



Support / Excel / Excel 2007 Help and How-to / Macros

Change macro security settings in Excel

Applies to: Microsoft Office Excel 2007

In Microsoft Office Excel, you can change the macro security settings to control which macros run and under what circumstances when you open a workbook. For example, you might allow macros to run based on whether they are digitally signed by a trusted developer.

For more information about macro security settings in Microsoft Office documents, see [Enable or disable macros in Office documents](#).

In this article

- ↓ [Macro security settings and their effects](#)
- ↓ [Change macro security settings](#)
- ↓ [Using digital signatures](#)
- ↓ [Troubleshooting](#)

Macro security settings and their effects

The following list summarizes the various macro security settings. Under all settings, if antivirus software that works with 2007 Microsoft Office system is installed and the workbook contains macros, the workbook is scanned for known viruses before it is opened.

- **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 that contain unsigned macros that you do 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.
- **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.
- **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 macro 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.
- **Enable all macros (not recommended, potentially dangerous code can run)** Click this option to allow all macros to run. Using this setting makes your computer vulnerable to potentially malicious code and is not recommended.
- **Trust access to the VBA project object model** This setting is for developers and is used to deliberately lock out or allow programmatic access to the VBA object model from any Automation client. In other words, it provides a security option for code that is written to automate an Office program and programmatically manipulate the Microsoft Visual Basic for Applications (VBA) environment and object model. This is a per user and per application setting, and denies access by default. This security option makes it more difficult for unauthorized programs to build "self-replicating" code that can harm end-user systems. For any Automation client to be able to access the VBA object model programmatically, the user running the code must explicitly grant access. To turn on access, select the check box.

Change macro security settings

You can change macro security settings in the Trust Center, unless a system administrator in your organization has changed the default settings to prevent you from changing the settings.

1. On the **Developer** tab, in the **Code** group, click **Macro Security**.

TIP If the **Developer** tab is not displayed, click the **Microsoft Office**




Button, click **Excel Options**, and then in the **Popular** category, under

Top options for working with Excel, click **Show Developer tab in the Ribbon**.

- In the **Macro Settings** category, under **Macro Settings**, click the option that you want.

NOTE Any changes that you make in the **Macro Settings** category in Excel apply only to Excel and do not affect any other Microsoft Office program.

TIP You can also access the Trust Center in the **Excel Options** dialog box. Click

the **Microsoft Office Button** , and then click **Excel Options**. In the **Trust Center** category, click **Trust Center Settings**, and then click the **Macro Settings** category.

Using digital signatures

The 2007 Office release uses Microsoft Authenticode technology to enable macro creators to digitally sign a file or a macro project. The certificate that is used to create this signature confirms that the macro or document originated from the signer, and the signature confirms that the macro or document has not been altered.

After you install your digital certificate, you can sign files and macro projects.

OBTAINING A DIGITAL CERTIFICATE FOR SIGNING

You can obtain a digital certificate from a commercial certificate authority (CA), or from your internal security administrator or information technology (IT) professional.

To learn more about certificate authorities that offer services for Microsoft products, see the list of [Microsoft Root Certificate Program Members](#).

CREATING YOUR OWN DIGITAL CERTIFICATE FOR SELF-SIGNING

You can also create your own self-signing certificate by using the Selfcert.exe tool.

NOTE Because a digital certificate that you create isn't issued by a formal certificate authority, macro projects that are signed by using such a certificate are referred to as self-signed projects. Microsoft Office trusts a self-signed certificate only on a computer that has that certificate in your Personal Certificates store.

For more information about how to digitally sign a macro, see [Digitally sign a macro project](#).

Troubleshooting

I CAN'T CHANGE MY MACRO SECURITY SETTINGS

Some users may not be able to change Trust Center settings due to group security policies in their organizations. In such cases, you need to contact the IT administrator for your organization.

WHAT HAPPENED TO THE VERY HIGH, HIGH, MEDIUM, AND LOW SECURITY SETTINGS?

| EXCEL 2003 SETTING | EXCEL 2007 EQUIVALENT | ADDITIONAL INFORMATION |
|--------------------|---|--|
| Very High | Disable all macros without notification | <p>In Excel 2003, VBA macros can run only if the Trust all installed add-ins and templates option (in Excel 2003, the Trusted Publishers tab in the Security dialog box) is selected and the macros (whether signed or unsigned) are stored in a specific trusted folder on the user's hard disk.</p> <p>If not all of these conditions are met, VBA macros cannot run under the Very High security setting in Excel 2003.</p> |
| High | Disable all macros except digitally signed macros | <p>In Excel 2003, executable files (such as .exe or .com) must be signed by an acknowledged trusted source (that is, they must have a certificate of trust) in order to run. Otherwise, all executables associated with or embedded in documents are automatically disabled without warning the user when those documents are opened.</p> <p>By default, all Office 2003 programs are installed with macro security set to High.</p> |
| Medium | Disable all macros with notification | <p>In Excel 2003, users are prompted to enable or disable executables when a document is opened. This level requires the acceptance of a certificate</p> |

of trust for each executable, which is accepted by adding the certificate to a segment of the computer's Windows registry.

Subsequent requests to run a macro from a trusted source are automatically accepted (the executable runs without prompting the user).

| | | |
|-----|---|--|
| Low | Enable all macros (not recommended; potentially dangerous code can run) | In Excel 2003, all macros are run without restrictions. This security level does not protect against malicious programs, does not allow for acceptance of certificates of trust, and is not considered secure in general. This level is not recommended. |
|-----|---|--|

See [About macro security](#) to learn more about the security settings in Excel 2003 so that you can better understand the differences between the Office 2003 and Office 2007 macro security models.