DocumentsAntiExploit tool.

Important remarks.

The home users should avoid installing MS Office and Adobe Acrobat Reader, except when it is necessary.
These applications can be fully protected only in theory, because the more protection, the greater the chances to see some documents unreadable.
Generally, it is recommendable to use online services or Universal Applications from Microsoft Store (**if they use AppContainer**), for managing documents (Office Online, Google Drive, Word Mobile, Excel Mobile, PowerPoint Mobile, Xodo PDF, Adobe Reader Touch, etc.).

Such popular applications like Libre Office, WPS Office, or SoftMaker Office are also the better choice, but they are not as safe as the above solutions. For compatibility reasons, some active content of documents can be still functional in these applications.

Anyway, some users have no choice and are obliged to use Acrobat Reader or MS Office. So, what can they do to provide enhanced security?

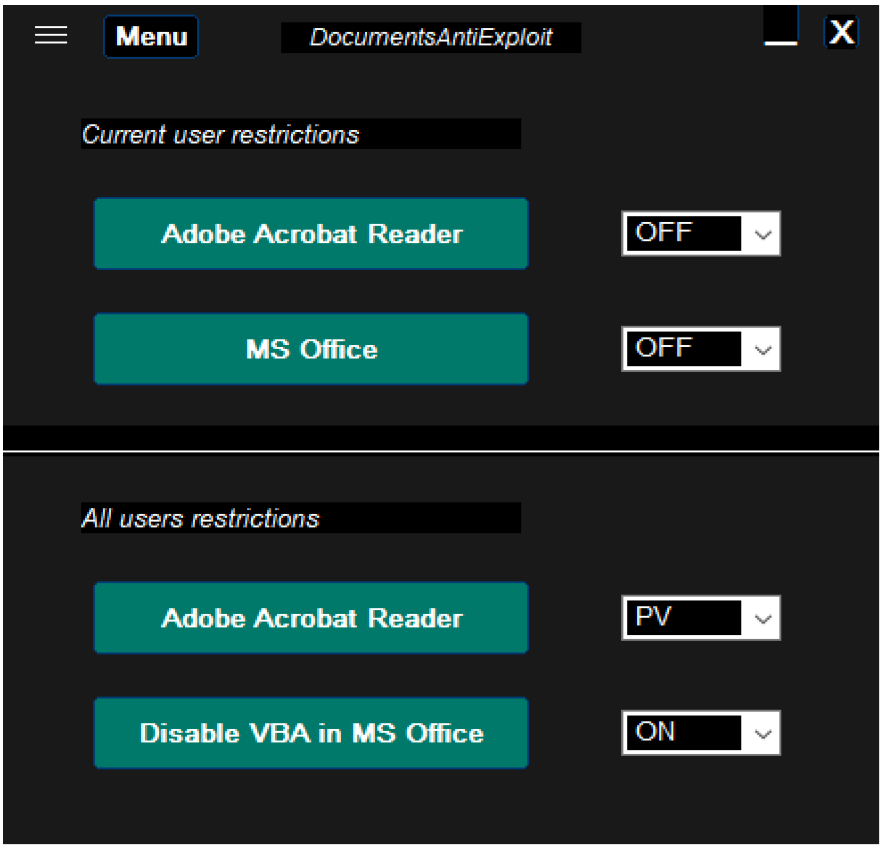
MS Office 2007 and newer versions provide not so bad default protection against weaponized office documents, but the user has to avoid allowing the active content (macros, OLE, DDE, ActiveX, etc.). That is hardly possible for inexperienced users, who usually do not understand the security alerts.

On Windows 8+ it is recommendable to install Adobe Acrobat Reader DC (from the year 2019 at least), because of the AppContainer feature which can mitigate many dangerous actions.

DocumentsAntiExploit tool is a companion utility to Simple Windows Hardening (and Hard_Configurator). It can be used to prevent exploiting the system via MS Office and Adobe Acrobat Reader applications, when opening the weaponized documents.

The main application window is divided into two parts.

