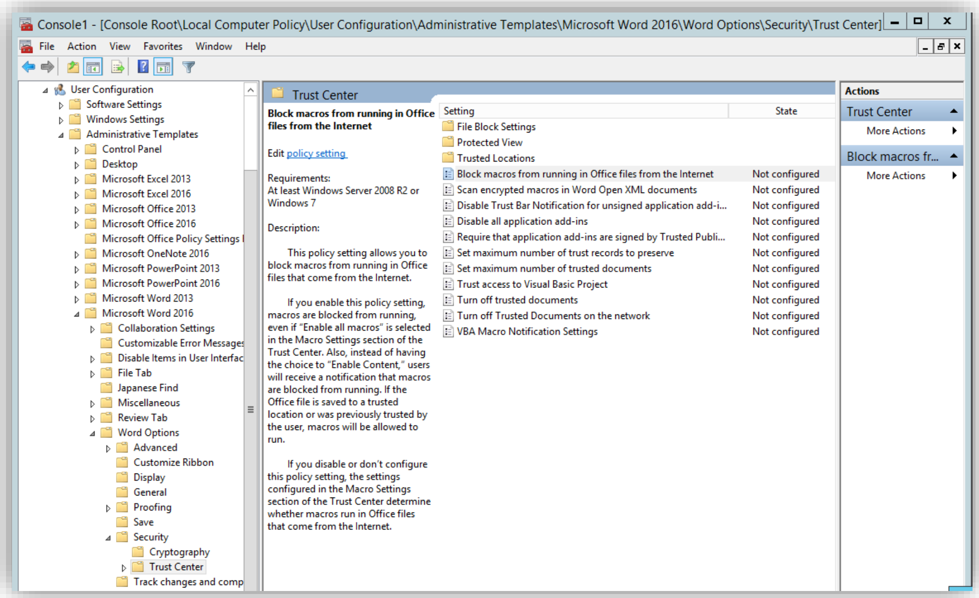
If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different available macro configuration options, please go here.

Using Group Policy for Enforcing the Macro Block or Configuring Macro Use in Windows Server 2012

1. On the **Start** screen, click the **Apps** arrow.
2. On the **Apps** screen, type **gpmc.msc** and then click **OK** or press **ENTER**
3. In the **Group Policy Management Editor**, go to **User Configuration**
4. Click **Administrative Templates** > **Microsoft Word 2016** > **Word Options** > **Security** > **Trust Center**
5. Open the **Block macros from running in Office files from the Internet** setting to configure and enable it



Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

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. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different available macro configuration options, please go here.

How to Disable or Configure Macros in Microsoft Office Applications in Office 2007, 2010, and 2012

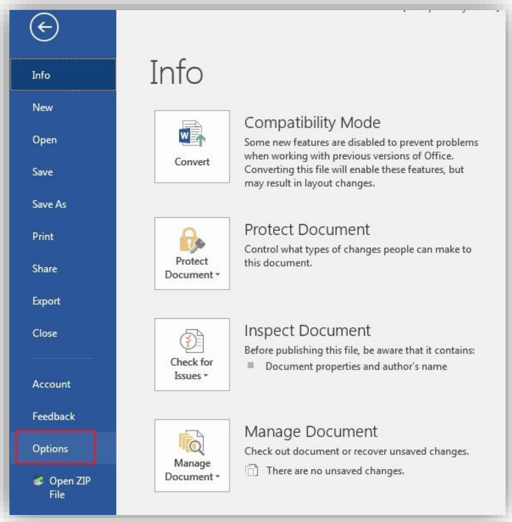
1. Open the Microsoft Office application of choice (eg, Office, Excel, Access, Powerpoint)
2. Click the **Microsoft Office Button** (example below) and then click **Options** (Note: The word "Options" will be preceded by whichever Office program you are in).

