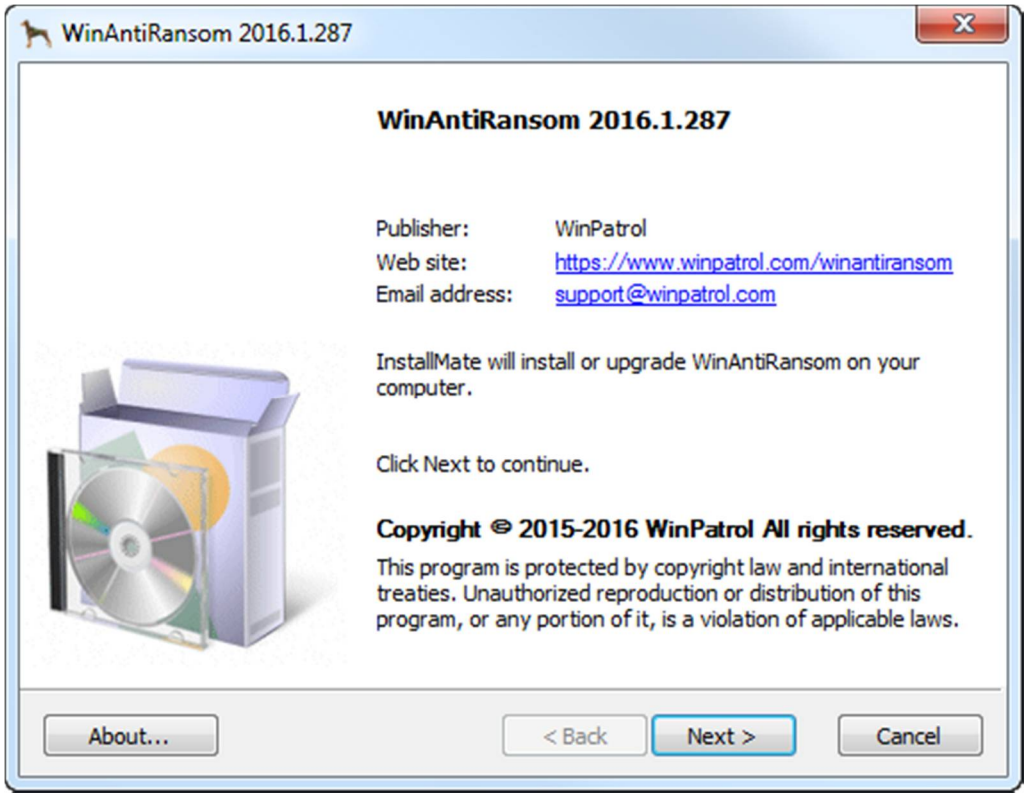
WinAntiRansom Fast Start Guidelines

Installation

Downloading:

https://www.winpatrol.com/downloads/winantiransom-setup.exe



Installation:

During installation you'll be asked to accept our License Agreement and the folder into which you want WinAntiRansom installed. That's it.

Installation does not take long. Upon completion the WinAntiRansom service, tray application and explorer will automatically start.

If for any reason installation fails, please try a second time. If it still fails, please check your other security solutions to ensure nothing has a false positive on WinAntiRansom or one of our components. That has not occurred so far and we hope it remains a non-issue.

WinAntiRansom Fast Start Guidelines

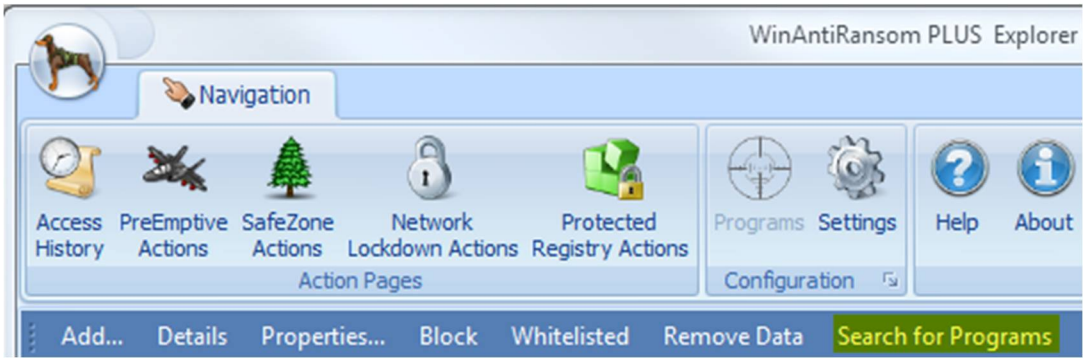
Post Installation:

The Auto-Discovery process is automatically run post-installation. Depending on the speed and configuration of your computer it can take anywhere from a few minutes to 10 minutes or more to run to completion. We've configured it to utilize very little resources while running, so that it won't interfere with anything else you may be doing while it is running.

Auto-Discovery will search your computer for "known" programs and automatically add those found to your Program Configuration page.

Please review the results when completed to ensure programs you want are allowed.

Once Auto-Discovery has run to completion once, it will not run again unless you ask it to do so by selecting the "Search for Programs" menu option on the Program Configuration page. Please see highlight below.



While Auto-Discovery is running, it is a good time to register your copy of WinAntiRansom using the Settings page.

Whitelisting:

We have dramatically improved "Smart Recognition" in the most recent release and most programs are now automatically recognized and allowed by default.

However, it cannot hurt make sure all your startup programs are whitelisted under Programs in WinAntiRansom prior to restarting.

Programs can also be manually added to the Programs page whitelisted as described in the Programs Page section below.