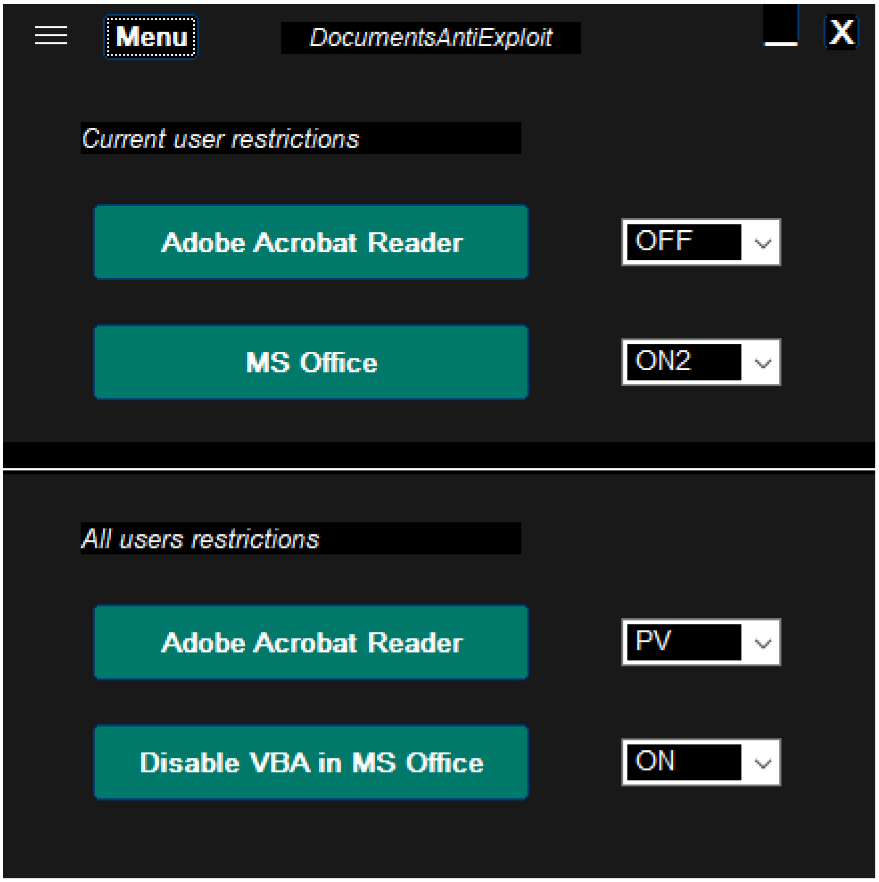
- The upper part includes settings for the current user. They will not apply to other users.
- The lower part includes settings for all users - these settings can be also changed via Hard_Configurator. For example, the 'Adobe + VBA' setting in H_C will look in the DocumentsAntiExploit window as follows:



The above settings are recommendable for users who use well updated Windows 10/11 with **Microsoft Defender** as primary Antivirus, installed MS Office **desktop versions**, installed Adobe Acrobat Reader **DC**, and applied ConfigureDefender **HIGH** Protection Level.

Otherwise, some additional hardening is required by applying restrictions from the upper part of the application window (Current user restrictions). These restrictions are limited to the particular user account. So, they have to be configured separately for each user account.

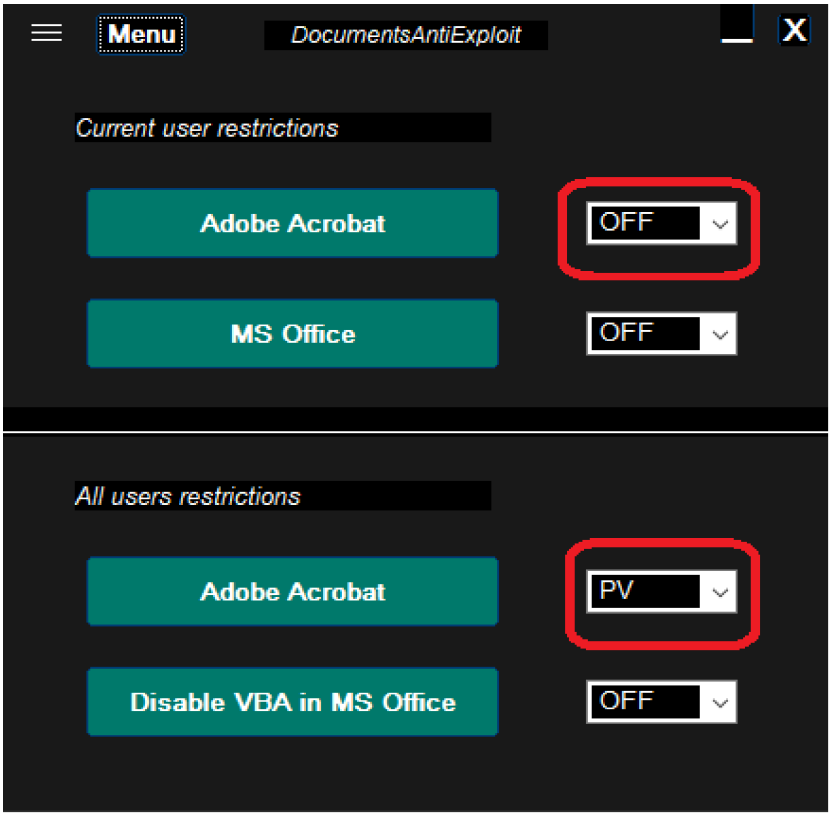
Such settings are also required when non-desktop MS Office (**Universal Windows Platform apps**) are installed - they must be restricted via **<MS Office> = ON2** setting. The ON2 setting works both for desktop and UWP versions and ON1 setting works only for desktop versions of MS Office.