    a. If you are in Outlook, click the **Tools** menu

3. Click **Trust Center**, then click **Trust Center Settings**, and then click **Macro Settings**
4. Click the option that you want. Options include the following:
    a. **Disable all macros without notification**: Click this option if you don't trust macros. All macros in documents and security alerts about macros are disabled. If there are documents with unsigned macros that you can trust, you can put those documents into a trusted location. Documents in trusted locations are allowed to run without being checked by the Trust Center security system.
    b. **Disable all macros with notification**: This is the default setting. Click this option if you want macros to be disabled, but you want to get security alerts if there are macros present. This way, you can choose when to enable those macros on a case by case basis.
    c. **Disable all macros except digitally signed macros**: This setting is the same as the **Disable all macros with notification** option, except that if the macro is digitally signed by a trusted publisher, the macros can run if you have already trusted the publisher. If you have not trusted the publisher, you are notified. That way, you can choose to enable those signed macros or trust the publisher. All unsigned macros are disabled without notification.
    d. **Enable all macros (not recommended, potentially dangerous code can be run)**: Click this option to allow all macros to be run. This setting makes your computer vulnerable to potentially malicious code and is not recommended.
    e. **Trust access to the VBA project object model**: This setting is for developers. It provides a security option for code that is written to automate an Office program. This is a per user and per application setting, and denies access by default. This makes it more difficult for unauthorized programs to build "self-replicating" code that can harm end-user systems.

How to Disable or Configure Macros in Microsoft Office Applications in Office 2016

1. Open the Microsoft Office application of choice (eg, Word, Excel, Powerpoint, Outlook)
2. Click the **File** tab, then click **Options**.



Info

Compatibility Mode

Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware that it contains:

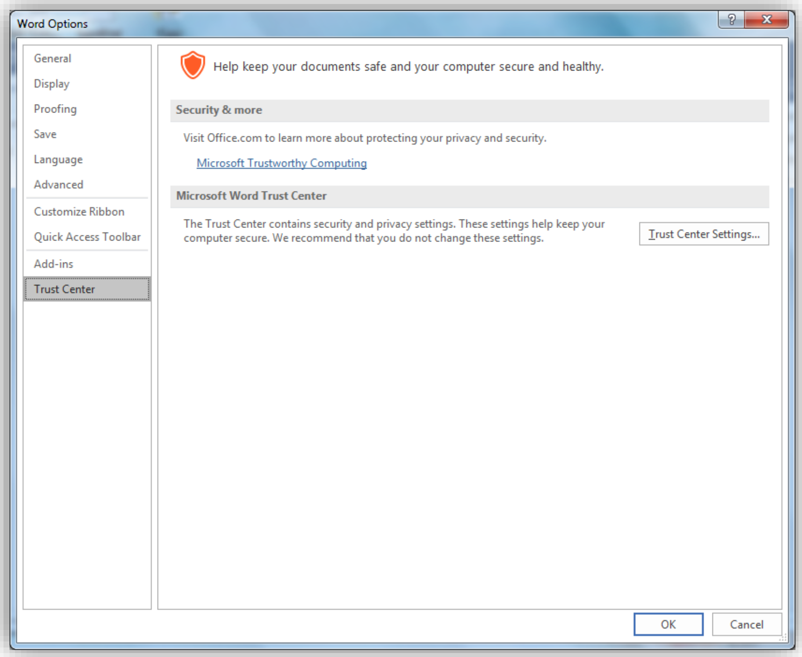
- Document properties and author's name

Manage Document

Check out document or recover unsaved changes.

There are no unsaved changes.

3. Click on **Trust Center** and then the **Trust Center Settings** button



Help keep your documents safe and your computer secure and healthy.

Security & more

Visit Office.com to learn more about protecting your privacy and security.

Microsoft Trustworthy Computing

Microsoft Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

4. Click the option you want. Options include the following:
   a. **Disable all macros without notification**: Click this option if you don't trust macros. All macros in documents and security alerts about macros are disabled. If there are documents with unsigned macros that you can trust, you can put those

documents into a trusted location. Documents in trusted locations are allowed to run without being checked by the Trust Center security system.

b. **Disable all macros with notification**: This is the default setting. Click this option if you want macros to be disabled, but you want to get security alerts if there are macros present. This way, you can choose when to enable those macros on a case by case basis.

c. **Disable all macros except digitally signed macros**: This setting is the same as the **Disable all macros with notification** option, except that if the macro is digitally signed by a trusted publisher, the macros can run if you have already trusted the publisher. If you have not trusted the publisher, you are notified. That way, you can choose to enable those signed macros or trust the publisher. All unsigned macros are disabled without notification.

d. **Enable all macros (not recommended, potentially dangerous code can be run)**: Click this option to allow all macros to be run. This setting makes your computer vulnerable to potentially malicious code and is not recommended.