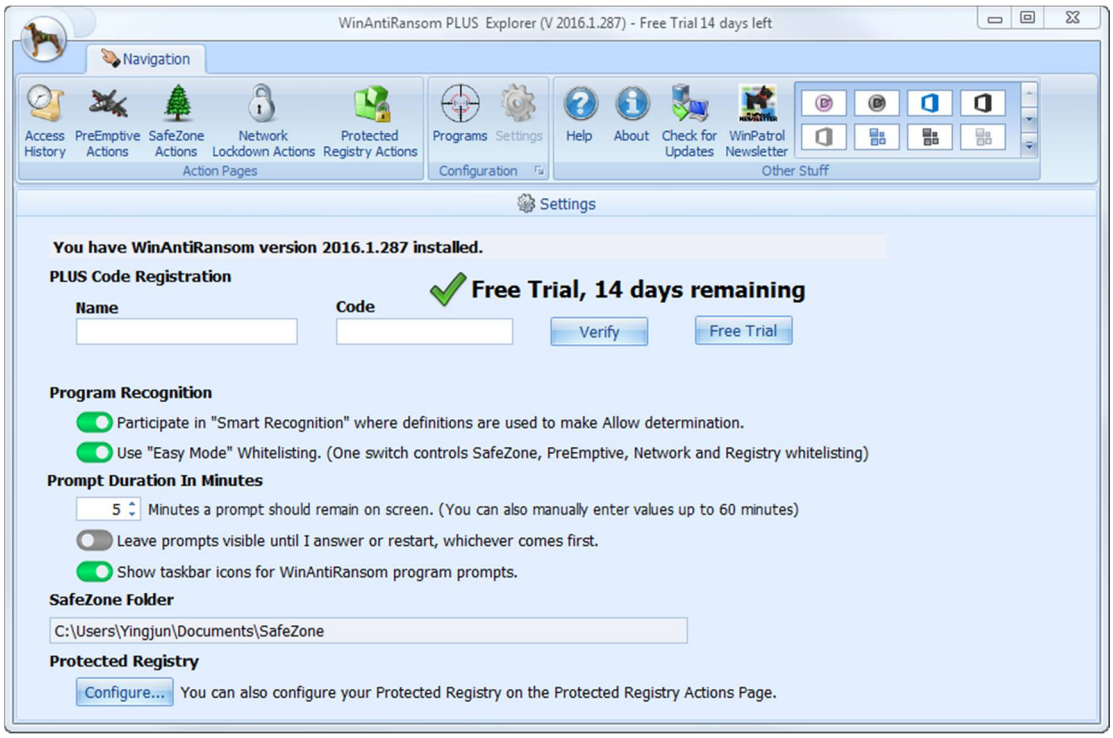
WinAntiRansom Fast Start Guidelines

Please note: Because we installed a device driver, restarting your computer may be required to ensure WinAntiRansom is working perfectly. If you restart your computer before Auto-Discovery is complete, it will not hurt anything. Auto-Discovery will simply run again after restart.

Configuration (Settings Page)

Registration:

- Your registration code for WinAntiRansom is 9 characters long. WinAntiRansom will warn you if the key is not the correct length.
- You may copy and paste both your registration name and code. ***Copy/paste is the recommended way of entering them.***
- Neither the registration name nor code is case sensitive.
- A 15 day free trial is also available.



The image above contains the WinAntiRansom default settings, other than the UserName in which the SafeZone folder is created. The default format for the SafeZone folder is "C:\Users\<username>\Documents\SafeZone".

WinAntiRansom Fast Start Guidelines

Program Recognition:

We default both settings under Program Recognition to on.

"Smart Recognition" tells WinAntiRansom to use our definitions in determining which programs should automatically be allowed or blocked.

"Easy Mode" empowers you to set all four features, PreEmptive Strike ,SafeZone, Network lockdown and Protected Registry for any program with a single click. Using WinAntiRansom in this manner greatly simplifies configuration and is the recommended way to use WinAntiRansom unless you are an advanced computer user.

Prompt Duration:

You have the ability to set WinAntiRansom's prompt behavior.

The default response is immediately applied to all new prompts.

First, is the duration a prompt will remain visible in minutes. You can select any value between zero and sixty. The default setting is 5 minutes.

- *If you select zero, WinAntiRansom **WILL NOT** raise any prompts.*
- Any value other than zero will result in the prompt remaining visible for that many minutes before WinAntiRansom automatically closes the prompt using the default response. (Button highlighted in green)

Next, you have the ability to instruct WinAntiRansom to leave all prompts visible until you answer the prompt yourself or your computer is restarted. If you fail to answer any prompts, the default response is automatically applied.