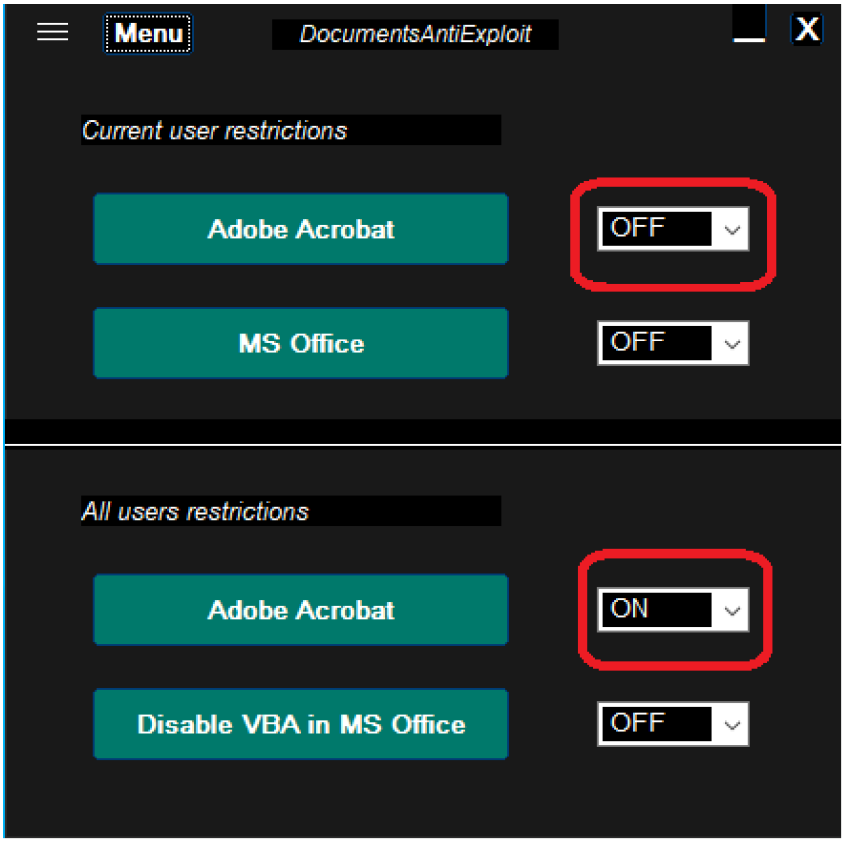


Available options for Adobe Acrobat.

For Adobe Reader, the behavior of 'Current user restrictions' can depend on 'All users restrictions'. Here are some interesting configurations:

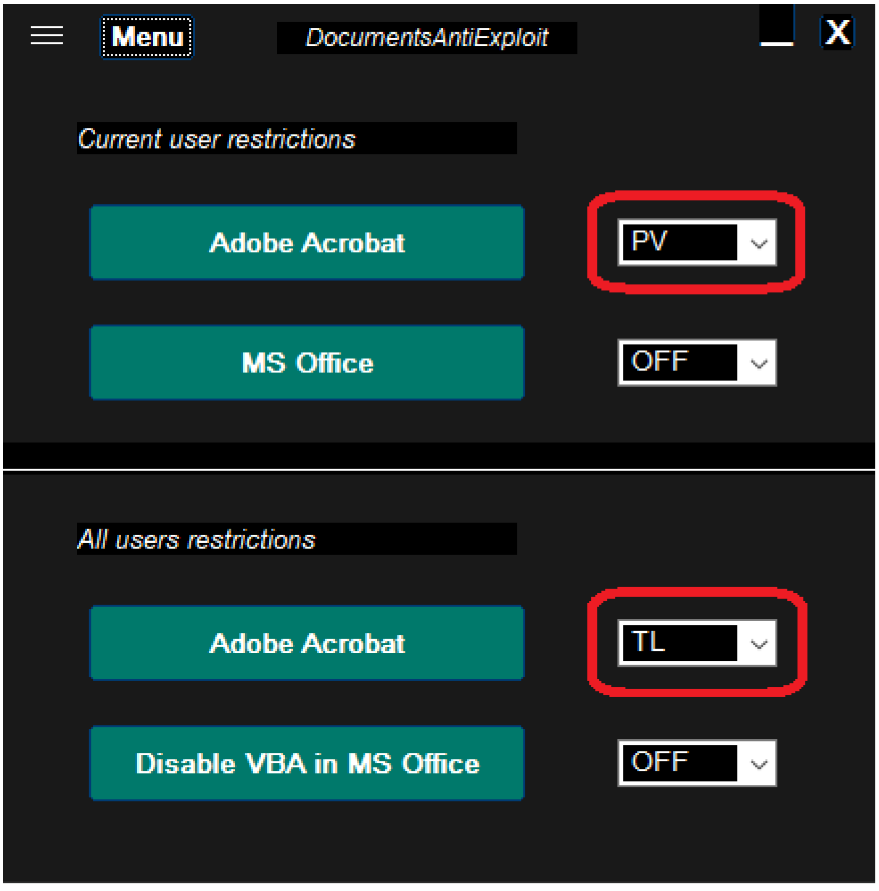
1. **Adobe Acrobat: OFF + PV** and **OFF + ON**

