

**SRG/STIG Applicability Guide**

**and**

**Applicable SRG/STIG Collection Tool**

**READ ME FIRST**

**Version 1 Release 3**

**June 2015**

Developed by DISA for the DoD

Table of Contents

Page

[1. Warnings 1](#_Toc421607900)

[Mobile Code WARNING 1](#_Toc421607901)

[Document Variable WARNING 1](#_Toc421607902)

[Document Opening / Activation Delay WARNING 1](#_Toc421607903)

[2. Use/installation and Distribution 2](#_Toc421607904)

[2.1 Use/Installation 2](#_Toc421607905)

[2.2 Distribution 2](#_Toc421607906)

[3. Tool Automation Enablement 3](#_Toc421607907)

[3.1 Macro Enablement in Word 2010 3](#_Toc421607908)

[3.2 Macro Enablement in Word 2007 6](#_Toc421607909)

[4. Known problems 8](#_Toc421607910)

[4.1 Version of Word 8](#_Toc421607911)

[4.2 Installation of .zip 8](#_Toc421607912)

[4.3 Installation Path 8](#_Toc421607913)

[4.4 Trust Center Settings 9](#_Toc421607914)

[4.5 Microsoft Patch MS14-082 / KB2553154 10](#_Toc421607915)

[5. Document Revisions 12](#_Toc421607916)

# Warnings

Mobile Code WARNING

The SRG/STIG Applicability Guide and Tool document contains Signed Mobile Code in the form of Visual Basic for Applications (VBA) macro code and ActiveX controls which provides the tool automation elements. Some security systems might flag these macros as a security risk when transferring the file in some manner. Please note that this code works solely within the folder housing the document and does not access the system on which it is run except to retrieve the current date and to create its output documents. SRG/STIG Collection documents (the Guide/Tool output) along with associated .ini files are saved to the “Output” folder within the folder containing the Guide/Tool document. These output documents do not contain macros or other active content besides hyperlinks that enable the user to download the selected SRGs and STIGs and document bookmarks used in the collection development process. The macro code has been signed using a DoD PKI code signing certificate which should validate as being signed by “CS.DISA RE71.DISA080006”. If this is not the case, the macros in this document should not be trusted or enabled. More information regarding the macros and their signature validation and activation can be found in “Tool Automation Enablement” below.

Document Variable WARNING

The automation in SRG/STIG Applicability Guide and Tool document makes use of document variables to store variable values that would otherwise be transient between macro sessions. These variables are integral to making the automation work. These are only created when the macros are enabled. They are stored within the Guide/Tool document if it is saved. Please note: some security systems might flag these variables as a security risk when transferring the file in some manner. These variables contain no sensitive information. Additionally, the values for some of these document variables is saved to a .ini file associated with each SRG/STIG

Document Opening / Activation Delay WARNING

The automation in SRG/STIG Applicability Guide and Tool document consists of many ActiveX controls and many lines of VBA macro code. Due to this and the large size of the document, there is a delay of approximately two (2) minutes while the automation is enabled. (Your time may vary.) During this time, Word may show the “Microsoft Word (Not Responding)” message in the window title or it may look like it has crashed. This is not the case unless the time noted above has been greatly exceeded. Once the automation is activated a dialogue box will be displayed indicating the Tool has been activated and reset.

NOTE: if the code signing certificate is trusted as noted in “Tool Automation Enablement” below, this activation delay will be added to the time it takes to open the Guide/Tool document and the behavior may be the same. Otherwise, the document will open and present the windows shown below. The activation delay will then be incurred as the automation is activated.

# Use/installation and Distribution

## Use/Installation

To use/install the SRG/STIG Guide and Tool, UNZIP THE DISTRIBUTION PACKAGE TO A FOLDER in a convenient location on your workstation. DO NOT double-click on the .zip file. The tool has the capability to determine its location so that its output can be generated successfully. That said, the GUIDE & TOOL…docm file requires that the “Resource” and “Output” folders be located within the same folder as the document. DO NOT separate these.

IMPORTANT NOTE: The SRG/STIG Guide and Tool CANNOT BE RUN from within an explorer window that opens when double clicking on the .zip file. The folder inside the .zip file must be extracted then opened. If an archive application such as WinZip is not installed, you must right-click on the .zip file and select “Extract All…” from the context menu.

