



# AppGuard Solo

## User Guide

**Version 6.0**

**June 2018**

14120 Parke Long Court, Suite 103  
Chantilly, Virginia 20151  
[www.AppGuard.us](http://www.AppGuard.us)

All Products are provided with RESTRICTED RIGHTS.

Use, duplication or disclosure by the Government is subject to restrictions set forth herein and in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, as applicable.

AppGuard® Solo is a registered trademark of AppGuard LLC.

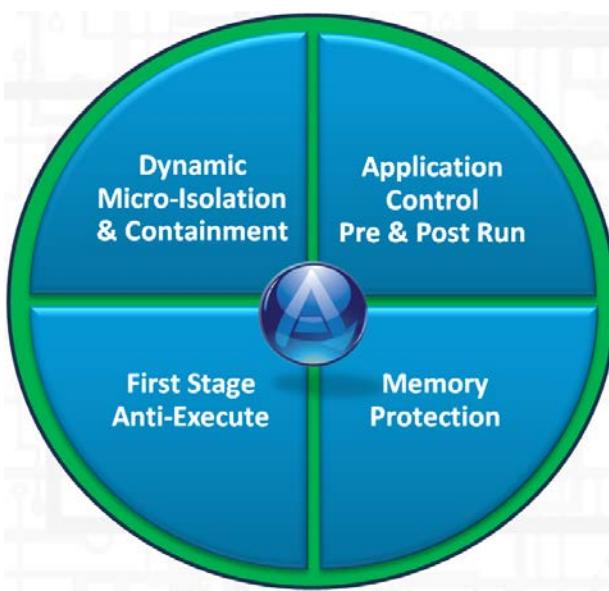
## Table of Contents

Introduction.....	4
AppGuard Solo.....	4
Operating System Requirements .....	4
Hardware Requirements .....	4
Prerequisites .....	4
Installing AppGuard Solo Overview .....	4
Installation Steps .....	5
Operating AppGuard Solo .....	9
AppGuard Solo Protections.....	9
AppGuard Solo System Tray Icon.....	9
Protection Levels and AppGuard Solo User Interface.....	10
Help .....	12
Definitions .....	12
Protection .....	12
Control and Audit.....	13
Policy Related Terms.....	14
User Interface.....	14
Tray Icon .....	14
Popup and Toaster Messages.....	16
AppGuard Solo Activity Report.....	17
Important Software Installation Note .....	21
Customizing AppGuard Solo Policy (Optional) .....	22
Alerts Tab .....	22
User Space Tab.....	24
Adding User Space Folders .....	24
Defining User Space Exclusions .....	24
Network Drives .....	25
White-listing User Space Executables.....	25
Publishers List .....	25
Automatic Updates.....	27
Guarded Apps Tab.....	27

Guarded Apps List.....	28
Folders Settings.....	28
Protected Folders.....	31
Exception Folders.....	31
Private Folders .....	31
Advanced Settings Tab .....	31
Suspension Timeout .....	32
Pass the hash protection .....	32
AppGuard Solo Updates .....	32
Privileged Operation – Administrative Controls.....	32
Self-Protection .....	34
Privileged Mode.....	34
Power Applications .....	35
Restore All Settings to Default.....	36
Application Notes .....	36
Running with UAC Enabled .....	36
Click-to-Run Applications .....	36
Google Chrome .....	36
Network Shares Anomalies .....	37
Support.....	37
Product Online Help .....	37
Contact Support .....	37
Windows Event Viewer .....	38

## Introduction

Conventional “detect and respond” approaches available are not enough in today’s cyber world. AppGuard Solo delivers a multi-layered defense, protecting the endpoint at multiple points, including: launch control, run-time application control, and memory protection, to prevent one application from reading or writing to the memory of another. AppGuard Solo protects your computer against certain applications with the greatest risk of malware, such as Microsoft and Adobe products. AppGuard Solo stops the cyberattacks that traditional security products often miss, **even zero-day and file-less malware**. AppGuard Solo prevents suspicious applications from running and stops even allowed applications (such as your browser) from performing high-risk activities that might result in an infected computer.



This document provides information on installing, configuring and using AppGuard Solo.

## AppGuard Solo

### Operating System Requirements

- Microsoft Windows 7 and above

### Hardware Requirements

- Minimum 1.80 GHz 1.00 GB of RAM
- 10 MB Hard Disk free space

### Prerequisites

- Disable any antivirus software
- Close all applications and utilities
- The system should have at least the minimum configuration described above

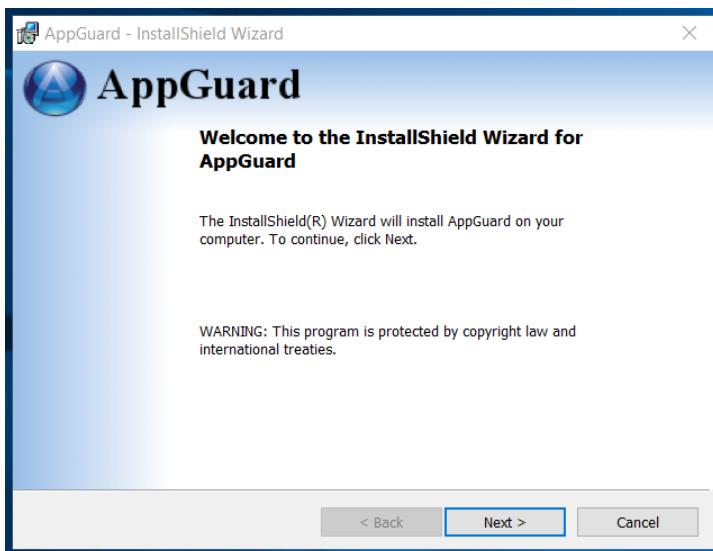
### Installing AppGuard Solo Overview

1. To run the installation program, log-on as a user with local administrator rights on the system.  
**Note:** The user does not require administrator privileges to run the application, only for installation.