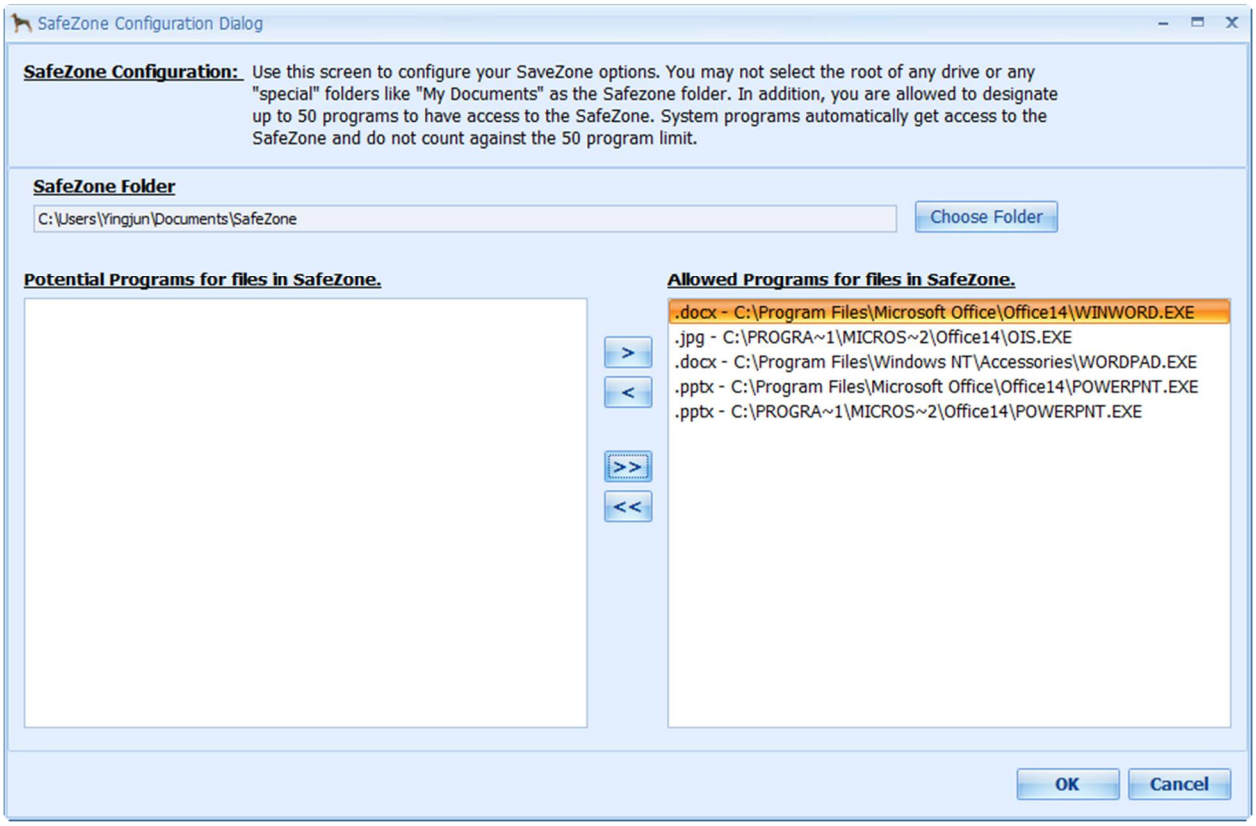
Lastly, you are able to tell WinAntiRansom to create taskbar icons for all WinAntiRansom prompts. Creating a taskbar icon is the default setting.

WinAntiRansom keeps track of all open prompts and will not raise a second prompt for the same issue.

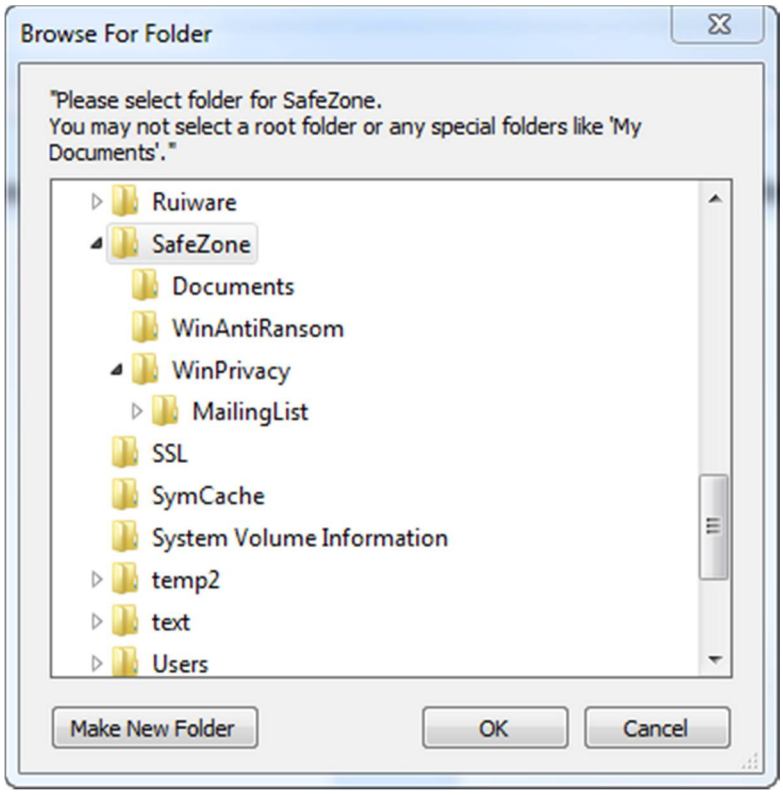
SafeZone Folder:

- Configuring your SafeZone can be done in a multitude of ways, but below is what we recommend for easiest/fastest results.
- The SafeZone folder defaults to a folder named SafeZone under Documents (MyDocuments).

  - You can create/use any “non-special” folder as your SafeZone folder. In other words, you cannot use the root of MyDocuments or C:\Windows or C:\Program Files as your SafeZone folder.
  - SafeZone **DOES NOT** require executable files are moved into your SafeZone.
  - **Your SafeZone should only contain data you want to protect like Documents, pictures, music, things like that.**
  - The folder does not need to be named SafeZone.
  - You may use an entire drive other than your system drive as your SafeZone.
  - You may use an existing folder as your SafeZone or you can create a folder you want to use as your SafeZone.
  - You may create sub-folders inside of your SafeZone to help you categorize your data. These will also be protected.
  - If you are creating a SafeZone, copy the data files you want protected into your SafeZone. **For example**: file.docx, file.xls, file.png, file.jpg
  - Programs **SHOULD NOT** be copied into SafeZone. You should continue to run them from their current location.
- The Configure button will open the SafeZone Configuration Dialog.



- In the SafeZone Configuration Dialog, click Choose Folder and navigate to the folder you created to house your SafeZone data and select it.