## Distribution

The files in the .zip distribution package mist be kept together when redistributing the GUIDE & TOOL. The following files may be distributed separately:

* ABOUT - SRG, CCI, STIGs, Checklists, Tools, & Automation.docx
* HOW TO VIEW - SRGs and STIGs.docx

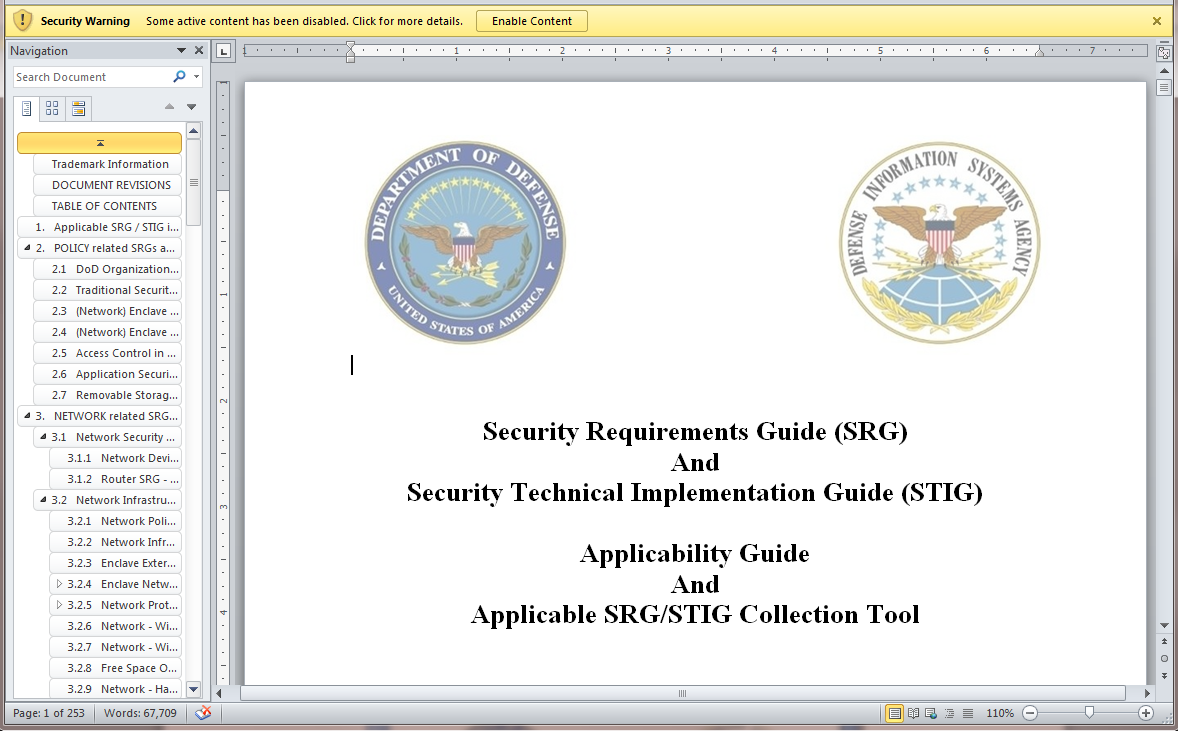
# Tool Automation Enablement

The document contains Visual Basic for Applications macro code to provide the automation elements of the tool. The macro code must be enabled for it to fulfill its function. The macro code has been signed using a DoD PKI code signing certificate and will remain signed unless modified. Operating the automation does not affect the signing. The automation will not function if MS Word’s macro security level is set too high. The macro code was developed in MS Word 2007 and will operate on a system with the trust center macro settings set to “Disable all macros with notification”. This permits the user to decide whether or not to enable the active content and use the macros. Under this security setting, a security warning will appear above the ruler but under the MS Word ribbon when the document is first loaded. This warning will contain a message that states “Some active content has been disabled” accompanied by an “Options” or “Enable Content” button which must be clicked to enable the automation. Certificate validation and macro enablement is slightly different depending on the version of Word in use. The following sections show the process for Word 2010 and 2007.

## Macro Enablement in Word 2010

DO NOT CLICK (See CAUTION below)

The Word 2010 security warning shows as follows:



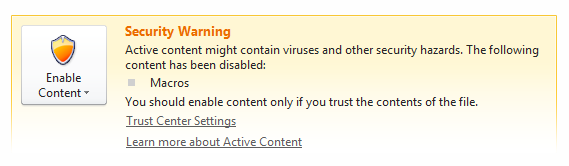
CLICK (See CAUTION below)

CAUTION: It is highly recommended that the user validate the code signing certificate before enabling macros on first use. DO NOT click “Enable Content” button before verification. Clicking the “Enable Content” button at this point will enable the macros and add the document to the “trusted document” list without user verification of the code signing certificate. This allows the document to be opened on subsequent occasions without receiving the security warning. Once the document is trusted in this manner, the only way to validate the certificate is as described below is to access it through the VBA editor’s tools/Digital Signature feature.