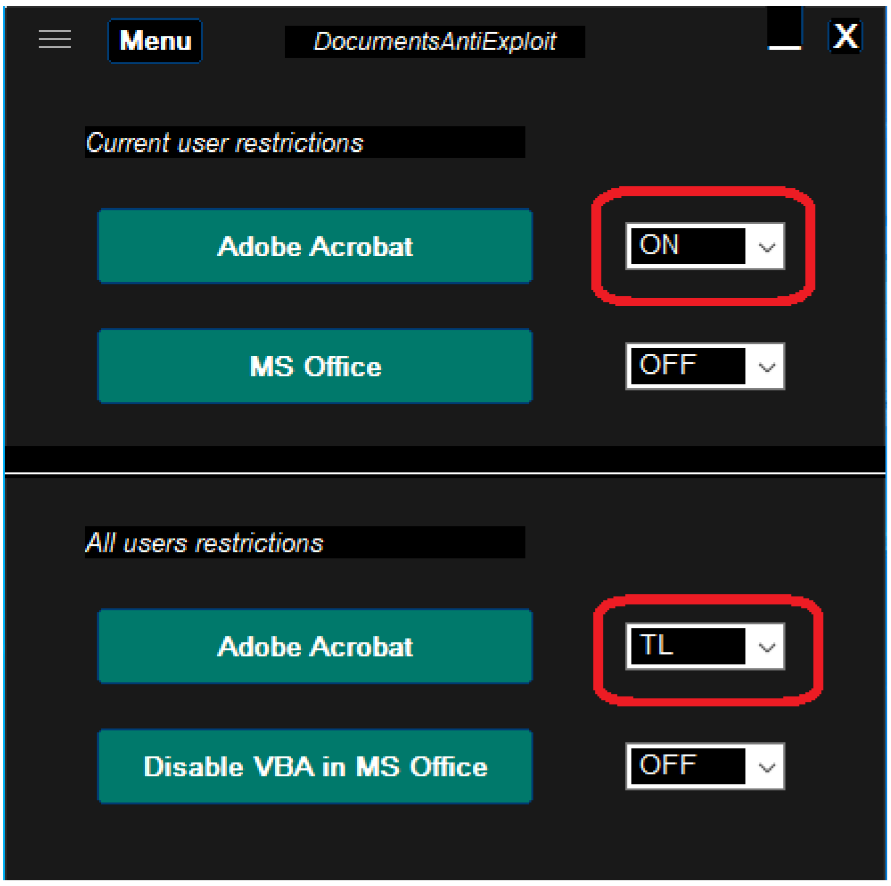




The difference between the setups **OFF + PV** and **OFF + ON**, is that the first setup allows opening URLs embedded in the documents, and the second does not.
PDF documents are opened in Protected View, so most of Adobe Acrobat features are disabled.
If the user would choose to use <Enable All Features> on the 'Yellow Bar', then the default restrictions are enabled and also some additional system-wide restrictions for JavaScript, 3D content, embedded attachments, external applications, PDF handler switching, trusted websites, and trusted folders.
These restrictions cannot be changed from Adobe Acrobat applications via the 'Preferences .... ' option.
The documents are not added to 'Privileged Locations' even after using <Enable All Features>.

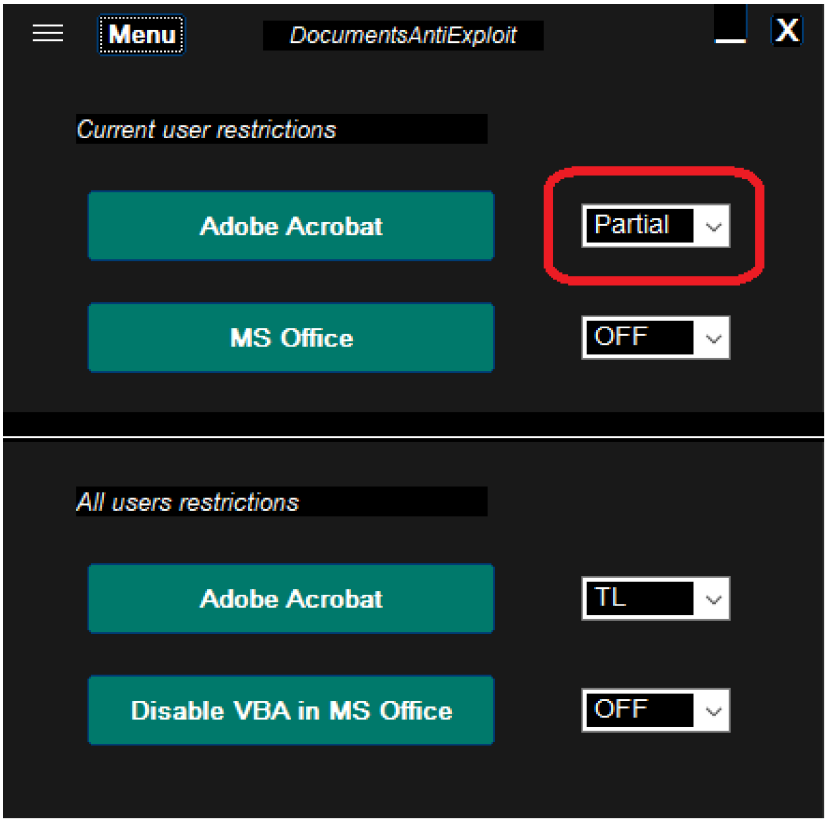
2. Adobe Acrobat: **PV + TL** and **ON + TL**





The system-wide **TL** setting is usually applied together with some 'Current user restrictions' of Adobe Acrobat. It prevents adding the documents to 'Privileged Locations'.
The difference between the setups **PV + TL** and **ON + TL**, is that the first setup allows opening URLs embedded in the documents, and the second does not.
The above restrictions are similar to the restrictions from point 1, but now most of them apply only to the current user and they can be modified via the Adobe Acrobat 'Preferences .... ' option (except switching PDF handler). PDF documents are opened in Protected View, so most of the Adobe Acrobat features are disabled.
If the user would choose to use <Enable All Features> on the 'Yellow Bar', then the default restrictions are enabled, and also some additional non-system-wide restrictions for JavaScript, 3D content, embedded attachments, external applications, and trusted websites.
The JavaScript restrictions for the particular document can be removed by choosing the option from the 'Yellow Bar'.

