WinAntiRansom Fast Start Guide

Installation

**Downloading:**

![WinAntiRansom Setup Screen](image.png)

**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.
Post Installation:

WinAntiRansom Explorer will open to the Settings page by default when it is initially installed. Please feel free to enter your credentials immediately.

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.

If you’ve entered your credentials, you will see a dialog that looks like the one below.

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

Upon completion, the above dialog is closed and the one below is opened.
Please review the results on the Programs Page when AutoDiscovery completes 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.
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”.

Program Recognition:

Program Recognition

- Participate in “Smart Recognition” where definitions are used to make Allow determination.
- Use “Easy Mode” Whitelisting. (One switch controls SafeZone, PreEmptive, Network and Registry whitelisting)

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.

“Smart Recognition” is on by default and automatically whitelists “known good” programs when found during AutoDiscovery or by WinAntiRansom afterwards. It is best to review the Programs page post installation to ensure 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.

“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.

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

**Protected Registry:**

WinAntiRansom automatically protects hundreds of system critical registry keys without your having to do anything special.

In addition to that, we’ve added the ability for you to define additional keys you want protected. If you can’t think of any, then you may not need to define any keys in addition to those WinAntiRansom already protections.

Clicking the Configure... button will open the Protected Registry Selection Dialog where you can select registry keys to protect.
Once an item is selected, click OK and you will see it on the Protected Registry Dialog screen.

**SafeZone Folder:**

- You can configure up to 10 folders as SafeZone folders.
- Configuring a 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 SafeZones 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 existing folder as your SafeZone or you can create a folder you want to use as your SafeZone.
- You may use an entire drive other than your system drive as your SafeZone.
  - If you have a D:\ drive where you store all of your data, simply designate that as a SafeZone.
  - In addition, if you own a Wireless Hard drive, it is automatically protected by our Network Lockdown feature as a SafeZone.
- You may create sub-folders inside of your SafeZone to help you categorize your data. All subfolders are also 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 Add button will open a folder browser where you can navigate to an existing folder to set as a SafeZone.
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.
WinAntiRansom Fast Start Guide

- 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 WinAntiRansom had not yet seen and was not whitelisted.

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 program’s settings and none of WinAntiRansom’s protections will operate.

**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.
WinAntiRansom Fast Start Guide

- **Why would I want to allow a folder?** Downloading executable files into a temporary folder and then executing them is a behavior that is typical of Ransomware and/or 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. An example of a program many do not want running is shown as Blocked in the screenshot above with the resulting prompt show below. Blocked programs reverse the background and font colors for ease of identification.

![Blocked GWXDetector.exe](image)

Program blocked as requested by user.

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

**Feature Testing**

**PreEmptive Strike:**

To test PreEmptive Strike:

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

WinAntiRansom Fast Start Guide

- 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.

![Open File - Security Warning dialog]

- 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).
• Please note the “What other’s do” section. If this were a “known” program, WinAntiRansom will provide you with the results of what other do as far as allowing or blocking the program.
• The program did not run and you have a new entry in your PreEmptive Strike page.
If you do not want WinAntiRansom to block this program, simply highlight the entry and select “Whitelist Program”. That’s it, WinAntiRansom will now let the program run.

**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.
- 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.

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.

Of course it is highly doubtful you would want to always block Chrome, so I returned to the Programs Page, highlighted Chrome again and selected “Unblock”.

> 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.
Yep, removing a block is that easy.

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

**Access History:**
Access History 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.

In addition, Access History shows you when new programs are detected.

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.
### File/Folder Access History, Last 500 Items

<table>
<thead>
<tr>
<th>When</th>
<th>File Accessed</th>
<th>Program</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/16/2015 5:46:47 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
<tr>
<td>10/16/2015 5:46:45 PM</td>
<td>C:sers[User]\AppData\Local\Temp_TSCTestFile3.5.exe</td>
<td>Snag2332.exe</td>
<td>C:\Program Files (x86)\Tech...</td>
</tr>
</tbody>
</table>
WinAntiRansom Fast Start Guide

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 Help and About, Stop/Start Protection 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.

Stop WinAntiRansom Protection

This feature will comes in handy if you are running a troublesome installer, uninstaller or application. Simply Stop protection, run the application and then...
select Start Protection to re-enable WinAntiRansom. Start Protection is only visible if protection is not active.

**Conclusion**

WinAntiRansom uses a combination of Whitelisting, artificial intelligence algorithms 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.