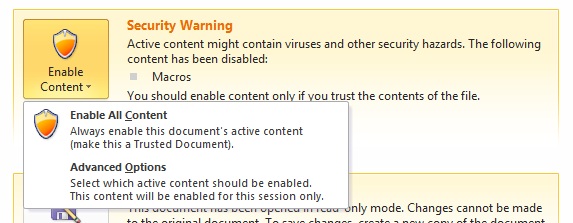
To verify the code signing certificate (highly recommended) follow the steps below:

Click on the text “Some active content has been disabled. Click for more details”.

The “File” tab will open showing the following:

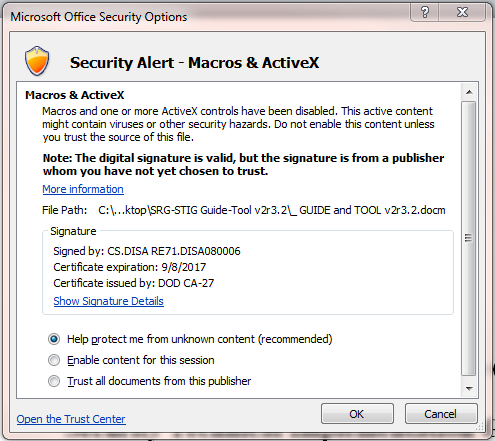


Clicking the “Enable Content” button displays the following:



Click “Advanced Options” to display the certificate information:

Continued on Next page…



The user should validate that the dialogue box indicates that the document is signed, that the certificate is valid, and that the code is signed by “CS.DISA RE71.DISA080006”.

The user must then select the “Enable this content” radio button and click OK to permit the automation to function while the document remains open.

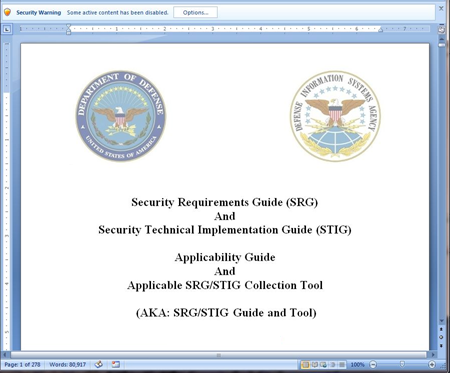
Optionally the user could select the radio button (if present) to “Trust all documents from this publisher” (recommended). Once validated and this certificate is trusted in this manner, the security warning will no longer be displayed when the document is opened or when subsequent documents signed with the trusted certificate are opened.

If need be, this trust can be eliminated by deleting the certificate from the Trusted Publishers list under Word Options/Trust Center/Trust Center Settings/Trusted Publishers.

NOTE: See “Document Opening / Activation Delay WARNING” above.

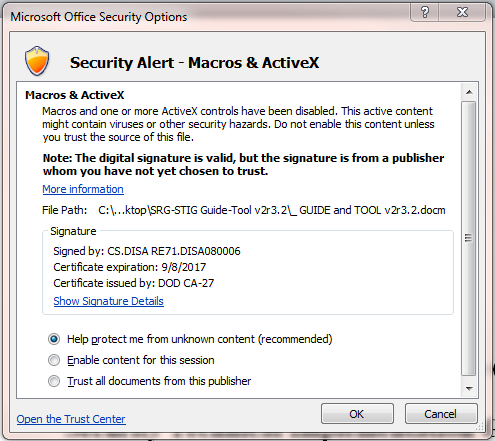
## Macro Enablement in Word 2007

The Word 2007 security warning shows as follows:



Continued on Next page…

Clicking this button should display a dialogue box similar to the following:



The user should validate that the dialogue box indicates that the document is signed, that the certificate is valid, and that the code is signed by “CS.DISA RE71.DISA080006”.

The user must then select the “Enable this content” radio button and click OK to permit the automation to function while the document remains open.

Optionally the user could select the radio button (if present) to “Trust all documents from this publisher” (recommended). Once validated and this certificate is trusted in this manner, the security warning will no longer be displayed when the document is opened or when subsequent documents signed with the trusted certificate are opened.

If need be, this trust can be eliminated by deleting the certificate from the Trusted Publishers list under Word Options/Trust Center/Trust Center Settings/Trusted Publishers.