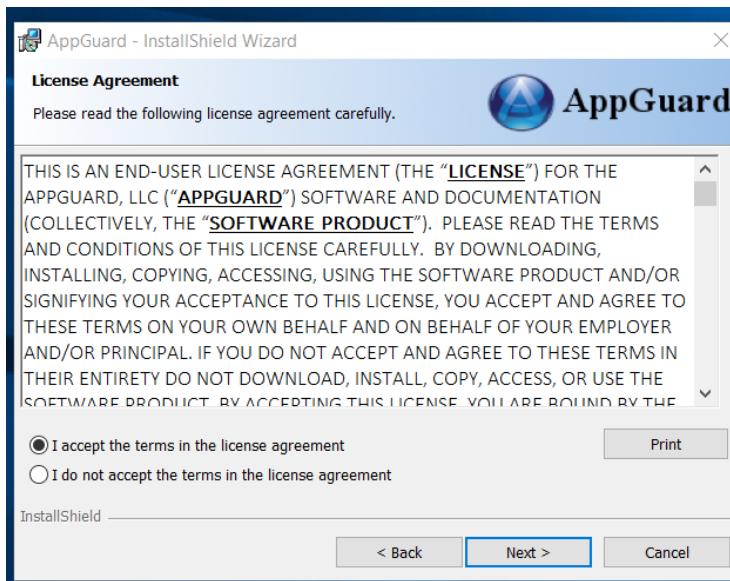
2. Launch the setup program from the download or your disk drive.
3. Make sure you have your License ID and Password during the install; you will be prompted to enter them for activation.
4. Reboot the computer when prompted.

## Installation Steps

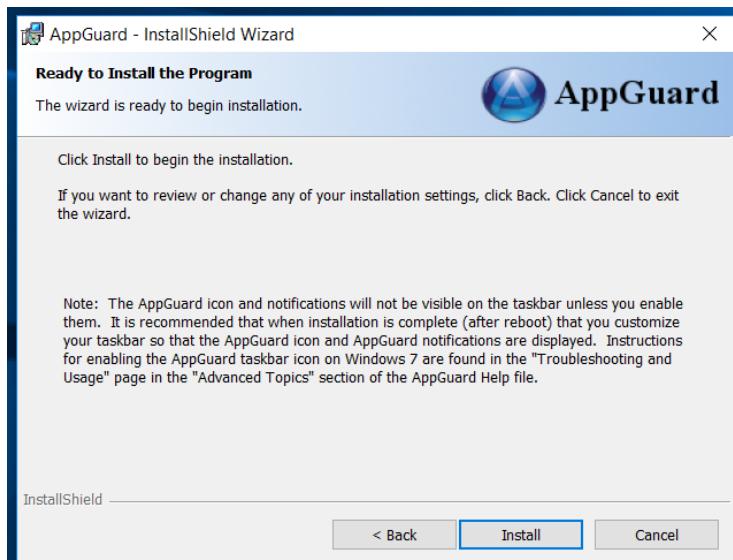
- Click the AppGuardSetup.exe file to begin the installation.
- In the User Account Control message, click **Yes** to allow AppGuard Solo to make changes to your computer.
- The InstallShield Wizard will begin and display the Install message below. Click **Next** to continue.



- Accept the License Agreement and click **Next** to continue.



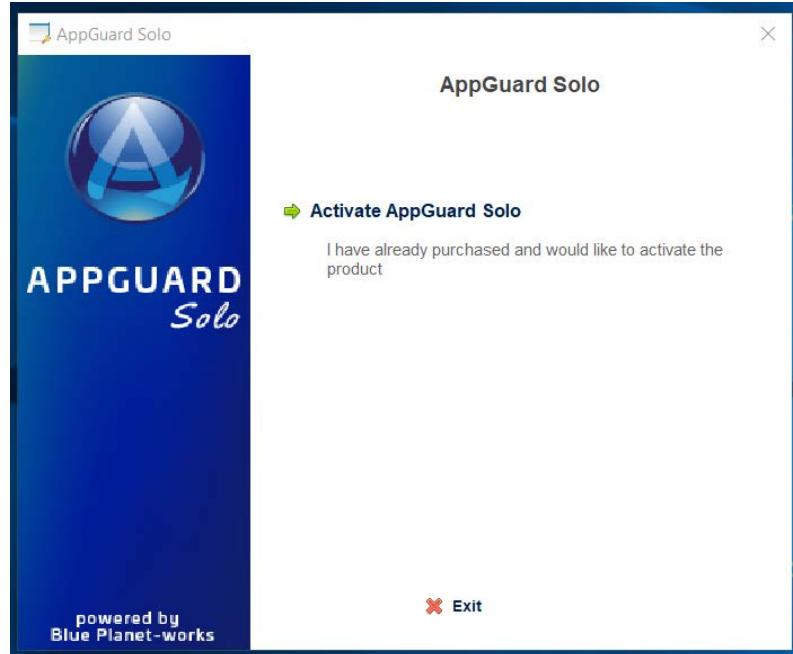
- Click **Install** to begin the installation. Make sure you have your License ID and Password available.



