What to do if a Security Program prevents installation of Excel OM/QM or POM/QM for Windows

It is possible that either Windows or your virus protection program will give you a message indicating that you should not install Excel OM/QM or POM/QM for Windows. These messages are false positives. That is, both packages are safe. In some cases you will be given the opportunity to install the software anyway while in other cases you will not have this opportunity and will need to take steps to get your virus protection program to allow the software to download and install.

In general, there are three ways to allow the software to not be blocked and you should follow them in the order below.

1. Try downloading the software using a different browser.
2. Create an exclusion/exception in the virus protection program for the file or web site
3. Temporarily turn off or disable the virus protection program that is blocking the download or installation

Because there are different versions of both Windows and your virus protection software, in order to create an exclusion or temporarily disable the software you should search the **Help** from the virus protection program for "allowing downloads", "allowing exclusions", "false positives" or "turn off" or "disable" or search the **Web** using the name of your virus protection program, and one of the terms immediately above. For example, search for "turn off windows 10 defender" or "Symantec exclusions" or "disable malwarebytes" without the quotes.

Below are some links to information in this document about four commonly used virus protection programs.

- Windows SmartScreen
- Windows Defender
- Symantec
- Malwarebytes

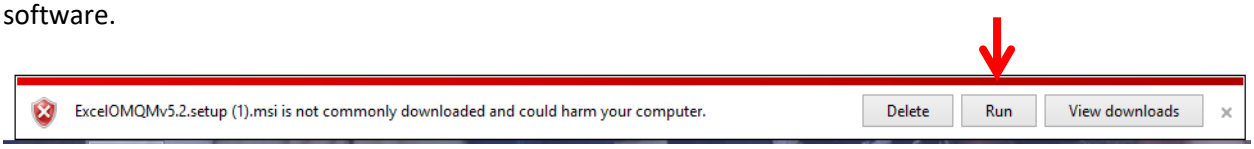
If you want some more evidence that the file is safe you can use https://www.virustotal.com/ to scan the file. Right-click on the Excel OM/QM or POM/QM installation file link on the Pearson web site, right-click on the download link, select copy link address and then paste this address into the search box at https://www.virustotal.com/.

If you still have difficulty, please contact hweiss@comcast.net

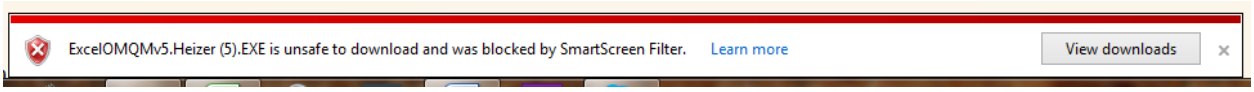
Windows SmartScreen

Depending on your version of Windows and your browser there are different messages that may appear.

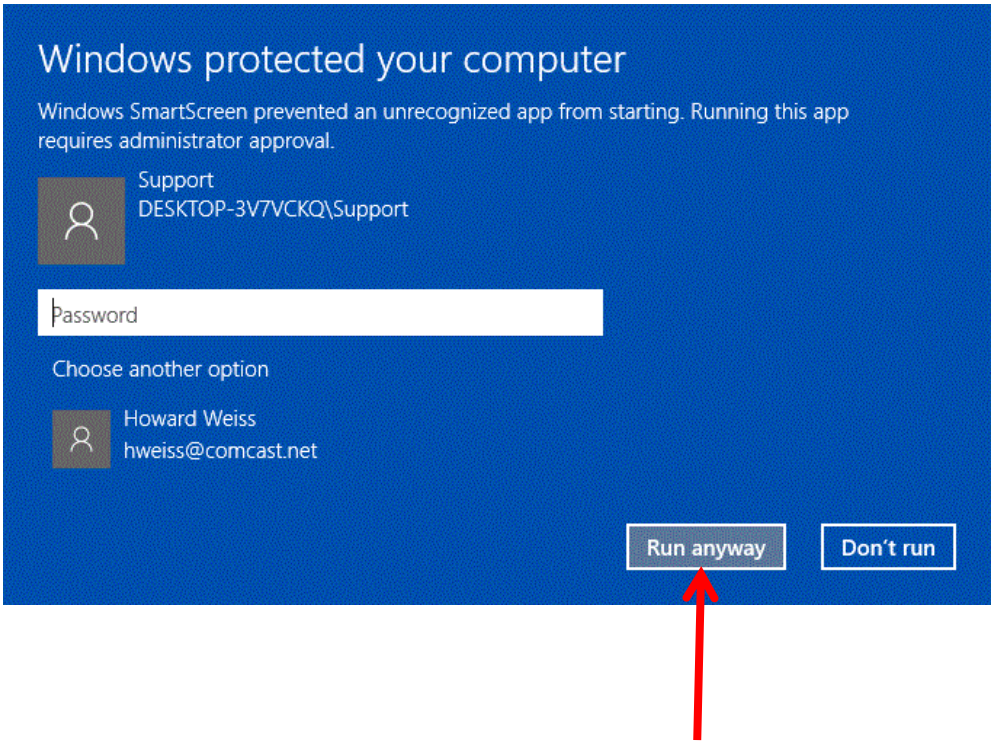
One message might be similar to the one below. In this case, simply select the option to **Run** the software.



