ABOUT THIS DOCUMENT

Applies to Chronolator Version	3.5
Document version	3.5.02
Purpose	Describes Word Options and Microsoft Office Group Policy Administrative Templates that affect the ability to run macros, and thus the ability to run Chronolator.

MICROSOFT DOCUMENTATION

Microsoft describe the Group Policy Administrative Templates that pertain to Office 2016 in the article ***Plan security settings for VBA macros in Office 2016***, available from here:

https://technet.microsoft.com/en-us/library/ee857085%28v=office.16%29.aspx or http://tinyurl.com/zn5bs9d.

Office 2010 and 2013 use the same definitions, apart from ***Block macros from running in Office files from the Internet***, which is not directly relevant to Chronolator.

RECOMMENDATIONS

The Microsoft defaults allow a user to choose whether or not to run macros. If they choose to do so, macros will run successfully.

However, these defaults allow users to run *any* macro, with the risk that macro-borne viruses might infect their computer. Chronolator Version 3.5 macros are **digitally signed** by Berrick Computing Ltd, allowing you to set a more restrictive macro execution policy while still allowing Chronolator to run.

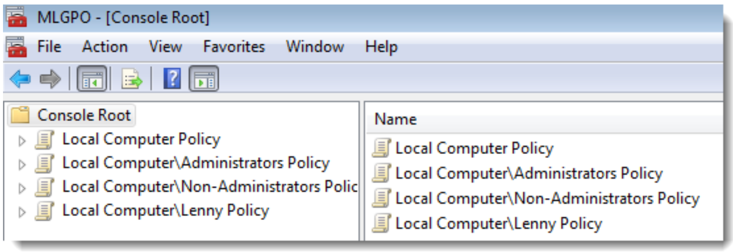
You can use Group Policy to enforce such a policy by setting `VBA Macro Notification Settings` to `Disable all except digitally signed macros`.[1]

Group Policy allows you to set a more restrictive level for most users and just allow your Chronolator users to run macros.

[1] WARNING! See the Microsoft documentation mentioned above. If any of your users use Access, this setting will prevent them opening unsigned Access databases..

A RESTRICTIVE POLICY EXAMPLE

Chronolator has been successfully tested using a Local Group Policy. The GP Management Console was set up with these Snap-ins:



Console Root
- Local Computer Policy
- Local Computer\Administrators Policy
- Local Computer\Non-Administrators Polic
- Local Computer\Lenny Policy

Name
- Local Computer Policy
- Local Computer\Administrators Policy
- Local Computer\Non-Administrators Policy
- Local Computer\Lenny Policy

Very restrictive policies were set at the **Local Computer Policy** level, and relaxed for an individual user called **Lenny**. The **Administrators** and **Non-Administrators** policies were not changed. Similar options are possible depending on how and whether you want to set site-wide policies (for example, in a Non-Administrators policy rather than for the Local Computer).

Policy	Template Path	Setting
Automation Security	**Local Computer Policy**\User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings	Enabled: Disable all macros by default
Disable VBA for Office applications	"	Enabled
Disable all Trust Bar notifications for security issues	"	Enabled
VBA Macro Notification Settings	**Local Computer Policy**\User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center	Enabled: Disable all without notification
Automation Security	**Local Computer\Lenny Policy**\ User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings	Enabled: Use application macro security level
Disable VBA for Office applications	"	Disabled
Disable all Trust Bar notifications for security issues	"	Disabled
VBA Macro Notification Settings	**Local Computer\Lenny Policy**\ User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center	Enabled: Disable all except digitally signed macros

BERRICK COMPUTING AS A TRUSTED PUBLISHER

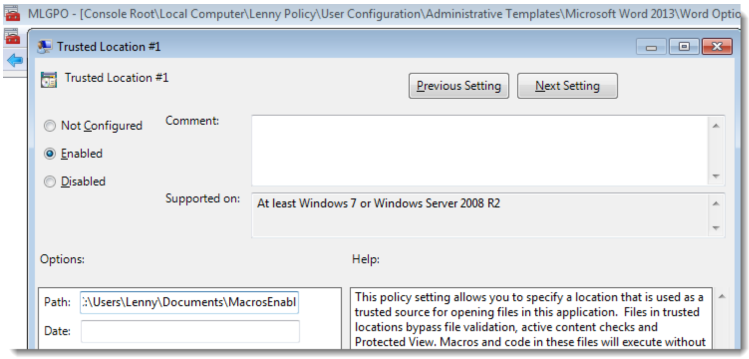
Berrick Computing does not *need* to be a **Trusted Publisher**, but being one makes things more convenient for users by removing the need for them to enable macros on a case-by-case basis.

Users can usually add Berrick Computing to their personal Trusted Publishers list by using standard Word features when opening a Chronolator Document. The Chronolator documentation tells them how to do this.

Some organisations might not want users to have this capability, and can use Group Policy to prevent it. If that applies to your organisation, and you want to add Berrick Computing to users' Trusted Publishers lists 'by hand', please contact berrick@berrick-computing.co.uk for a copy of the digital certificate .

USING A TRUSTED LOCATION

Another way to allow an individual user to run macros is to give them a Trusted Location in Group Policy path **Local Computer*username* Policy\ User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center\Trusted Locations.**



MLGPO - [Console Root\Local Computer\Lenny Policy\User Configuration\Administrative Templates\Microsoft Word 2013\Word Optio

Trusted Location #1

Trusted Location #1

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 7 or Windows Server 2008 R2

Options:

Path: :\Users\Lenny\Documents\MacrosEnabl

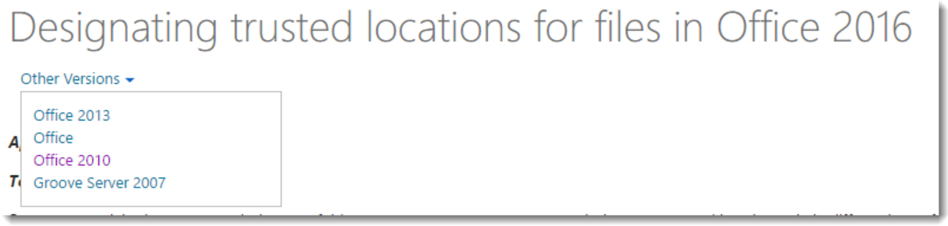
Date:

Help:

This policy setting allows you to specify a location that is used as a trusted source for opening files in this application. Files in trusted locations bypass file validation, active content checks and Protected View. Macros and code in these files will execute without

This option is less convenient than the one above in that it forces users to store data in a particular location. It is arguably less secure than setting `Disable all except digitally signed macros` in that if a malicious document were saved in that location it would be allowed to run macros without notification.

For Microsoft's advice on securing Trusted Locations, see https://technet.microsoft.com/en-us/library/cc179039(v=office.16).aspx or http://tinyurl.com/zvavbzk. The article is for Word 2016, but at the time of writing this document it has a link near the top to similar information for earlier versions:



Designating trusted locations for files in Office 2016

SETTINGS THAT PREVENT CHRONOLATOR FROM RUNNING SUCCESSULLY

- Not surprisingly, disabling VBA entirely by setting `Disable VBA for Office applications` will stop Chronolator running.
- Setting `Automation security` to `Disable macros by default` will allow macros to run at first (assuming the user or IT policy has allowed them to do so), but Chronolator will fail when one Chronolator Document attempts to open another one. This can happen when creating a new Internal Chronology or Composite Chronology from the Online Workbench, and when importing a chronology document into a Composite Chronology.

  Note that the `Automation security` setting overrides any Trusted Locations that may be defined.