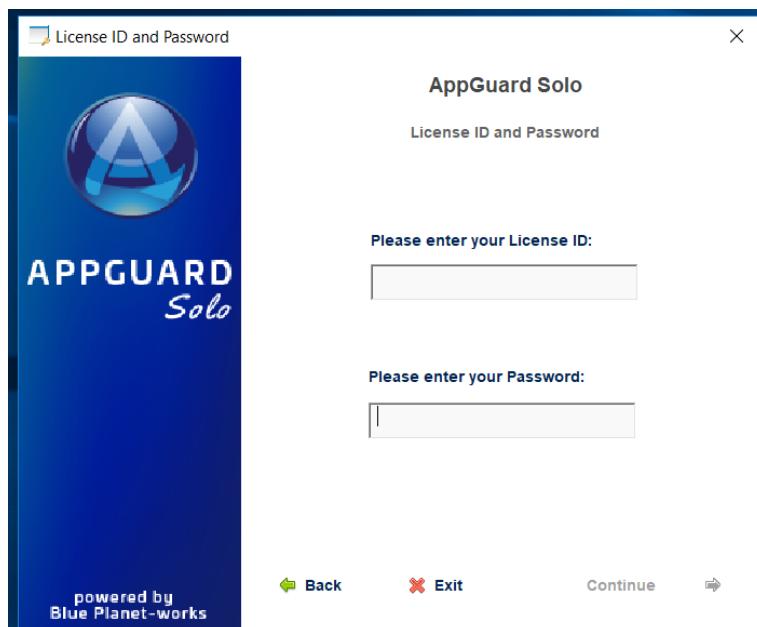
- The Activate AppGuard Solo screen will be displayed. If it does not display, please look for this symbol in the system tray to bring up the screen:



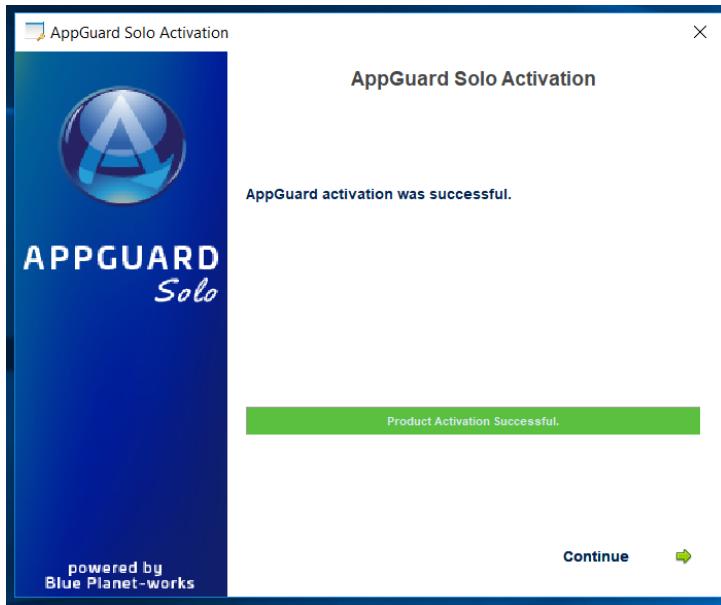
- Click the link to Activate AppGuard Solo.
- Click the **Exit** button if you are not ready or do not have your License ID and Password.
- Click the **Go to Website** link to purchase a License.
- If you click **Exit**, you will need to begin the Install process again when you are ready.



- Enter your License ID and Password in the fields provided and click **Continue**.



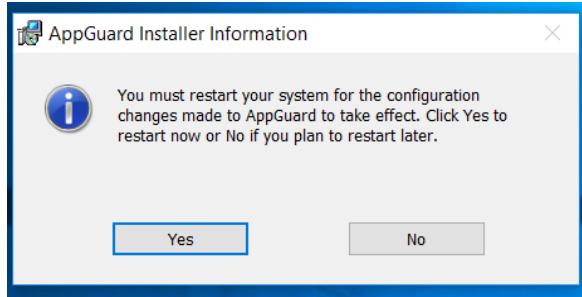
- AppGuard Solo will check with the license server, and then display "Product Activation Successful". Click **Continue** to resume the installation.



- AppGuard Solo will continue with the installation and provide a progress screen.
- When the install is complete, click the **Finish** button.



- Click **Yes** to restart now, or **No** to restart later. You must restart for AppGuard Solo to begin protecting your system.



## Operating AppGuard Solo

### AppGuard Solo Protections

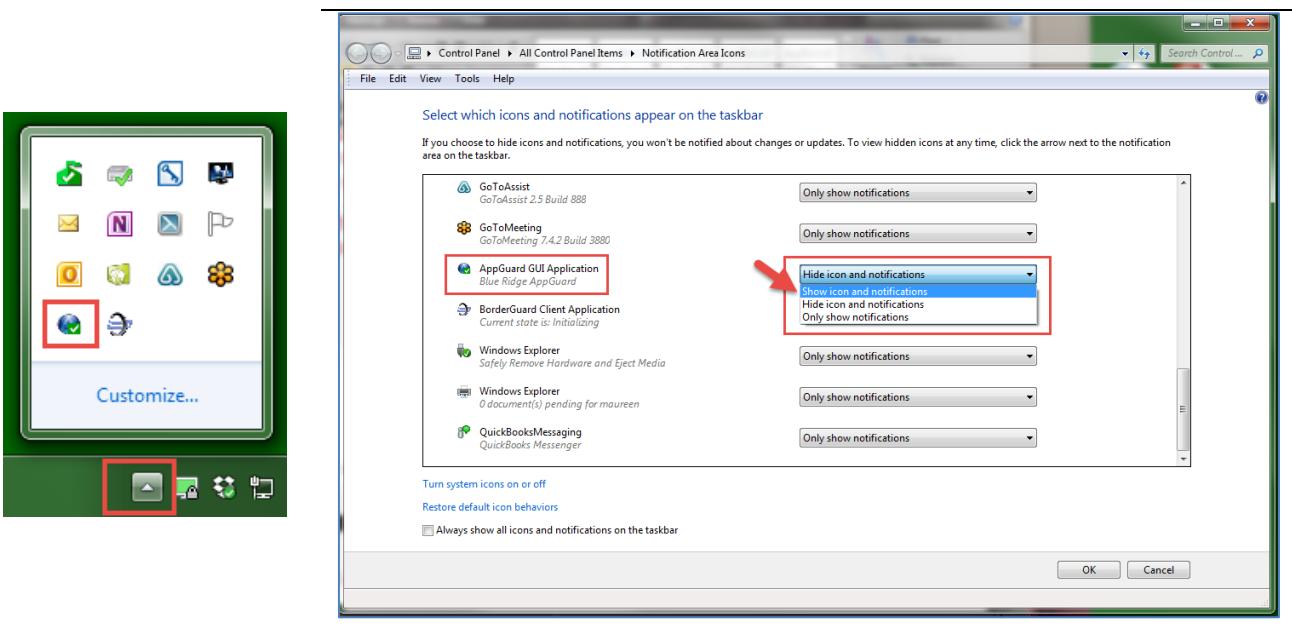
AppGuard Solo contains several types of protection:

- **Zero-day and unknown malware defense** – assumes all high target applications contain zero-day malware and guards them to prevent any zero-day exploit.
- **Drive-by Download Protection** stops suspicious programs from launching.
- **Application Containment/Guarded Execution** ensures protected applications are prevented from performing high-risk activities that might be exploited by malware.
- **MemoryGuard** prevents protected programs from writing to, or reading from, other processes' memory.
- **InstallGuard** prevents installation of programs from untrusted vendors.
- **Privacy Mode** prevents browsers from reading private folders.
- **Pre-Execution Controls and Run-time Protections** continually enforce policies.
- **File-less types of malware** which use built-in Windows tools are blocked by AppGuard Solo.

### AppGuard Solo System Tray Icon

AppGuard Solo's User Interface consists of the main user interface, log viewer and tray icon/menu. These interfaces are described in the sections to follow.

The install places an icon on the system tray at the bottom right of the screen. If the icon is not visible, click on the up arrow to Show hidden icons. You can also then click the **Customize** button to make the AppGuard Solo icon always visible.



## Protection Levels and AppGuard Solo User Interface

The AppGuard Solo user interface provides the current status of the AppGuard Solo protection level. AppGuard Solo allows you to change the protection level for installations, updates and other functions as required. The image below is the main AppGuard Solo user interface which describes the basic Protection Levels. Click on the AppGuard Solo icon to open the window.

**Protected:** All trusted applications are protected. If AppGuard Solo interferes with an application or if you want to access a private folder with an application, you can add protection for the application according to the instructions below while leaving the protection level at the Protected setting. Setting the protection level to Protected introduces minimal risk while providing the most protection.



**Allow Installs:** Use this level only when installing or updating software. Note that there is a default time of 20 minutes for this level of protection. This period can be changed in the Customize sections described below.



**Off:** Choose this option to temporarily turn AppGuard Solo protection completely off. **Note:** There is a default time of 20 minutes for this level of protection. This period can be changed in the "Customize" sections described below.



## Help

AppGuard Solo includes built-in help, accessible from a link on every user screen. Click on the link to bring up a comprehensive help program, including FAQs.

If you need further assistance, contact [Support@AppGuard.us](mailto:Support@AppGuard.us). Please include the following information in your email:

1. Version of AppGuard Solo, found by right-clicking on the tray icon and selecting the "About" option.
2. Explanation of your problem and any troubleshooting steps you may have tried.

Refer to the [Support](#) section for more detailed information.

## Definitions

The table below provides an explanation of terms used with AppGuard Solo and is itemized by categories.

These definitions and concepts are each used and described in detail throughout this document.

Protection
<b>Guarded Applications</b> AppGuard Solo provides multiple types of protection to endpoints. AppGuard Solo blocks malware by preventing the vulnerabilities in specified applications from being used by attackers to implant malware. This is achieved by blocking write operations of applications to the common targets of attackers (program files, system directories, critical registry keys, and more). AppGuard Solo will also automatically Guard any child processes launched by <a href="#">Guarded Applications</a> .
<b>InstallGuard</b> InstallGuard prevents end users and malware from installing or uninstalling software using the built-in Windows installer (msi) tools. All msi files which are digitally signed by Microsoft will be allowed to install in any protection level. All other installations require the <b>Protection Level</b> to be changed to <b>Install</b> . Refer to <a href="#">Important Software Installation Note</a> for further information.
<b>MemoryGuard</b>

Memory protection is designed to prevent one process (originator) from altering or reading the memory of another process (target). Attackers try to re-allocate memory, place executable code into the newly allocated memory, and then execute this code. This attack is called memory code injection or memory scraping. This type of attack is widely used in file-less malware, which exists only in memory, and Trojan malware.

### User Space Protection

User Space is the set of folders that are typically accessible by non-admin Windows users (the desktop, My Documents and removable media). To prevent drive-by download attacks and attacks from malware on USB removable memory devices, AppGuard Solo creates a set of application control policies. The User Space policies specify which applications are allowed to run if they are located in User Space. If a User Space application is permitted to run, AppGuard Solo policy can also specify post-launch controls on the application so that if it is compromised, it is unable to harm the system.

- If the program is signed by a publisher on the [Publisher List](#), then the post-launch controls defined in the publisher list will be applied.
- If the application is signed by a publisher **not** included in the default Publisher List, then the post launch controls are to Guard, MemoryGuard and execute in Privacy Mode.
- Scripts and unsigned applications are not allowed to execute at all.

### System Space Protection

System Space is protected by Guarding the applications most vulnerable to malware attacks. These are generally the most widely used applications, those that communicate to the Internet or handle information that originated from an untrusted source (Ex: an email attachment or a document downloaded from the Internet). AppGuard Solo includes a [default set of applications](#) which are already Guarded.