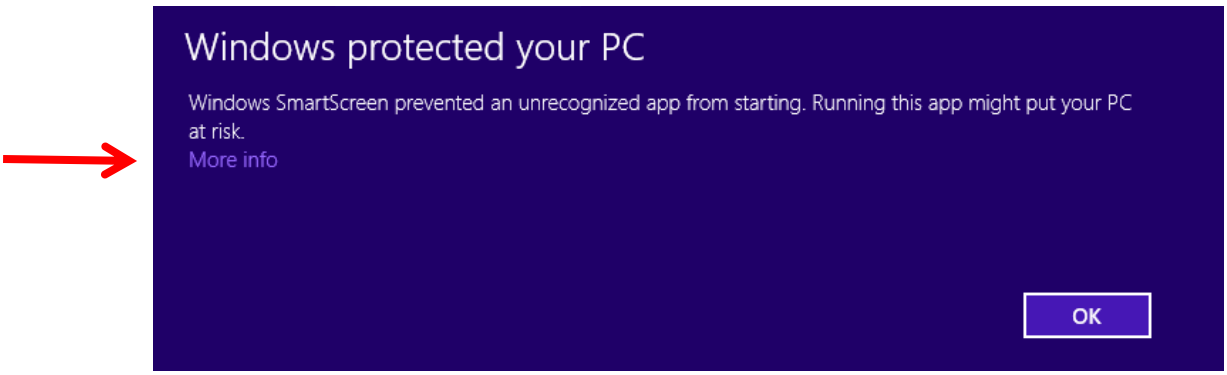
A stricter message might appear that does not give you the option to run the software. In this case you will need to [turn off SmartScreen] using the options below.



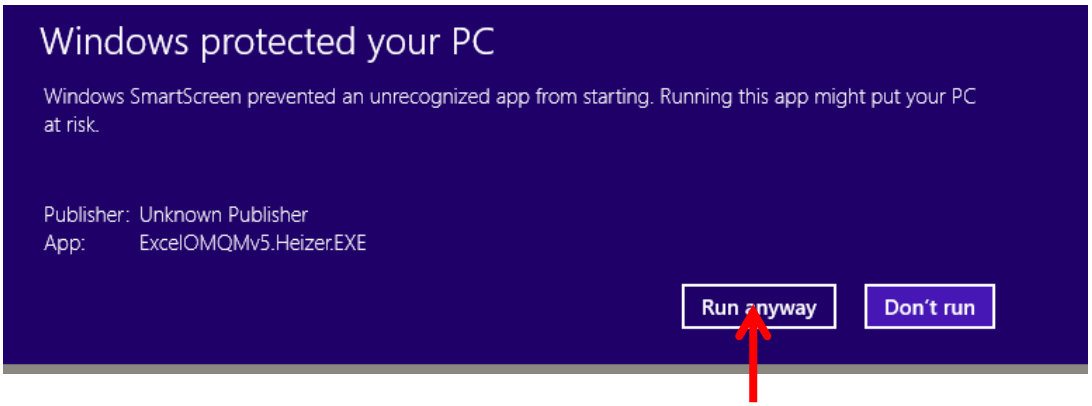
Another message might appear as below. Clearly, you simply need to select **Run anyway**.



Yet another protection message might appear as below.