- WinAntiRansom will identify all programs associated with the files in that folder and place them into the Potential Programs for files in your SafeZone box on the left side of the screen. (See screenshot in previous page)
- You may select whichever programs you want to be allowed to access the files in the SafeZone.
- If Auto-Discovery has already completed, the programs discovered may already be allowed to access the SafeZone.
- Once you've selected the programs you want allowed to access your SafeZone, click OK.
- That will return you to the Setting Page.

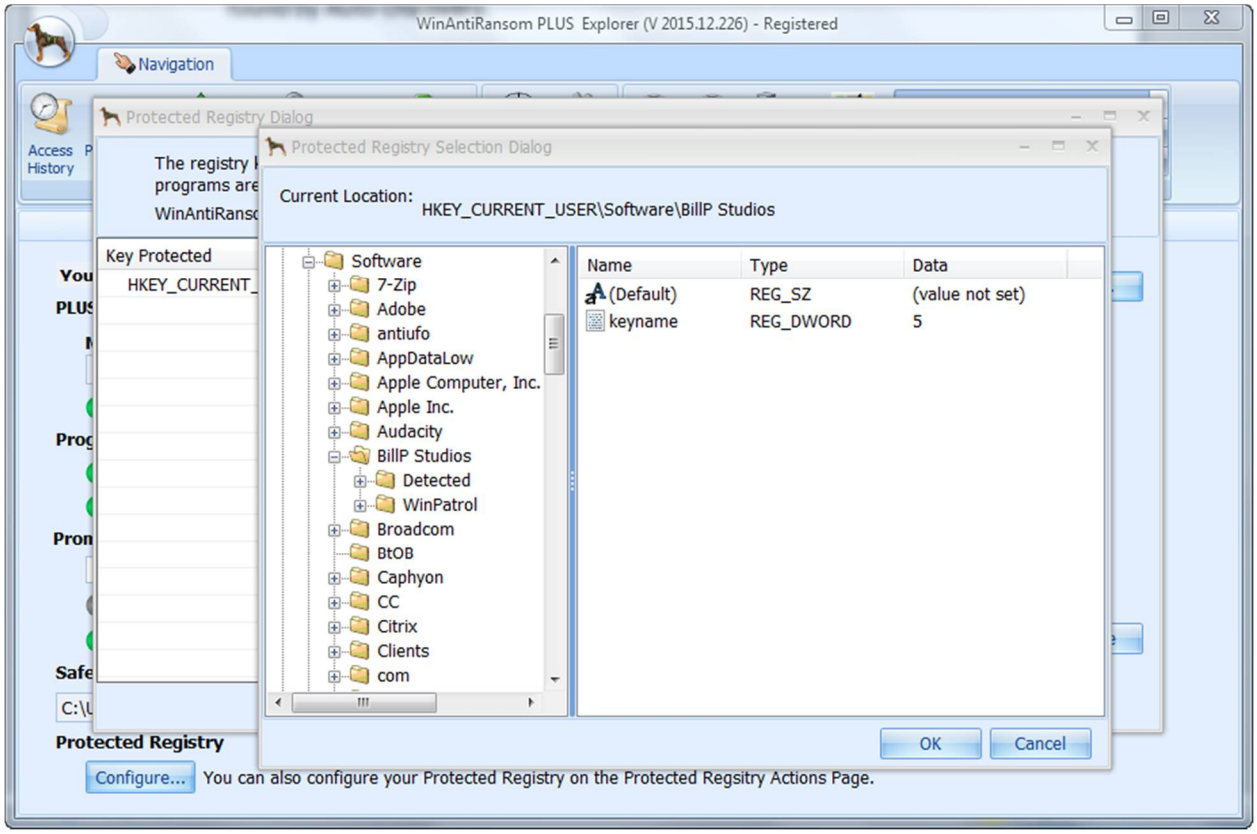
Protected Registry:

WinAntiRansom automatically protects dozens of registry folders typically attacked by Ransomware and Malware. For security reasons we do not list those keys in the application.

The Protected Registry Dialog empowers you to add any additional registry folders you want protected.

WinAntiRansom Fast Start Guidelines

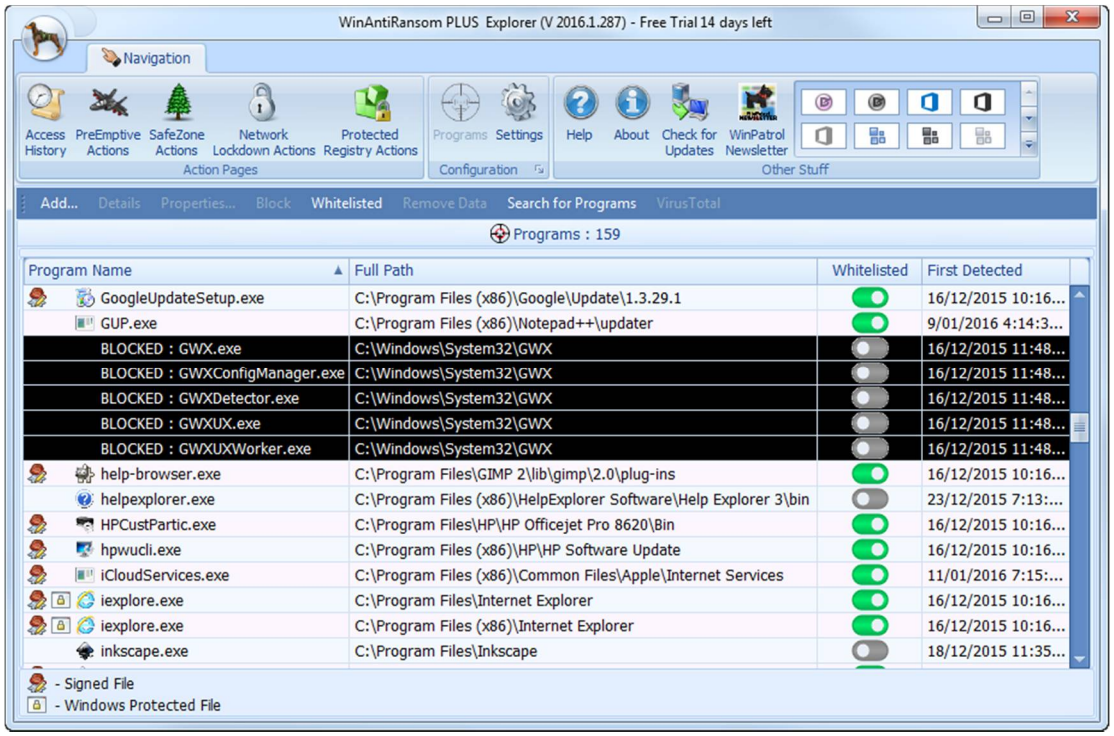
Selecting a registry folder to protect is as simple as navigating to the folder in question in our Protected Registry Selection Dialog and clicking OK.