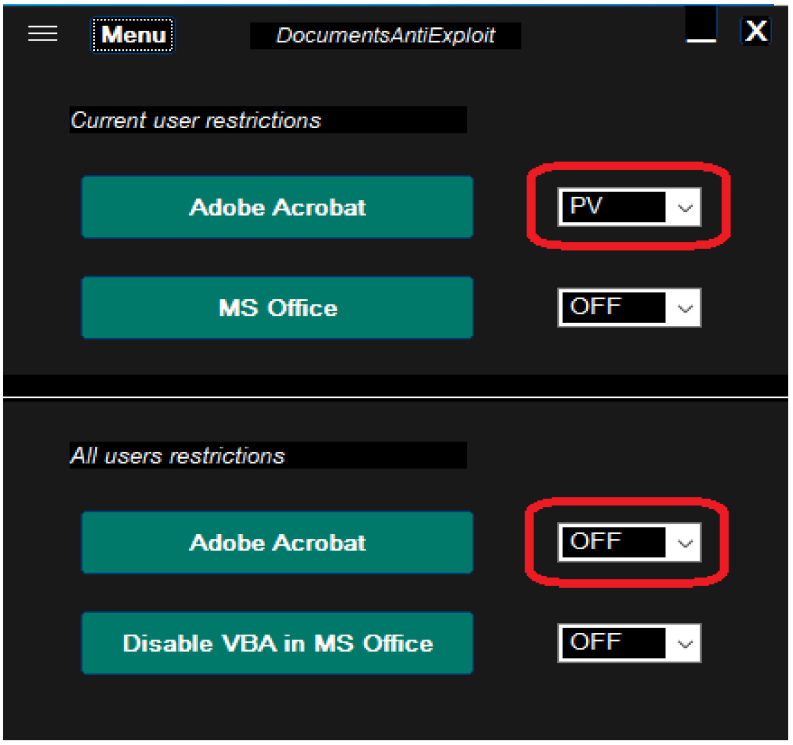
The **ON + TL** is more appropriate for casual users.
The setups with a **TL** setting can be convenient for users who would like to change the settings a little via the Adobe Acrobat 'Preferences .... ' option and apply custom restrictions.
After making such a custom setup the Adobe Acrobat setting in the 'Current user restrictions' section changes to 'Partial', for example:



3. Adobe Acrobat: **PV+ OFF**

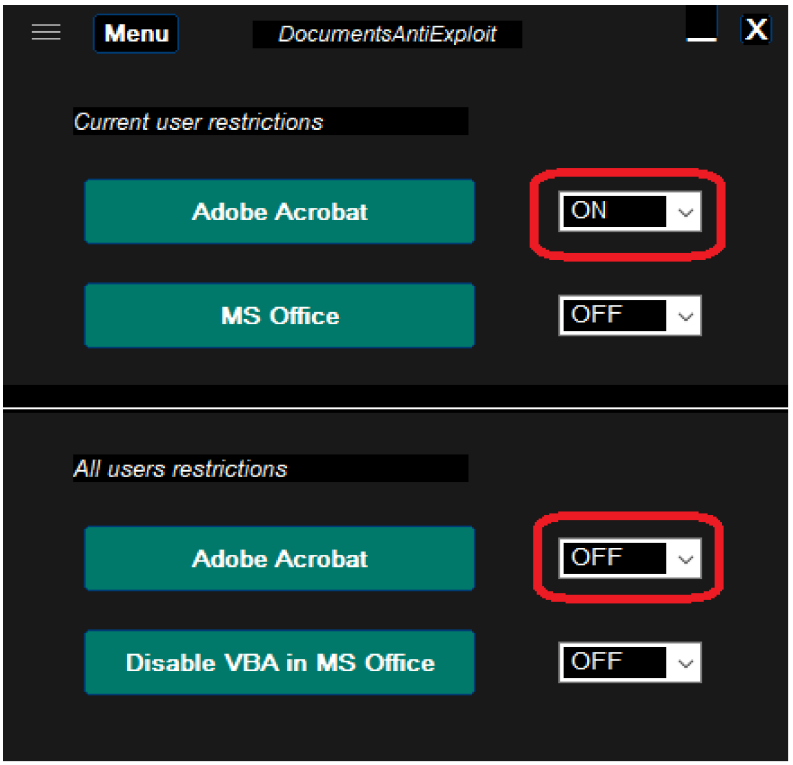
These settings are similar to the setup OFF + PV, but there are two important differences:

1. All settings are now applied only to the current user.
2. Documents are opened in Protected View, but after using <Enable All Features> from the 'Yellow Bar', the documents are added to 'Privileged Locations' (Trusted Locations), so documents are opened with Adobe Acrobat default settings, even if some non-default settings were included in the setup.