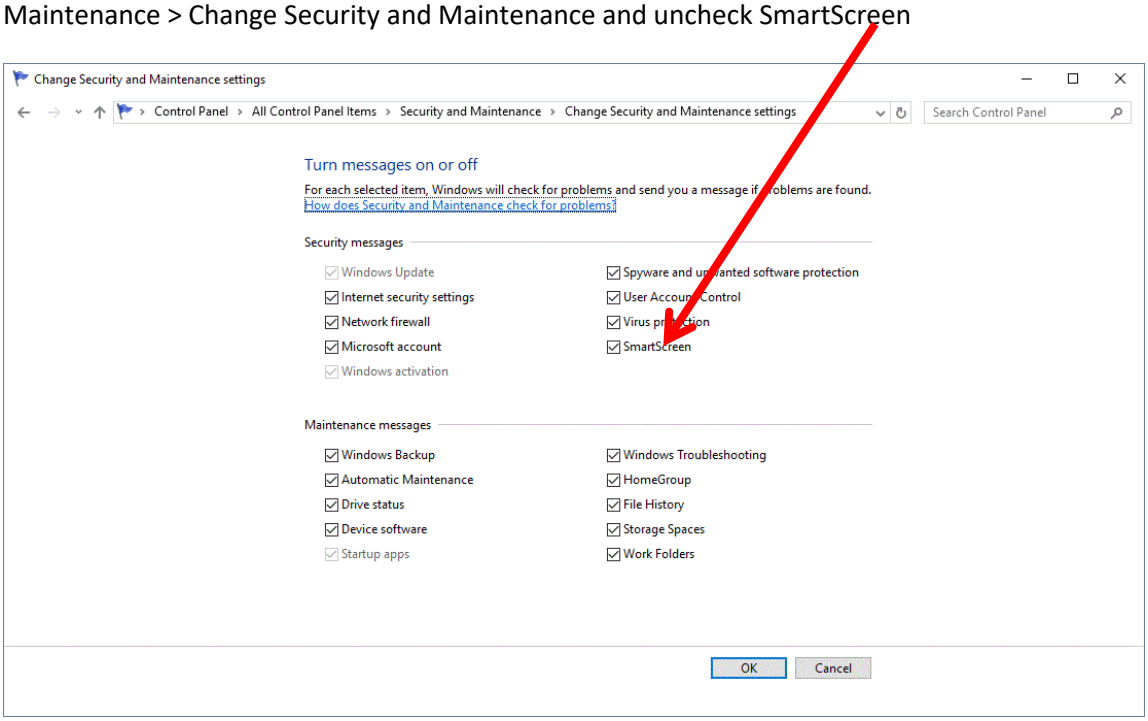
Select **"More Info"** which will then give you the screen below with the option to **Run Anyway**.



If none of these allow you to proceed with the installation then you may need to turn off SmartScreen using the options below.

To turn SmartScreen on or off

If you have Windows 8 or later then go to Control Panel> All Control Panel Items > Security and Maintenance > Change Security and Maintenance and uncheck SmartScreen



For a more detailed explanation please go to

http://www.howtogeek.com/75356/how-to-turn-off-or-disable-the-smartscreen-filter-in-windows-8/

Alternatively, perform the following steps.

1. In Internet Explorer, select the **Tools** button, then select **Safety**.
2. Select **Turn off SmartScreen Filter**, and then choose either **Turn off SmartScreen Filter** or **Turn on SmartScreen Filter**.
3. In the **Microsoft SmartScreen Filter** dialog box, select **OK**.

Be sure to turn SmartScreen on again after downloading the software.

For a more detailed explanation please go to

https://support.microsoft.com/en-us/help/17443/windows-internet-explorer-smartscreen-filter-faq

Windows Defender

Windows Defender is typically turned off if you have another virus protection program running.

From

https://support.microsoft.com/en-us/instantanswers/64495205-6ddb-4da1-8534-1aeaf64c0af8/add-an-exclusion-to-windows-defender

Add an exclusion to Windows Defender

- If you trust a file that Windows Defender has detected as malicious, you can stop Windows Defender from alerting you or blocking the program by adding the file to the exclusions list.
- Go to **Settings** and select **Update & security** > **Windows Defender.** Under **Exclusions,** select **Add an exclusion.** Select the **Add** button, navigate to the file, folder, or process, and then select **Exclude this file.**
- To exclude every one of a type of file, select **Exclude a file extension** and enter the file type.
- If you want to remove an exclusion later, just highlight it and select **Remove.**