Once an item is selected, click OK and you will see it on the Protected Registry Dialog screen.

WinAntiRansom Fast Start Guidelines

Programs



The Programs page shows you programs found on your computer by WinAntiRansom either during Auto-Discovery or by having run. In addition, operating specific programs are automatically allowed by default.

The picture above was taken while in "Easy Mode", which is the default setting.

You have many options available to you on this page.

- You can "Whitelist" programs to access the SafeZone, your network (If you have one), Protected Registry and get a free pass from PreEmptive Strike simply by clicking the button in the Whitelisted column for the program you wish to allow. If you change your mind, simply change it back.
- We highly recommend whitelisting all programs you use or that are known to you. Auto-Discovery will automatically fill the Programs page with programs it discovers and will also automatically whitelist all known safe programs.
- The button will light-up with a green color when whitelisted and turn gray when not whitelisted.

- You may also **BLOCK** programs from running. Blocked programs stand out, because of the reverse coloration of the text and background.

Below is a prompt I received while testing a program for which we did not allow access to our SafeZone. Because TextPad.exe is a program we trust, I clicked Allow on the prompt to grant TextPad.exe access to my SafeZone. The next time I attempted to access a document in my SafeZone using TextPad.exe, WinAntiRansom allowed it to access my SafeZone rather than killing it.

If TextPad.exe had been Ransomware, malware, spyware or any other unwanted program, your data would have been safe because of WinAntiRansom's killing any unauthorized program that attempts to access your SafeZone.

Please note: If you have not registered WinAntiRansom, you cannot alter a programs settings and none of WinAntiRansom's protections will operate. A 15 Day free trial mode is also available on the Settings page.

- **Add -> Add Program...** Using this option allows you to manually add programs to the WinAntiRansom program list. Once added, you can whitelist the program if you desire.
- **Add -> Add Folder...** Using this option allows you to add whitelisted folders, where every programs residing in that folder or any sub-folder are automatically allowed to run. With the improvement to "Smart Recognition", we hope to minimize the need for using the Add Folder feature.
    - **Why would I want to allow a folder?** Downloading unsigned executable files into a temporary folder and then executing them is a

behavior that is typical of Ransomware and Malware. Therefore, WinAntiRansom blocks this behavior. Regrettably, some valid applications are also doing this as well, so we've given you the ability allow such programs to run without WinAntiRansom killing them.

- **Block** – Simply by clicking this button, WinAntiRansom will block the highlighted program from running.
  This gives you the power to permanently block any questionable or unwanted program that won't let you uninstall it. In the screenshot above, you will see that blocked programs use reverse the background and font colors for ease of identification.

For more information, please see our documentation at
https://www.winpatrol.com/winantiransom-documentation

Feature Testing

PreEmptive Strike:

To test PreEmptive Strike:

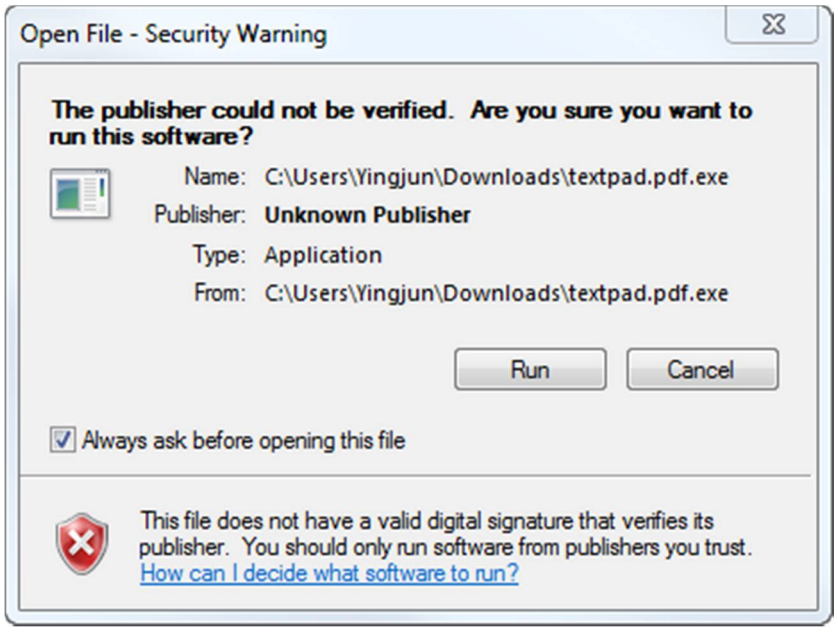
- Please download the following file and save it to disk:

  https://www.winpatrol.com/downloads/textpad.pdf.exe

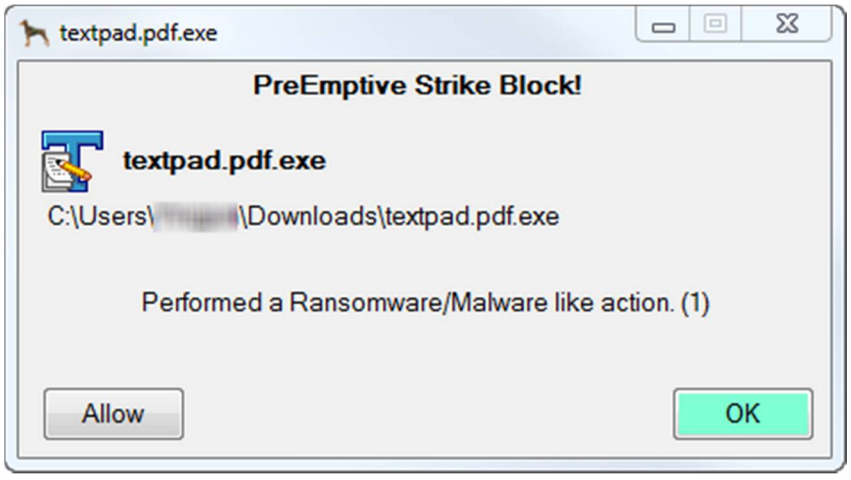
- The program textpad is perfectly safe, but we've renamed it to mimic something done by both ransomware and malware to trick you into running their program. They use extensions like .doc.exe, .xls.exe, .pdf.exe and many more, leveraging the fact that Microsoft hides file extensions by default. By doing so, they hope to trick you into thinking the file is a valid data file, rather than a malicious program.
- Once downloaded, open WinAntiRansom Explorer and open the

  PreEmptive Strike page.

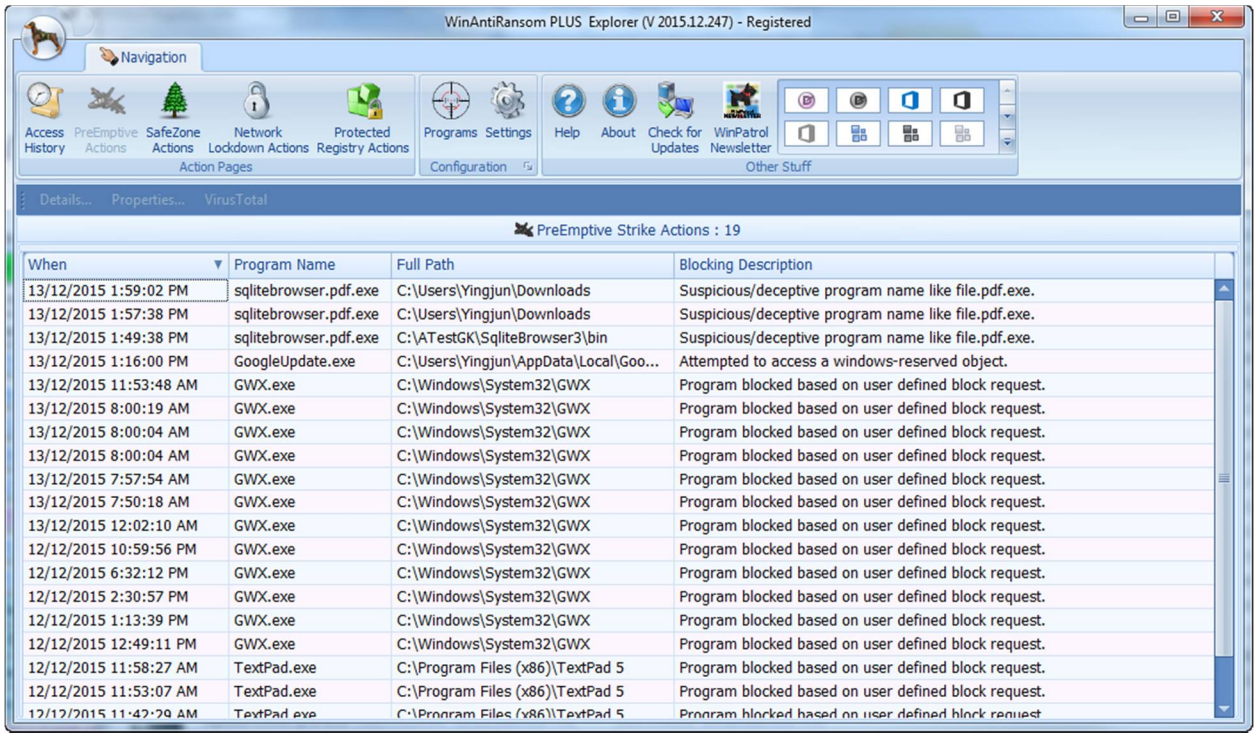
- Now, double-click on the test executable you downloaded to run it. You may receive a dialog like below, please click Run.



- When you click Run, you will immediately have a prompt raised like the one below.



- Click OK to the prompt. (If you click Allow, this will result in PreEmptive Strike ignoring this program in the future).
- The program did not run and you have a new entry in your PreEmptive Strike page.