NOTE: See “Document Opening / Activation Delay WARNING” above.

# Known problems

There are known issues that can prevent the tool from executing and some may cause the document to not open correctly. These are as follows:

## Version of Word

The version of Word that the SRG/STIG Guide and Tool is operated under can have an effect on its operation.

The SRG/STIG Guide and Tool was developed initially under Word 2007 then converted and tested under Word 2010. Development is continuing under Word 2010. The tool was not tested under any newer version of Word except by a user that has Office 2013. Initially the Tool could not add to (edit) the initially created collection document.

**Symptoms:** The collection document is created but the following error is displayed:

"Run-time error '6124':

You are not allowed to edit this selection because it is protected."

**Resolution:** This issue has been corrected by adding code to determine the version of Word and adjust accordingly.

## Installation of .zip

Do not attempt to execute the Tool portion of the SRG/STIG Guide and Tool from an explorer window that is opened by double clicking on the .zip file. This causes “File not Found” errors similar to the following:

"Runtime error '5174':

This file could not be found. ("C:\...\SRG-STIG Collection TEMPLATE...")

The Tool portion of the SRG/STIG Guide and Tool will not work unless the files and folders within the zipped distribution (.zip) file are extracted to folder in a convenient location on the hard drive. Users can be confused by Windows if they double click on the .zip file if there is no other archival application installed such as WinZIP. This is because the windows default behavior will open a .zip file in a windows explorer window that looks like a regular folder would look. As such the path to the collection template is not navigable by the tool macros. Therefore, if an application such as WinZip is not installed, the user must right click on the .zip file and select “Extract All…” from the context menu. If WinZIP is installed, then right click on the .zip file and select “WinZIP/Extract to Folder Path\Folder” from the context menu. In either case, accept the default folder name which will be that of the .zip file and the path to it.

## Installation Path

The path to the Resource and Output folders within the SRG-STIG Guide-Tool folder can be too long causing the maximum number of characters for a path to be exceeded.

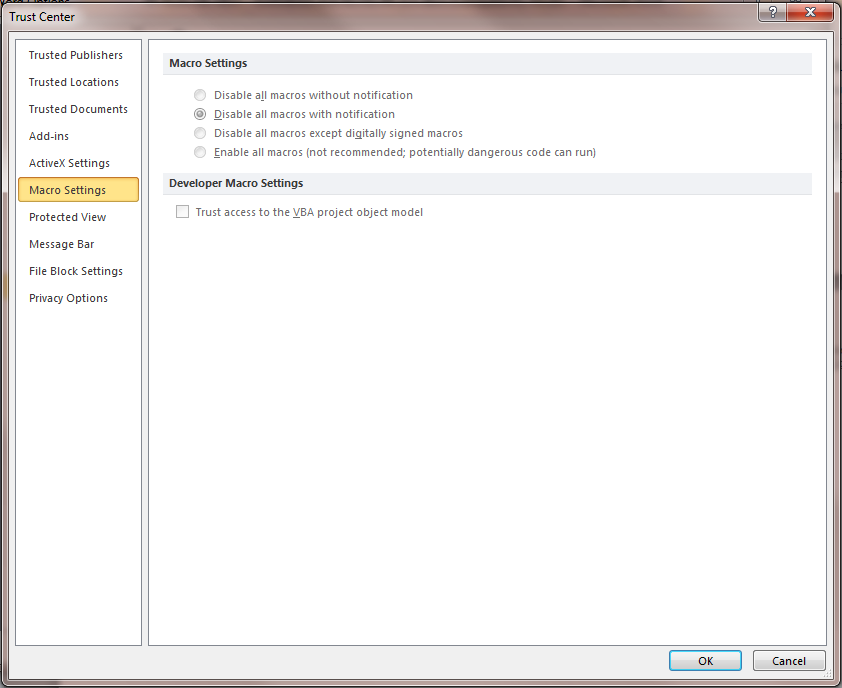
To help with this issue, the name of the SRG-STIG Guide-Tool .zip file has been shortened compared to what was originally used.

Additionally, no matter the unzipping method, once unzipped, the SRG-STIG Guide-Tool folder should only be one level deep. If the result is a folder within a folder, both having the same name, drag the inner folder out of the hosting folder so they are at the same level and then delete the original empty host folder.