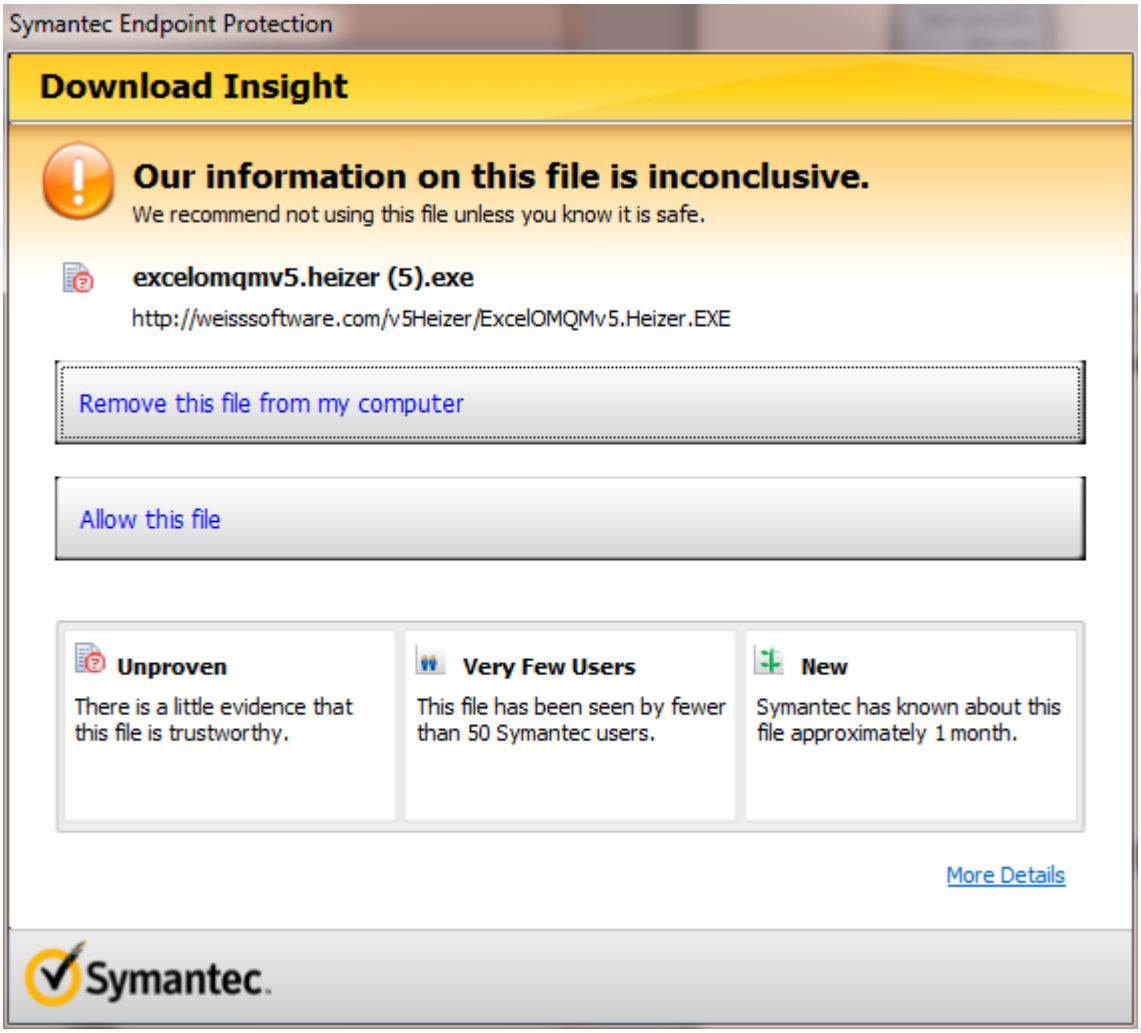
To turn Windows Defender off follow the advice from

http://www.howtogeek.com/howto/15788/how-to-uninstall-disable-and-remove-windows-defender.-also-how-turn-it-off/

Open up **Windows Defender**, go to Tools on the top menu, and then click on Options. Now click on Administrator on the left-hand pane, uncheck the box for “Use this program”, and click the Save button. You will then be told that the program is turned **off**.