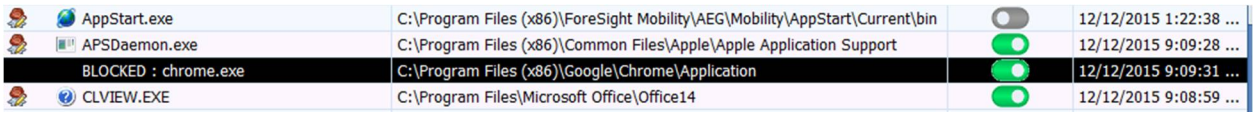
When	Program Name	Full Path	Blocking Description
13/12/2015 1:59:02 PM	sqlitebrowser.pdf.exe	C:\Users\Yingjun\Downloads	Suspicious/deceptive program name like file.pdf.exe.
13/12/2015 1:57:38 PM	sqlitebrowser.pdf.exe	C:\Users\Yingjun\Downloads	Suspicious/deceptive program name like file.pdf.exe.
13/12/2015 1:49:38 PM	sqlitebrowser.pdf.exe	C:\ATestGK\SqliteBrowser3\bin	Suspicious/deceptive program name like file.pdf.exe.
13/12/2015 1:16:00 PM	GoogleUpdate.exe	C:\Users\Yingjun\AppData\Local\Goo...	Attempted to access a windows-reserved object.
13/12/2015 11:53:48 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 8:00:19 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 8:00:04 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 8:00:04 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 7:57:54 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 7:50:18 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
13/12/2015 12:02:10 AM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 10:59:56 PM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 6:32:12 PM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 2:30:57 PM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 1:13:39 PM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 12:49:11 PM	GWX.exe	C:\Windows\System32\GWX	Program blocked based on user defined block request.
12/12/2015 11:58:27 AM	TextPad.exe	C:\Program Files (x86)\TextPad 5	Program blocked based on user defined block request.
12/12/2015 11:53:07 AM	TextPad.exe	C:\Program Files (x86)\TextPad 5	Program blocked based on user defined block request.
12/12/2015 11:42:29 AM	TextPad.exe	C:\Program Files (x86)\TextPad 5	Program blocked based on user defined block request.

- If you do not want WinAntiRansom to block this program, simply open the Programs tab and click the slider button located in the Whitelisted column for the program in question. (PreEmptive Strike column if you are not using Easy Mode)

Block:

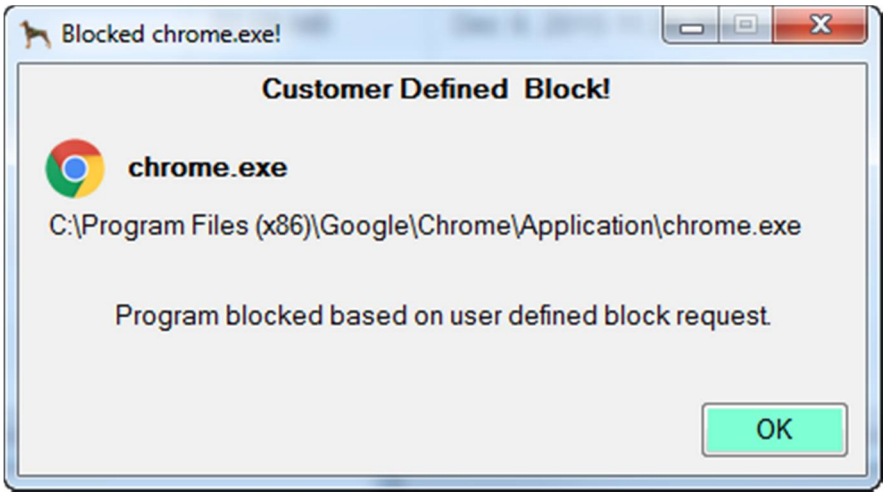
To test WinAntiRansom's ability to block a program, please do the following:

- Open the WinAntiRansom Programs page.
- Select the program you want to test. It is best to use a program you can run manually so that you do not have to wait for it to run.
- Please select a program that does not have any current copies open and running, WinAntiRansom does not yet support killing actively running programs that are set to block.
- I selected Chrome.exe and then selected Block from the page menu.
    - You can also right-click on a program and select Block from the menu that appears.
    - Below is what I see in the Programs page for Chrome.

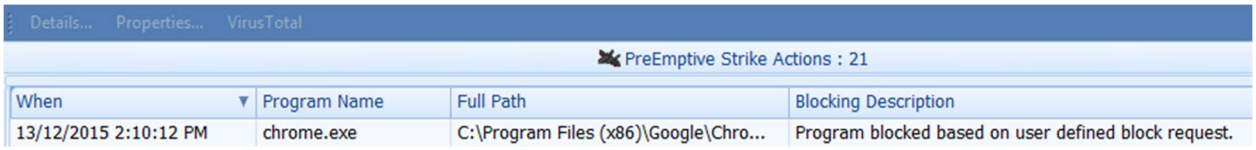


- Please note the "Whitelisted" box still shows as Allowed. We do not alter this setting so that if you are temporarily blocking a program you do not have to reconfigure the Whitelisting setting when restoring the program. Because we block the program from running, the Whitelisted setting does not matter for Blocked programs.

- Now run the program you blocked.



- You should have received a prompt like the one above.
- Also, when you open the PreEmptive Strike Actions page, you'll see we keep track of this for you on that page as well.