### Protected and Exception Folders

**Protected folders** are the areas of the system that Guarded applications are not permitted to alter. This is true even if the application is running with administrator privileges. The default policy includes the registry and all folders on the System drive (usually C:\) except for the user profile folder and program data folders.

**Exception folders** are those that Guarded applications are permitted to access. An example of an exception folder is C:\windows\scs\v2.0.6\namespace, which is a network folder and therefore usually restricted.

A default protected folder policy is included which denies access to "MyPrivateFolder" (created by AppGuard Solo during installation) under "My Documents".

### Control and Audit

#### Publishers

InstallGuard and Application launch control policy rules are based on the [Publisher List](#). Publishers can be added to the list along with their digital signing certificate.

#### Protection Levels

AppGuard Solo supports three [Protection Levels](#) to accommodate different situations. The end user can be prevented from changing the default Protection Level by using [Administrative Controls](#).

#### Power Applications

**Power Applications** are exempt from AppGuard Solo protections. In other words, Power Applications can access protected resources (even if launched by a Guarded Application) including the memory of a Guarded Application. Any application that is launched by a Power application also becomes a Power Application (even

Guarded Applications). Typically, only other security software products are added as Power Applications, and then only if AppGuard Solo indicates that it is blocking the security product's operation.

#### **Removable Media Access Control**

AppGuard Solo protects a computer from drive-by-download attacks by prohibiting the launch of executables from removable media by default.

#### **Logging**

All AppGuard Solo events and status messages are logged to the Windows Event Log, which can be viewed with the [Windows Event Viewer](#).

#### **Administrative Controls**

[Administrative Controls](#) provide a way to manage how AppGuard Solo can be modified by other users of the computer.

#### **AppGuard Solo Activity Report**

The [AppGuard Solo Activity Report](#) lists recent AppGuard Solo events on the main interface page.

- If the AppGuard Solo tray icon is flashing, open the Activity Report to see what is happening.
- Blocking actions are highlighted in red.

#### **TamperGuard**

AppGuard Solo includes **self-protection** features that prevent end users (even with local Administrator rights) and malware from stopping AppGuard Solo or tampering with AppGuard Solo's critical components. This prevents AppGuard Solo from being disabled.

### **Policy Related Terms**

#### **Application Guard List**

The [Guard List](#) is the set of applications that are explicitly configured to be Guarded by AppGuard Solo. For example, all Microsoft Office applications are Guarded by default.

#### **Privacy Mode**

AppGuard Solo prevents applications running in privacy mode from accessing (reading or writing) **Private Folders**. When AppGuard Solo is first installed, all browsers, User Space, and USB applications are executed in Privacy Mode, which stops them from accessing the My Documents\MyPrivateFolder directory created during install.

#### **Privacy Folders**

Applications running in **Privacy Mode** are forbidden from accessing any files in Private Folders. These folders are still accessible by unguarded applications as well as by guarded applications that are not running in **Privacy Mode**. When AppGuard Solo is installed, a new folder is also created in My Documents called "MyPrivateFolder".

## **User Interface**

### **Tray Icon**

The AppGuard Solo tray icon at the bottom right of your screen has two purposes:

1. Provides a status indication. The AppGuard Solo tray icon will flash to alert the user that AppGuard Solo has blocked an executable or installation package from launching. The icon will change, depending on the following states:



AppGuard Solo is in the Locked Down protection level, which is only accessible through the AppGuard Solo menu described below.



AppGuard Solo is in the Protected protection Level



This blinking icon state means that AppGuard Solo blocked either an application or script from executing.



At least one AppGuard Solo protection was disabled by the end user.

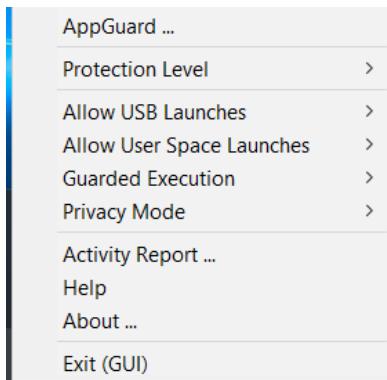


AppGuard Solo is in the Allow Installs protection level.



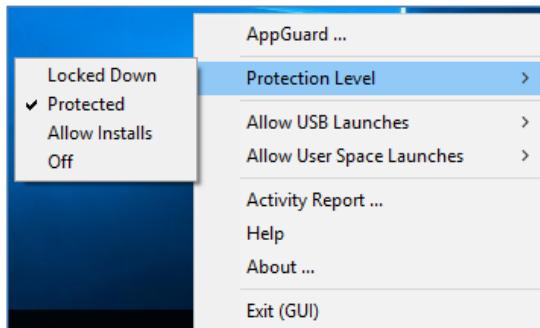
AppGuard Solo protection is off.

- When right-clicking on the tray icon, a menu will be displayed with the following options:



- AppGuard:** Displays the AppGuard Solo user interface
- Protection Level:** This menu option allows the user to change the protection level or **turn off** AppGuard Solo protection completely. The Locked Down protection level is available only through this menu.
- Allow USB Launches:** This menu option will enable the launch of an application or script from a USB memory device in either Guarded or unguarded mode.
- Allow User Space Launches:** This option will enable the launch of an application or script from User Space (the part of the computer for users) in either Guarded or unguarded mode.
- Guarded Execution:** This menu item will appear if you are running a Guarded Application. This will give you the option of unGuarding a single Guarded Application. If you unGuard one of your Guarded applications, this option will allow you to re-enable the protection.
- Privacy Mode:** This menu item will appear if you are running a Guarded Application in privacy mode. It gives you the option of suspending Privacy Mode for a single application. If you disabled privacy mode for an application, this option gives you the ability to reenable Privacy Mode.
- Activity Report:** Displays the AppGuard Solo activity events in an onscreen report. These events are then stored in the Windows Event Viewer.
- Help:** Displays the AppGuard Solo Help program.
- About:** Displays information about the AppGuard Solo application, including the version and the License ID. A link to the AppGuard Solo web page and the support email are also included.