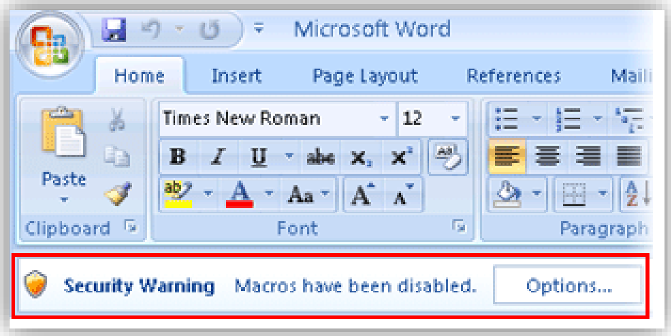
e. **Trust access to the VBA project object model**: This setting is for developers. It provides a security option for code that is written to automate an Office program. This is a per user and per application setting, and denies access by default. This makes it more difficult for unauthorized programs to build "self-replicating" code that can harm end-user systems.

The Trust Center and Macros (What to Expect)

Before enabling a macro in a document, the Trust Center checks for the following information:

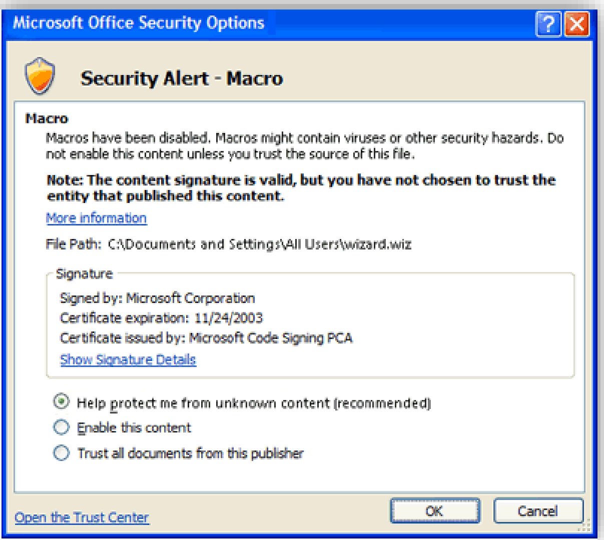
- The macro is signed by the developer with a digital signature
- The digital signature is valid
- This digital signature is current (not expired)
- Certificate associated with digital signature was issued by reputable certificate authority
- The developer who signed the macro is a trusted publisher

If the Trust Center detects a problem with any of these, the macro is disabled by default, and the Message Bar appears to notify you of a potentially unsafe macro.



Security Warning Macros have been disabled.

1. To enable macro, click **Options** on the Message Bar, and a security dialog box will open.
2. When the Security Options box appears, you can enable the macro or leave it disabled. You should only enable it if you are sure it is from a trustworthy source.



Security Alert - Macro

Macro

Macros have been disabled. Macros might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.

Note: The content signature is valid, but you have not chosen to trust the entity that published this content.

More information

File Path: C:\Documents and Settings\All Users\wizard.wiz

Signature

Signed by: Microsoft Corporation
Certificate expiration: 11/24/2003
Certificate issued by: Microsoft Code Signing PCA
Show Signature Details

● Help protect me from unknown content (recommended)
○ Enable this content
○ Trust all documents from this publisher

Open the Trust Center

3. Depending on the situation, the security dialog box describes the specific problem. The following is a list of possible problems as well as advice on actions to take in each case:
   a. Macro is not signed: Because the macro is not digitally signed, the identity off the macro publisher cannot be verified. Therefore, it is not possible to determine if the macro is safe or not.
   b. Advice: Before enabling unsigned macros, make sure it is from a trustworthy source. You can still work in your document even if the macro is not enabled.
   c. Macro signature is not trusted: The macro is potentially unsafe. The macro has been digitally signed and the signature is valid, but you have not chosen to trust the publisher who signed the macro.

Advice: You can explicitly trust a macro publisher by clicking **Trust all documents from this publisher** in the security dialog box. This option appears only if the signature is valid. Clicking this option adds the publisher to your Trusted Publishers list in the Trust Center.

d. **Macro signature is invalid**: The macro is potentially unsafe, because the macro has been digitally signed and the signature is invalid. **Advice**: It is recommended that you do NOT enable macros with invalid signatures. One possible reason the signature is invalid is that it may have been tampered with. For more info, see How to tell if a digital signature is trustworthy.

e. **Macro signature has expired**: The macro is potentially unsafe because it has been digitally signed and the signature has expired. **Advice**: Before enabling macros with expired signatures, make sure it is from a trustworthy source. If you have used this document in the past without any security issues, there is potentially less risk to enabling the macro.

Final Note

SECMON1 are available to review your macro security settings with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement macro security settings for your company.

Please feel free to visit our website at www.secmon1.com

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com