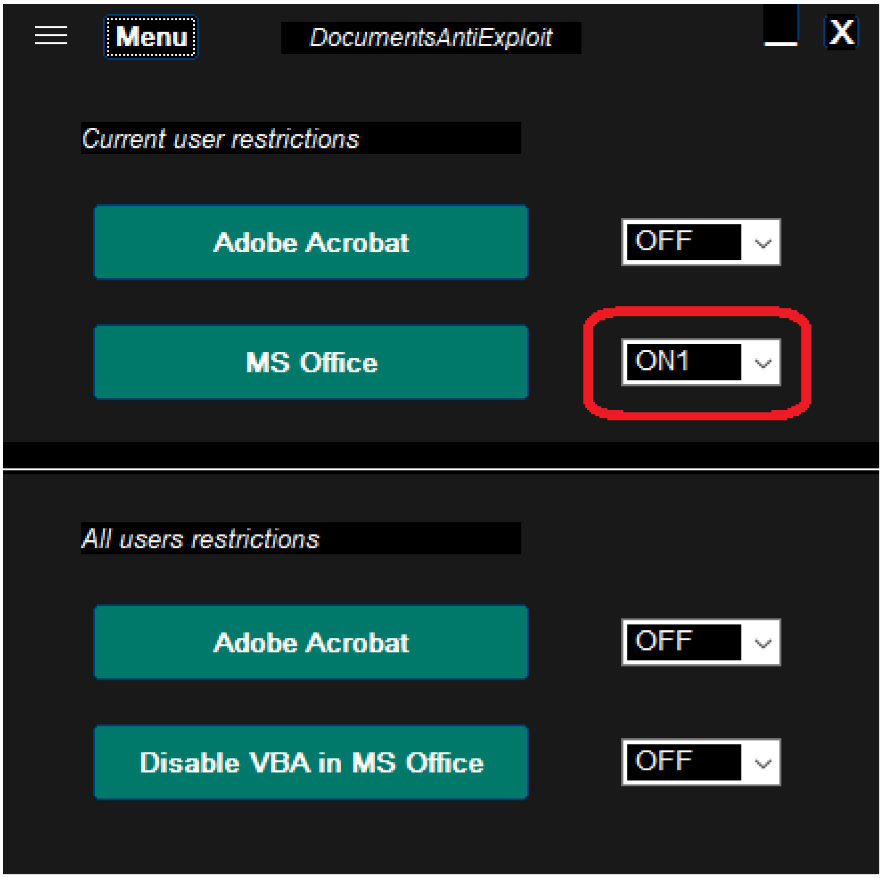
This setup can be used by responsible and cautious users, who can use the <Enable All Features> option only for known safe documents.

4. Adobe Acrobat: **ON + OFF**



This setup is not recommendable. It is similar to the PV + OFF setup from the previous example, but URLs embedded in documents are blocked. This is not a good combination, because the OFF setting in the 'All users restrictions' can be recommendable only for responsible and cautious users, so blocking URLs is not necessary.

Available options for MS Office.



The **<MS Office>** options **ON1** and **ON2** in the upper part of the Document-sAntiExploit window can apply the MS Office **restrictions to the current user** (valid up to MS Office 2021):

- Disabled Macros in MS Office XP and MS Office 2003+ (Word, Excel, PowerPoint, Access, Publisher, Outlook).
- Disabled Access to Visual Basic Object Model (VBOM) in MS Office 2007+ (Access, Excel, PowerPoint, and Word).