- **Exit (GUI):** Closes the AppGuard Solo GUI application. The AppGuard Solo service continues to protect your system, but GUI alerts and notifications are suppressed.



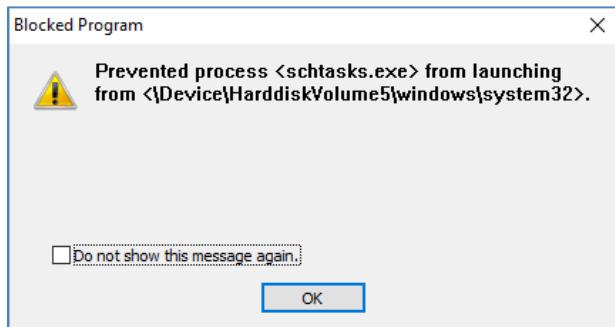
- **Locked Down:** This protection level is found using the process in the User Interface – Tray Icon section above. It eliminates the risk of drive-by download attacks by only allowing certain applications to run without restriction. In the Locked Down setting, AppGuard Solo may interfere with some programs such as GoToMeeting. If this occurs, reduce the AppGuard Solo protection level to Protected and initiate the GoToMeeting session. Then, return the protection level to Locked Down once the session is finished if desired.

## Popup and Toaster Messages

AppGuard Solo provides the user with notices about events in multiple ways. These alerts can be customized to show more or less events. The detail on customizing these alerts can be found in the “Customizing AppGuard Solo” section below.

### *Popup Messages*

Popup messages are displayed by default to alert users about blocked launches and privacy mode actions. A popup message requires the user to acknowledge the event and includes a checkbox to not show the message again. Refer to the Customizing AppGuard Solo section to display or hide more alerts.



## Toaster Messages

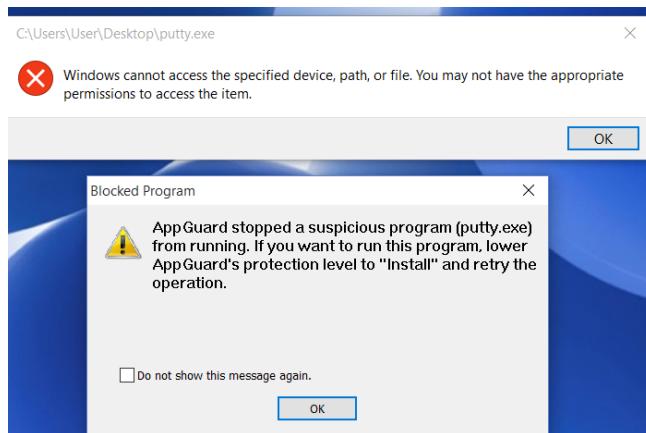
Toaster messages are displayed in the bottom right corner of the screen, last a few moments, and then disappear. Again, these messages can be customized in the Alerts tab using the **Customize** button, described in the Customizing AppGuard Solo section.



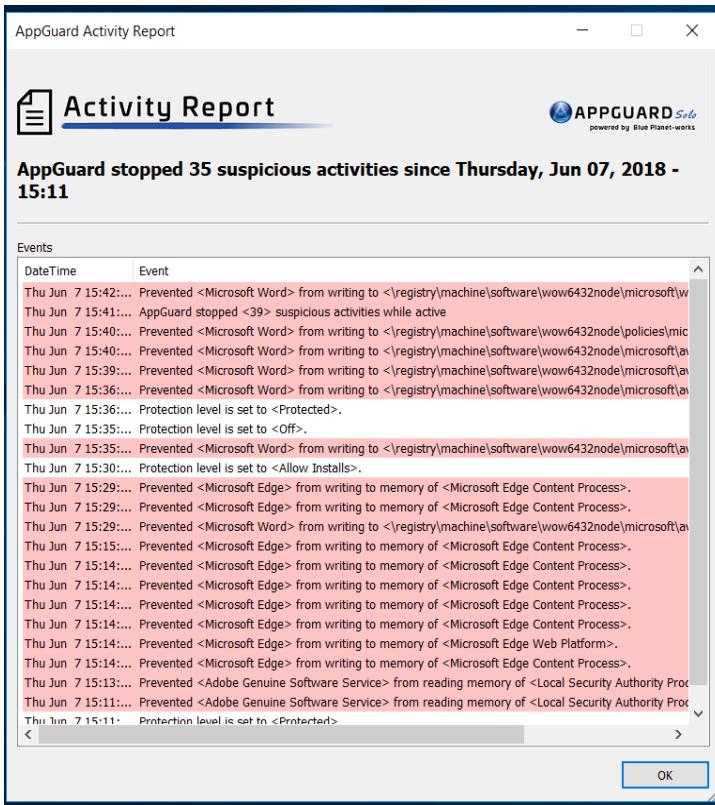
## AppGuard Solo Activity Report

To find out more about how AppGuard Solo is protecting your PC, click the **AppGuard Activity Report** button in the main AppGuard Solo interface.