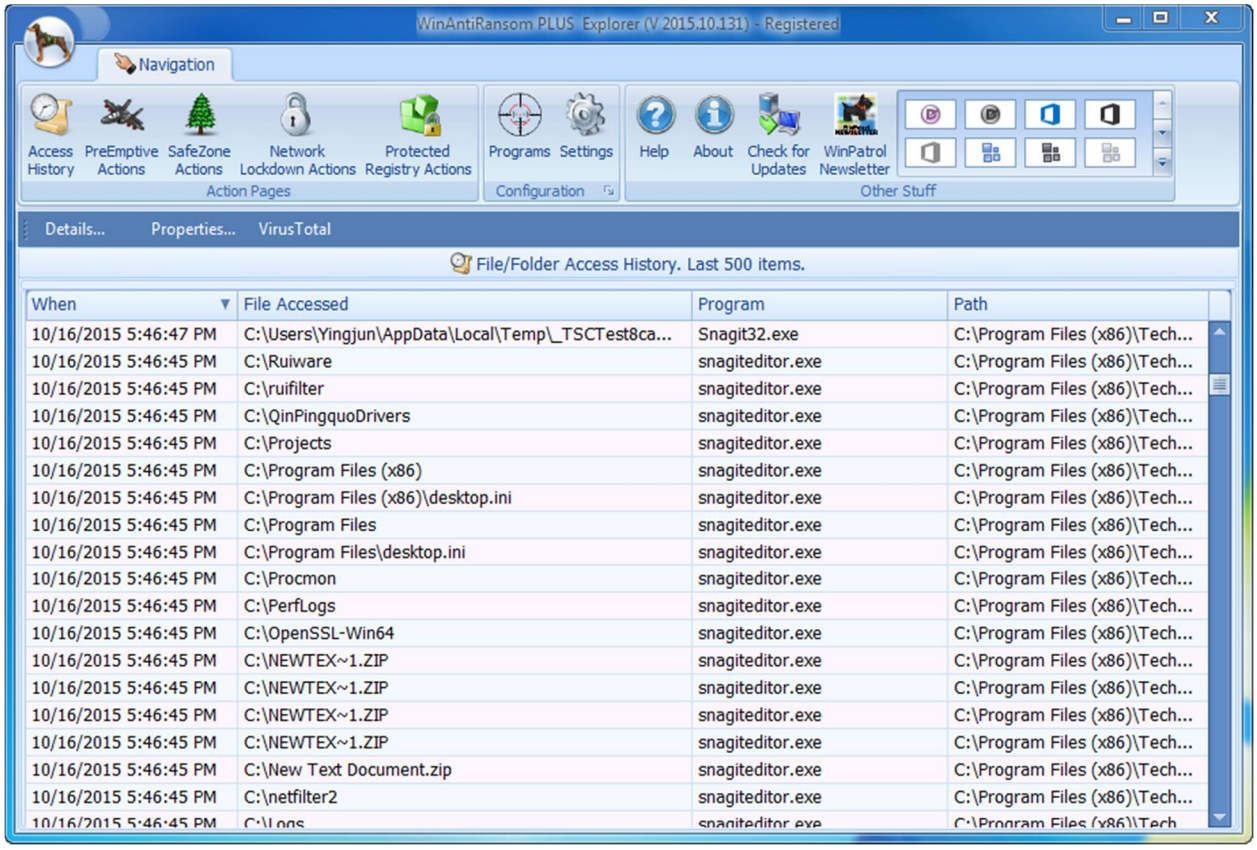
As you can see, WinAntiRansom has some very powerful features that act independently as a layered solution all of its own.

WinAntiRansom Fast Start Guidelines

Access History:

Access History ONLY collects information about programs that ARE NOT allowed to access your SafeZone. Programs allowed to access your SafeZone are considered friendly programs and therefore not monitored in this manner.

Access History has proven to be a very useful feature. When running the tests for this document, I was using a very old version of SnagIt I had laying around. Much to my surprise, I discovered that the editor component was scanning my hard drive in what I can only assume was an attempt to pro-actively find all pictures it could possibly open.

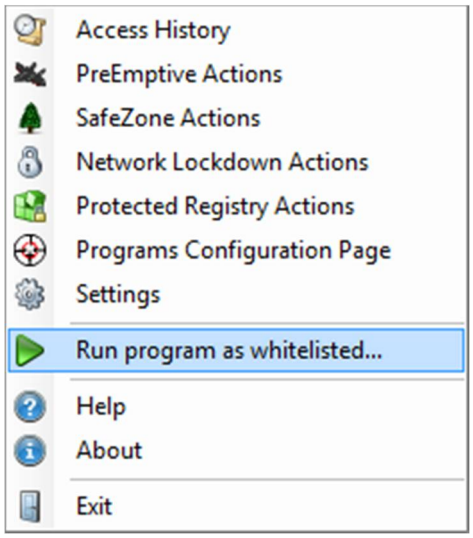


When	File Accessed	Program	Path
10/16/2015 5:46:47 PM	C:\Users\Yingjun\AppData\Local\Temp_TSCTest8ca...	Snagit32.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Ruiware	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\ruifilter	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\QinPingquoDrivers	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Projects	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Program Files (x86)	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Program Files (x86)\desktop.ini	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Program Files	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Program Files\desktop.ini	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Procmon	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\PerfLogs	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\OpenSSL-Win64	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\NEWTEX~1.ZIP	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\NEWTEX~1.ZIP	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\NEWTEX~1.ZIP	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\NEWTEX~1.ZIP	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\New Text Document.zip	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\netfilter2	snagiteditor.exe	C:\Program Files (x86)\Tech...
10/16/2015 5:46:45 PM	C:\Logs	snagiteditor.exe	C:\Program Files (x86)\Tech...

WinAntiRansom Fast Start Guidelines

Tray Application

The WinAntiRansom Tray Application is like most standard tray applications by allowing you to open any page of WinAntiRansom Explorer you'd like directly from the tray. In addition, he contains items from both Help and About and of course, "Exit".



Run Program as Whitelisted

What is really cool about this tray menu is the "**Run program as whitelisted...**" menu item. What does this do?

Say you have an installer that WinAntiRansom doesn't recognize. Well, simply open the tray application, click on Run program as whitelisted..., navigate to the installer in question and select it. WinAntiRansom will automatic run the program for you and allow it to run without blocking it.

Conclusion

WinAntiRansom uses a combination of Whitelisting, heuristics and definitions in a layered solution that protects your computer and your data from all known Ransomware and many kinds of Malware and Spyware. Plus gives you the ability to block any program you want from even running.