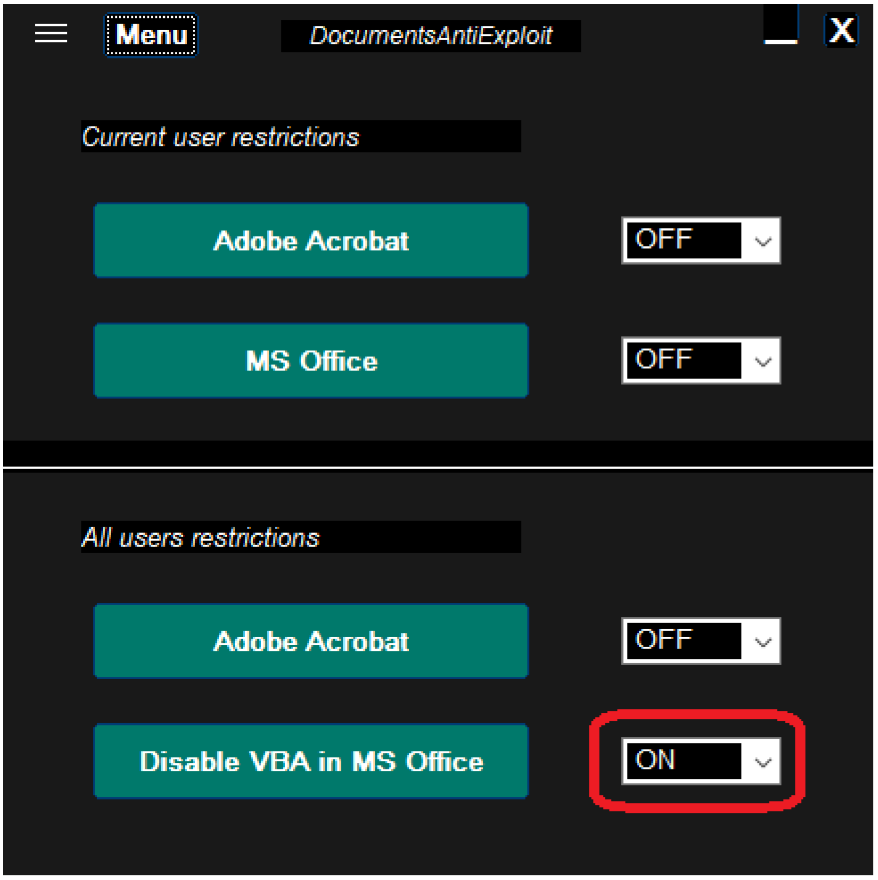
- Disabled DDE in Word 2007+ (requires Windows Updates pushed in January 2018, see Microsoft Security Advisory ADV170021).
- Disabled auto-update for any linked fields (including DDE and OLE) in Word 2007+, Excel 2007+, Outlook 2007+, One Note 2013+.
- Disabled ActiveX in MS Office 2007+.
- Disabled OLE in MS Office 2007+ (Word, Excel, PowerPoint).
- Disabled 'Run Programs' option for action buttons in PowerPoint 2007+.
- Disabled automatic download of linked images in PowerPoint 2007+.
- Disabled TrustBar notifications in MS Office 2007+ .

The meaning of available settings:

- ON2 - the restrictions apply via administrator policies and override (but do not overwrite) the native MS Office settings. The ON2 policies may not be visible in the Trust Center of MS Office applications.
- OFF2 - only the administrator policies are removed, and all other restrictions are not changed. This setting is not related to any predefined restriction setup.
- ON1 - the administrator policies are removed and the restrictions are applied via the native MS Office settings. Please note, that ON1 and OFF work only for MS Office desktop versions, which are installed by default in the 'Program Files' or 'Program Files (x86)' folder. They will not work for Mobile versions (Windows Universal Platform versions).
- OFF - the administrator policies are removed. The default values of the native MS Office settings are applied.
- Partial - the restrictions were configured via the external program and do not match the predefined OFF/ON/ON2 restriction setup. For example, after changing the ON1 settings within MS Word application (via Trust Center), the new settings will be seen as Partial in DocumentsAntiExploit.

Although ON1 and ON2 settings can trigger the same restrictions, only ON1 settings can be changed from within MS Office applications via Trust Center. Switching between ON2 and OFF2 can be convenient, because the user can switch between the locked/secure ON2 setup and the favorite setup (configurable within MS Office applications).

<Disable VBA in MS Office> option in the lower part of the DocumentsAntiExploit window can prevent MS Office from using the VBA interpreter. This restriction + Microsoft Defender (ConfigureDefender HIGH), can be used when the <MS Office> settings from the upper part of the DocumentsAntiExploit window are too restrictive.



Closing remarks.

DocumentsAntiExploit tool is a portable application, but before removing it from the computer, the user should apply the OFF setting for all available options. This should be done for all user accounts (for the current user and for other users). If not, then a few settings can be locked (non-configurable) in MS Office and Adobe Acrobat Reader.

@Andy Ful