Symantec

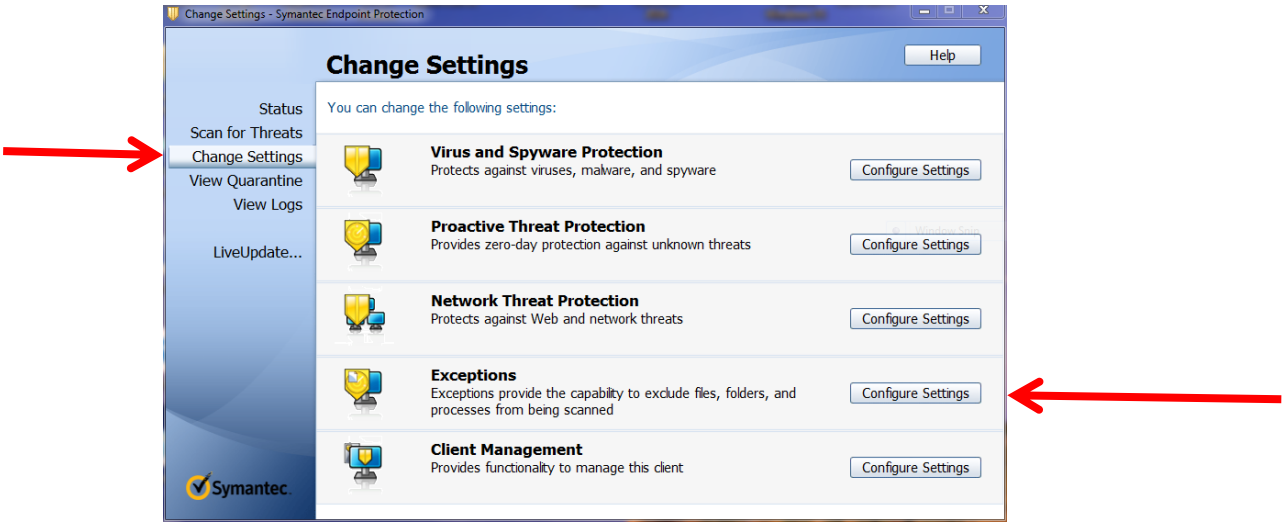
You may get a window which allows you to **“Allow this file”** in which case you simply click on that option.



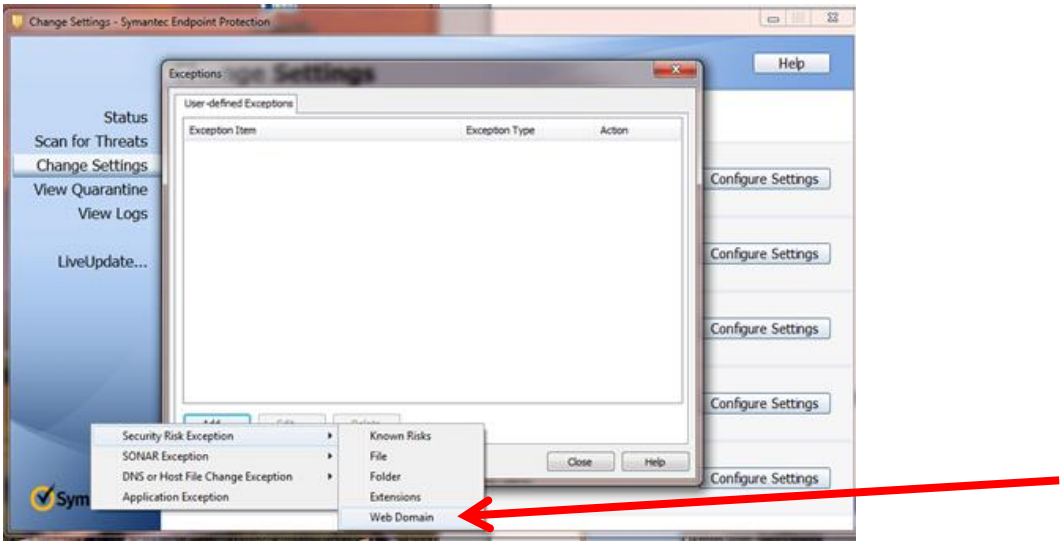
If not, you need to create an exception for the web site or for the files. The following instructions are from the Symantec Help Menu – see Creating exceptions or Web domain, excluding from scans.