Normally, the user’s desktop should be a good location for using the SRG-STIG Guide-Tool

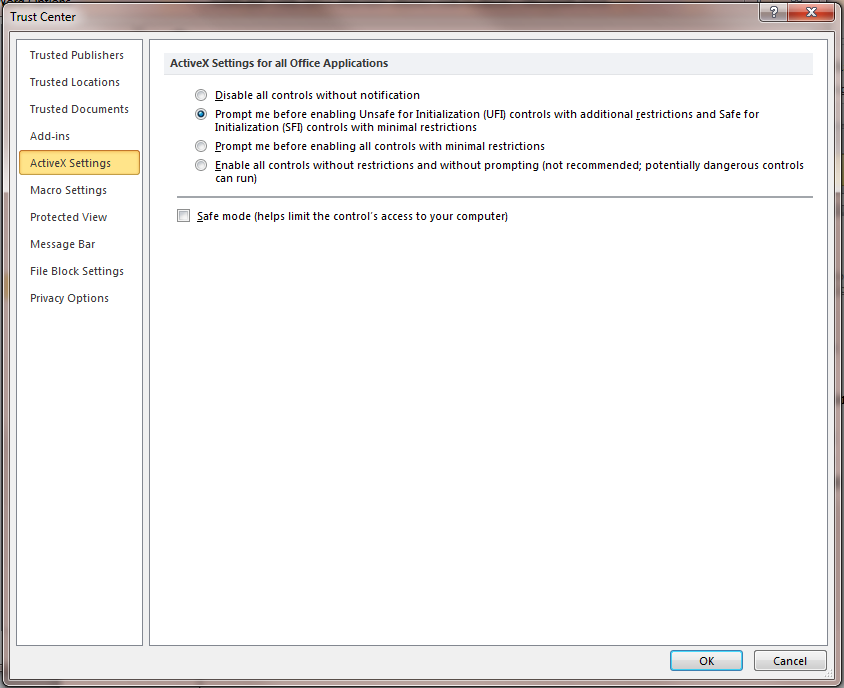
## Trust Center Settings

The trust center can be accessed via File/Options/Trust Center and the Trust Center Settings button. In Word 2010 the trust center Macro Settings page looks like the following:



In the event the “Disable all macros without notification” radio button is selected the automation in the tool will not work. This should not be an issue if any of the other 3 radio buttons are selected.

The “ActiveX Settings” page looks like the following:



In the event the “Disable all controls without notification” radio button is selected the automation in the tool will not work and the document will open directly into to the VB editor. This should not be an issue if any of the other 3 radio buttons are selected. Selecting safe mode does not seem to have a negative effect.

## Microsoft Patch MS14-082 / KB2553154

**Symptoms:** The SRG/STIG Guide/Tool document will open in protected mode on some systems (not all) displaying the VB editor based in the compiler’s inability to find CheckBox #1. The tool will not work even after resetting the debugger and closing the VB editor.

**Cause:** Microsoft released an update for Office 2010 (KB2553154) for MS14-082 on December 9, 2014.

**Resolution:** The fix for this issue is as follows:

1. Using Windows update and its “Update History” function, validate that the “Security Update for Microsoft Office 2010 (KB2553154)…” is installed.
   1. If so, continue to step 2, otherwise stop.
   2. NOTE : a related patch for Office 2013 is KB2726958
2. Close all Office applications
3. Go to <http://support.microsoft.com/kb/3025036/EN-US>
4. Execute either of the “FixIt” solution depending upon your situation.
   1. NOTE: this solution deletes the temp folders containing "MSForms.exd" or at least all their contents. See KB3025036 for details on what is done.

In the author’s case these .exd files were located in the %temp%\excel8.0, %temp%\word8.0, %temp%\vbe folders under %username%\AppData\local\temp\

These files and/or folders are re-created the next time Word is opened (presumably to match the file format to the patch).

ALTERNATELY, you can manually locate and delete all instances of "MSForms.exd" within the (all) %username%\AppData\ folder (s). NOTE: a search of the C:\ drive will NOT find all instances of the files in other user's file folders under C:\users\. Administrator privileges will be needed to access other user's file folders.

# Document Revisions

6/9/2015 Revised for clarity and added items in the Known Issues section.

6/2/2015 Updated the instructions for validating the code signing certificate for a new certificate and to include Word 2010

4/7/2015 Augmented the installation issues section

2/6/2015 Added the document revisions section

2/5/2015 Added the Important Note to the Use/Installation (2.1 at the time) regarding unzipping the .zip file.

Added the Known Problem section (4 at the time)

Under Known Problems:

Added the Installation issue section (4.1 at the time)

Added the Trust Center section (4.2 at the time)

Added a section on the fix for Microsoft Patch MS14-082 / KB2553154 (4.3 at the time)