These are the type of messages that will display if a launch is blocked. The one with the red X is a Windows message, and the bottom message is from AppGuard Solo. The AppGuard Solo icon will blink when this occurs, alerting the user to open the AppGuard Solo Activity Report and view the event



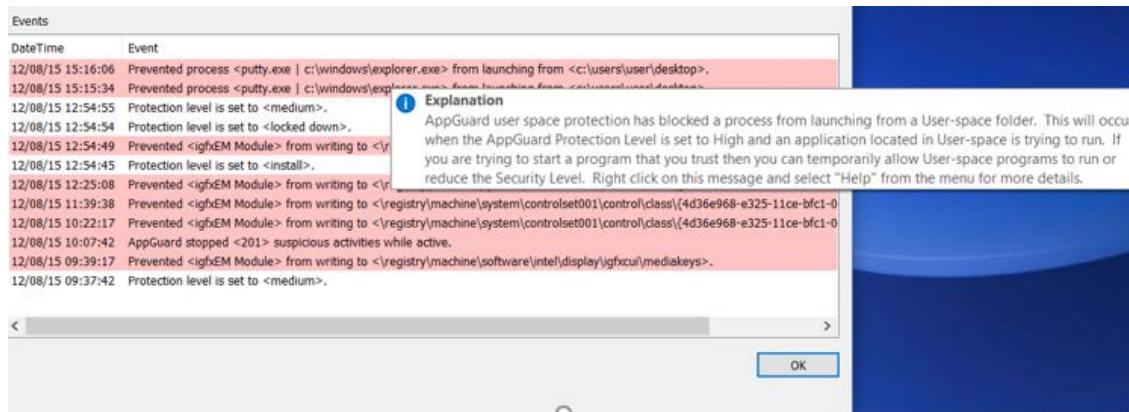
Open the AppGuard Solo main interface and click the **AppGuard Activity Report**. This will display the following types of events:



Malware-blocking events are found here. When the AppGuard Solo tray icon is flashing, open the AppGuard Solo user interface to find out what is happening. Blocking actions are highlighted in red. The following types of blocking events are reported when the Alert Level is set to the default settings:

- A potential User Space attack was stopped.
- A potential malware attack from a USB device was blocked.
- A suspicious installer file was prevented from executing.
- A protected application attempted a suspicious “write” operation.
- A protected program was prevented from reading or writing to the memory of another program.
- A protected program was prevented from writing into a protected registry key.

Move your cursor over any blocking event to see an explanation of the event:



View Help for a particular message by right-clicking on the event and choosing **Help** from the drop-down menu. This will bring up the online help, pointing to the specific issue.

**Events**

Date/Time	Event
12/08/15 15:16:06	Prevented process <putty.exe   c:\windows\explorer.exe> from launching from <c:\users\user\Desktop>.
12/08/15 15:15:34	Prevented process <putty.exe   c:\windows\explorer.exe> from launching from <c:\users\user\Desktop>.
12/08/15 12:54:55	Protection level is set to <medium>.
12/08/15 12:54:54	Protection level is set to <locked down>.
12/08/15 12:54:49	Prevented <igfxEM Module> from writing to <\registry\machine\system\controlset001\control\class\{4d36e968-e325-11ce-bfc1-0325-11ce-bfc1-0>.
12/08/15 12:54:45	Protection level is set to <install>.
12/08/15 12:25:08	Prevented <igfxEM Module> from writing to <\registry\machine\system\controlset001\control\class\{4d36e968-e325-11ce-bfc1-0325-11ce-bfc1-0>.
12/08/15 11:39:38	Prevented <igfxEM Module> from writing to <\registry\machine\system\controlset001\control\class\{4d36e968-e325-11ce-bfc1-0325-11ce-bfc1-0>.
12/08/15 10:22:17	Prevented <igfxEM Module> from writing to <\registry\machine\system\controlset001\control\class\{4d36e968-e325-11ce-bfc1-0325-11ce-bfc1-0>.
12/08/15 10:07:42	AppGuard stopped <201> suspicious activities while active.
12/08/15 09:39:17	Prevented <igfxEM Module> from writing to <\registry\machine\software\intel\display\igfxcu\mediakeys>.
12/08/15 09:37:42	Protection level is set to <medium>.

**Help...**

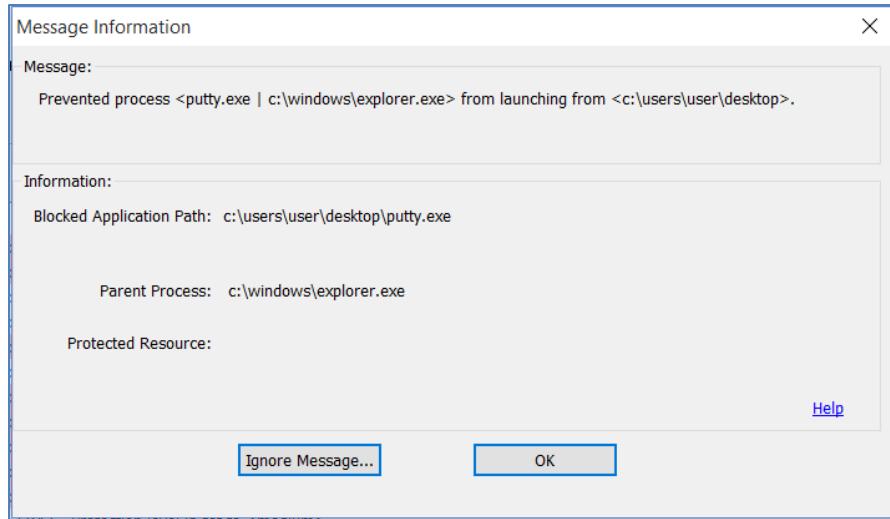
- Message Info...
- Ignore Message...
- Copy
- Select All
- Clear All
- Save As...

