ABOUT THIS DOCUMENT

Applies to Chronolator Versions	3.4 and higher
Document version	5.0.1
Purpose	Describes Microsoft Office Group Policy settings 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 and later versions in the article ***Plan security settings for VBA macros in Office 2016***, available from here:

https://docs.microsoft.com/en-gb/DeployOffice/security/plan-security-settings-for-vba-macros-in-office or https://tinyurl.com/officeVBA.

Office 2013 uses the same definitions, apart from ***Block macros from running in Office files from the Internet***.

RECOMMENDATIONS

The Microsoft defaults allow a user to choose whether or not to run macros when they open a document. 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. Since Version 3.4, Chronolator macros have been **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]

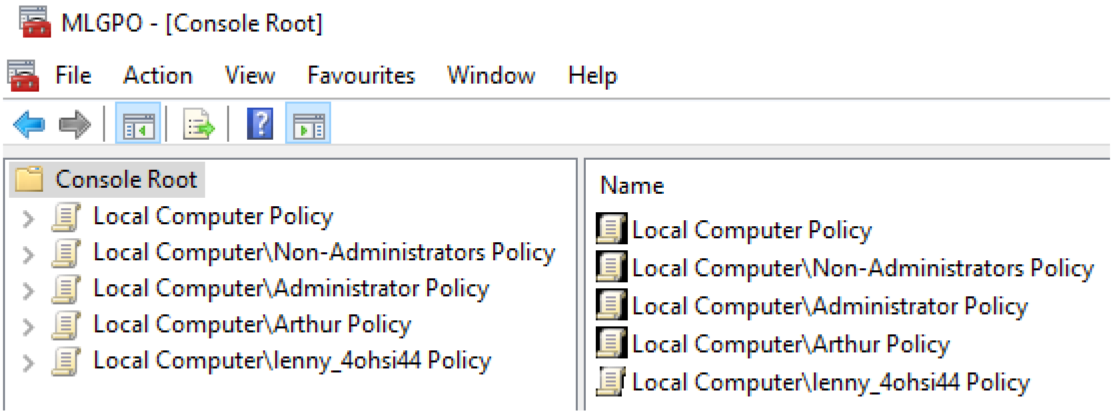
Group Policy allows you to set a more restrictive level for most users and allow only your Chronolator users to run macros.

[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 POLICY EXAMPLE

Chronolator has been successfully tested using the Local Group Policy described below.

The GP Management Console was set up with these Snap-ins:



MLGPO - [Console Root]

Console Root
- Local Computer Policy
- Local Computer\Non-Administrators Policy
- Local Computer\Administrator Policy
- Local Computer\Arthur Policy
- Local Computer\lenny_4ohsi44 Policy

Name
- Local Computer Policy
- Local Computer\Non-Administrators Policy
- Local Computer\Administrator Policy
- Local Computer\Arthur Policy
- Local Computer\lenny_4ohsi44 Policy

Very restrictive policies were set at the **Local Computer Policy** level, and relaxed for an individual user called **Lenny_4ohsi44**. The **Non-Administrators** and **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 the Local Computer Policy).

RESTRICTIVE DEFAULT POLICIES FOR ALL USERS

Policy	Template Path	Setting
Automation Security	**Local Computer Policy**\User Configuration\Administrative Templates\Microsoft *Office* 2016\Security Settings[2]"	Enabled: Disable all macros by default
Disable all Trust Bar notifications for security issues	"	Enabled
Disable VBA for Office applications	"	Enabled
Block macros from running in Office files from the Internet	**Local Computer Policy**\User Configuration\Administrative Templates\Microsoft *Word* 2016\Word Options\Security\Trust Center	Enabled
VBA Macro Notification Settings	"	Enabled: Disable all without notification

[2] N.B. This is a **User Configuration** setting. If set in **Computer Configuration** it cannot be overridden for individual users

RELAXED POLICIES FOR A CHRONOLATOR USER

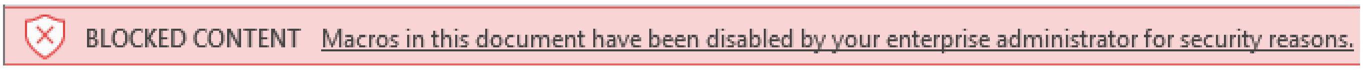
Policy	Template Path	Setting
Automation Security	**Local Computer\Lenny_4ohsi44 Policy**\ User Configuration\Administrative Templates\Microsoft *Office* 2016\Security Settings "	Enabled: Use application macro security level
Disable all Trust Bar notifications for security issues	"	Disabled
Disable VBA for Office applications	"	Disabled
Block macros from running in Office files from the Internet	**Local Computer\Lenny_4ohsi44 Policy**\ User Configuration\Administrative Templates\Microsoft *Word* 2016\Word Options\Security\Trust Center	See the note below this table
VBA Macro Notification Settings	"	Enabled: Disable all except digitally signed macros

Note re: user relaxation policy: **Block macros from running in Office files from the Internet**

Chronolator files are sometimes downloaded from the Internet:

- New customers download the software from www.chronolator.com
- Some existing customers use a web site to exchange Chronolator Documents

When macros are blocked, the Message Bar shows this:



BLOCKED CONTENT Macros in this document have been disabled by your enterprise administrator for security reasons.

To prevent this, you could set **Block macros from running in Office files from the Internet** to **Disabled** in the user relaxation policies. While this is a convenient option, it does still leave the loophole that downloaded malicious files can run if they are digitally signed.

The most secure option is not to configure this setting here and thus allow the global restriction to take effect. If you choose to do this, you or your users must make Berrick Computing a **Trusted Publisher**, or move the Chronolator files to a **Trusted Location.**

BERRICK COMPUTING AS A TRUSTED PUBLISHER

Berrick Computing does not *need* to be a **Trusted Publisher** (except in the circumstances just described), 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.**

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://docs.microsoft.com/en-gb/DeployOffice/security/plan-security-settings-for-vba-macros-in-office or https://tinyurl.com/officeTrustedLocations.

SETTINGS THAT PREVENT CHRONOLATOR FROM RUNNING SUCCESSULLY

- Disabling VBA entirely by setting `Disable VBA for Office applications` in the **Computer Configuration** policy will stop Chronolator running, regardless of any user policy.
- 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.