Perform the following steps:

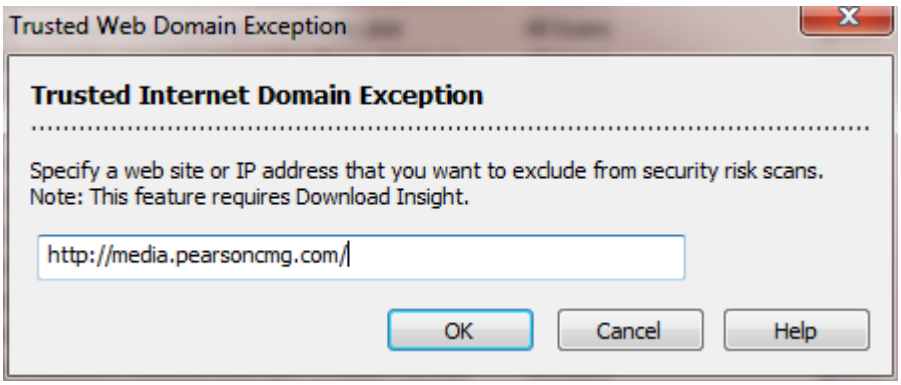
1. Select “Change Settings” from the left-side panel”
2. Select “Exceptions”



3. Select “Security risk, web domain”



4. Enter http://media.pearsoncmg.com/



To turn Symantec off

If the exclusion does not work then one option is to turn off Symantec. To do so, follow the instructions from https://support.symantec.com/en_US/article.TECH192023.html.

1. Open SEP client interface.
2. Click Change Settings
3. Click Configure Settings (next to Client Management)
4. Click the Tamper Protection tab
5. Perform one of the following actions:
    A. Uncheck Protection Symantec security software from being tampered with or shutdown. This disables Tamper Protection.
    B. Change the drop-down menu to Log only. Note: This setting leaves Tamper Protection enabled, however, Tamper Protection will no longer block attempts to modify SEP's files, folders, processes, and Registry values.
6. Click OK. Tamper Protection is now disabled for this SEP client.

After downloading the software be sure to repeat the process above except in Step 5B check the box.:

If you are unable to check the "Unprotect Protection box" then there is one more option.

Stopping Symantec

Click on the Windows button at the lower left of the screen and in the search box enter the following, without the quotes:

"smc –stop" (Note there is a space after "smc" and no space between the minus sign and "stop".

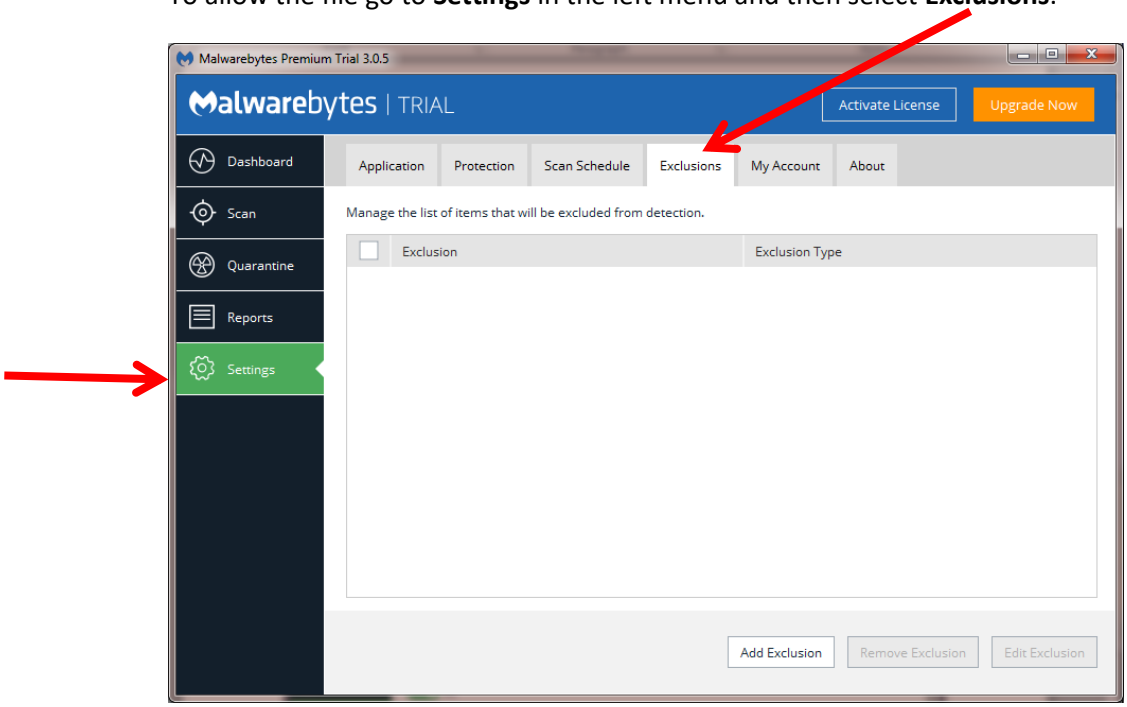
After downloading the software be sure to click on the Windows button at the lower left of the screen and in the search box enter the following, without the quotes:

"smc –start"

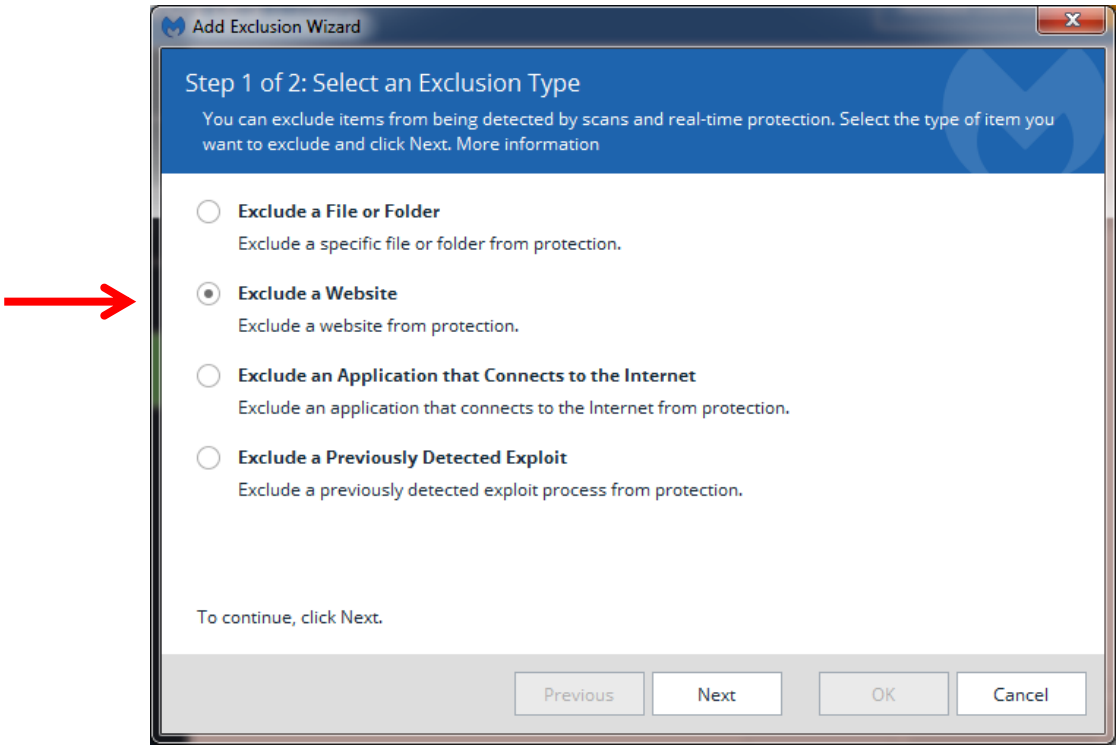
See https://support.symantec.com/en_US/article.TECH103048.html for the available command-line prompts.

Malwarebytes

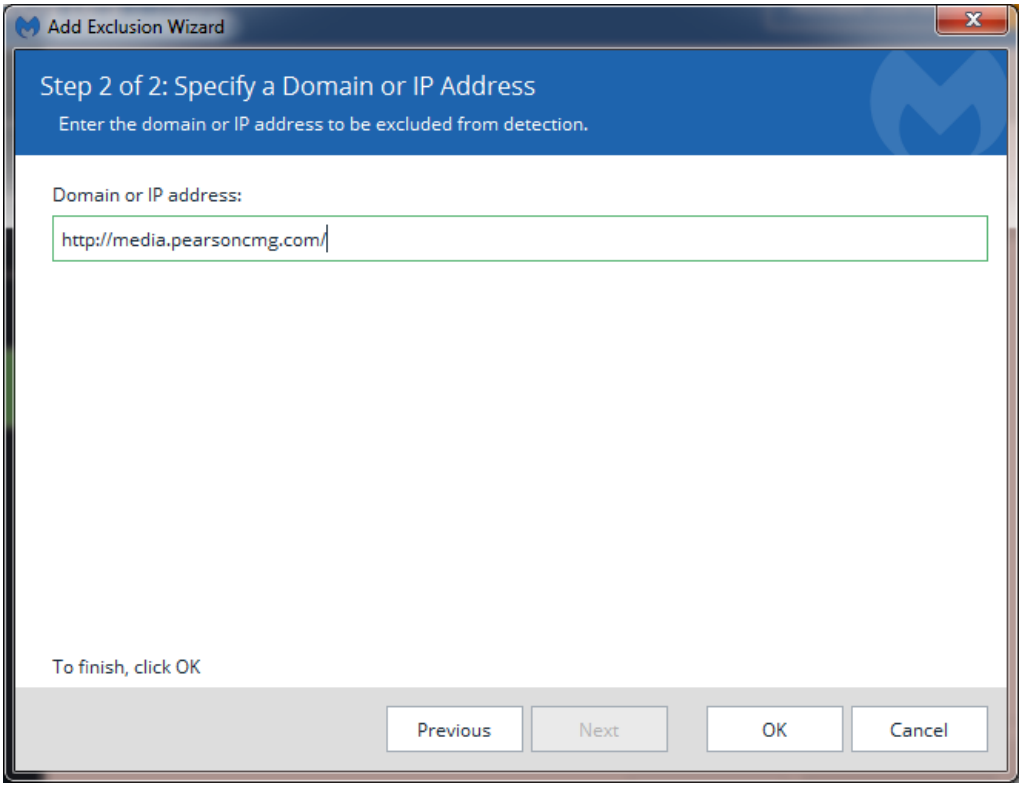
To allow the file go to **Settings** in the left menu and then select **Exclusions**.



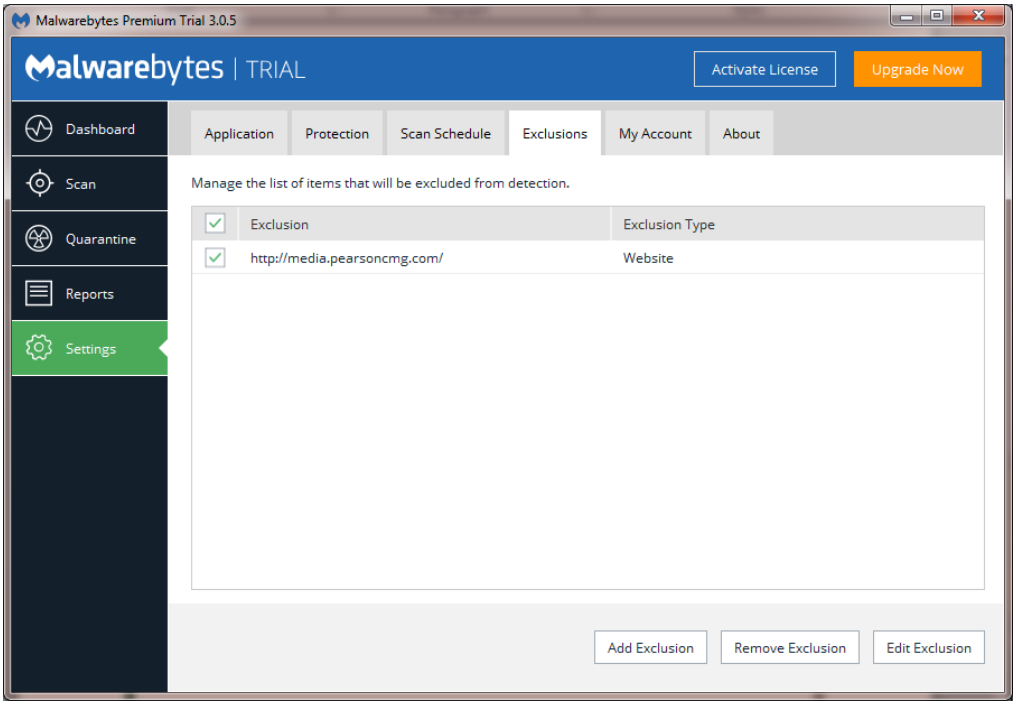
Select **Exclude a Website**



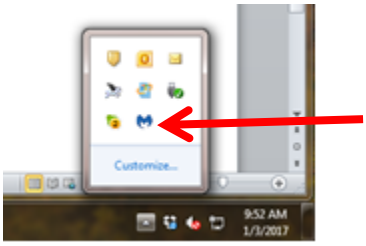
Enter http://media.pearsoncmg.com/



This will yield the following:



If this does not work you can turn off MalWarebytes by right clicking on the Malwarebytes Icon in the system tray and click on Exit.



If you do this be sure to load Malwarebytes afterwards.