**Prevented process < process\_name > from launching from < folder\_name >**

AppGuard [user space protection](#) has blocked a process (process\_name) from launching from a folder (folder\_name) located in [user space](#). This message will occur when the AppGuard [Protection Level](#) is set to Medium or Locked Down and an application located in user space is attempted. When trying to launch a program that you trust then you can [temporarily allow launches from user space](#) or reduce the [protection level](#).

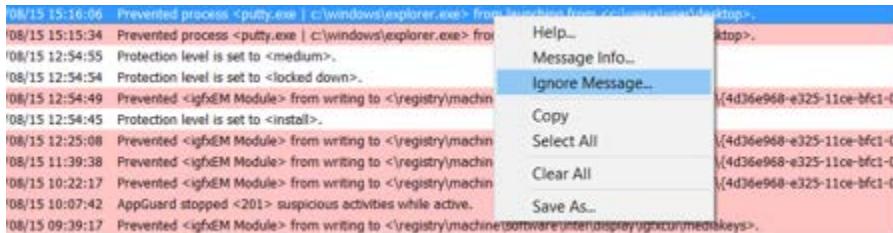
If you were not trying to start an application when this block occurred, then another program attempted to start the program. This could be

More details about the message can be viewed by selecting “Message Info” from the same menu:

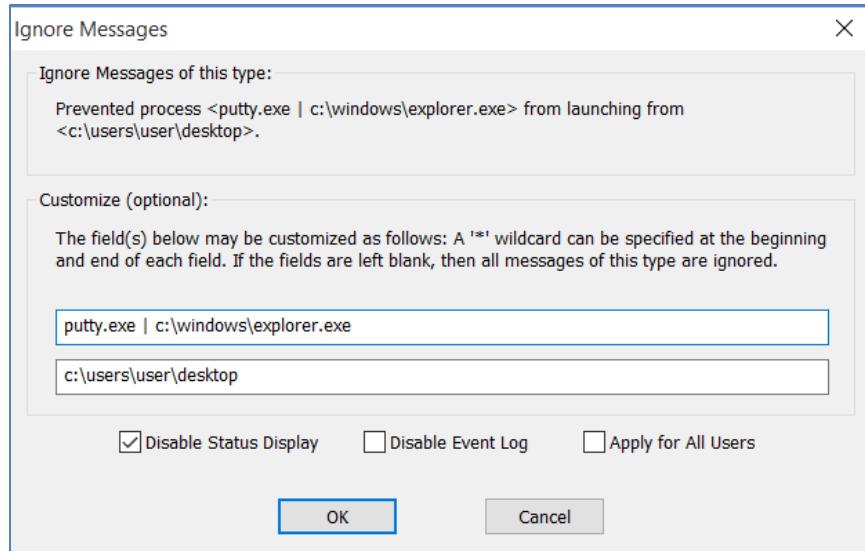


- Blocked Application Path:** The path of the application that is being blocked. In this case, putty.exe was blocked from launching from the desktop.
- Parent Process:** If the application is being launched by another application, the Parent Process will be shown. In this case, putty.exe is not a protected application, but it is being launched by Explorer.
- Protected Resource:** The resource that AppGuard Solo is protecting. In this case, there is no direct resource protected; putty cannot launch.

If you are getting blocking messages that are not interfering with normal operation and you prefer not to be notified, you can choose to suppress blocking messages by clicking on the **Ignore Message** button shown above, or right-clicking on the event and choosing **Ignore Message** from the drop-down menu:



This will display a window allowing you to ignore the message and choose how to suppress the message.

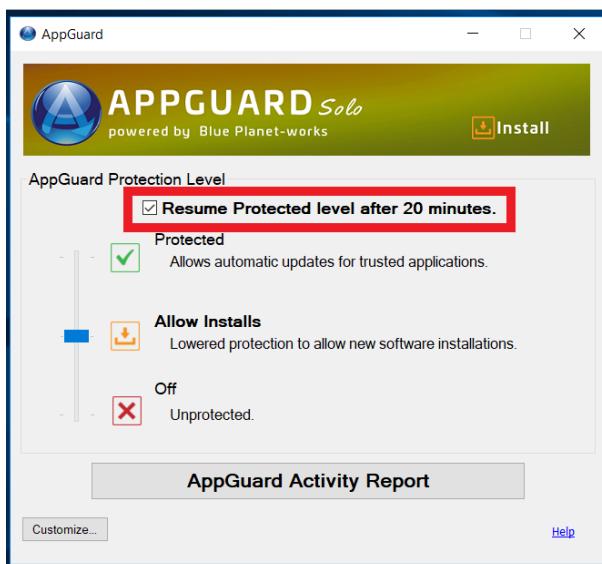


If you decide later that you would like to see a message that you previously set to ignore, you can either set the Alert Level to **All** or you can remove the message from the Ignored Messages List. This list is located on the Alerts Tab on the AppGuard Solo Configuration Interface.

The status messages will automatically clear out over time and are saved in the Windows Event Log.

## Important Software Installation Note

When installing applications, you must reduce AppGuard Solo's Protection Level to Install mode. If the software installation requires a reboot, check the "Automatically resume <protection level>" checkbox so the new software can continue installing after a reboot. AppGuard Solo will resume after 20 minutes. This suspension timeout value can be changed in the **Customize → Advanced tab**.



## Customizing AppGuard Solo Policy (Optional)

The default protection policy that is installed with AppGuard Solo generally does not require customization. If you wish to make changes or exceptions based on your system, the following information will help you to customize AppGuard Solo without compromising security.

The AppGuard Solo user interface allows you to customize AppGuard Solo for your computers. Click the **Customize** button to perform any customization.



Each of these tabs will be described in greater detail in the sections following.

- Change the Alert Level and manage Ignored Messages.
- Modify the definition of User Space.
- Add or remove an application from the Guarded Apps list.
- Modify the Trusted Publisher list.
- Modify the Advanced settings.

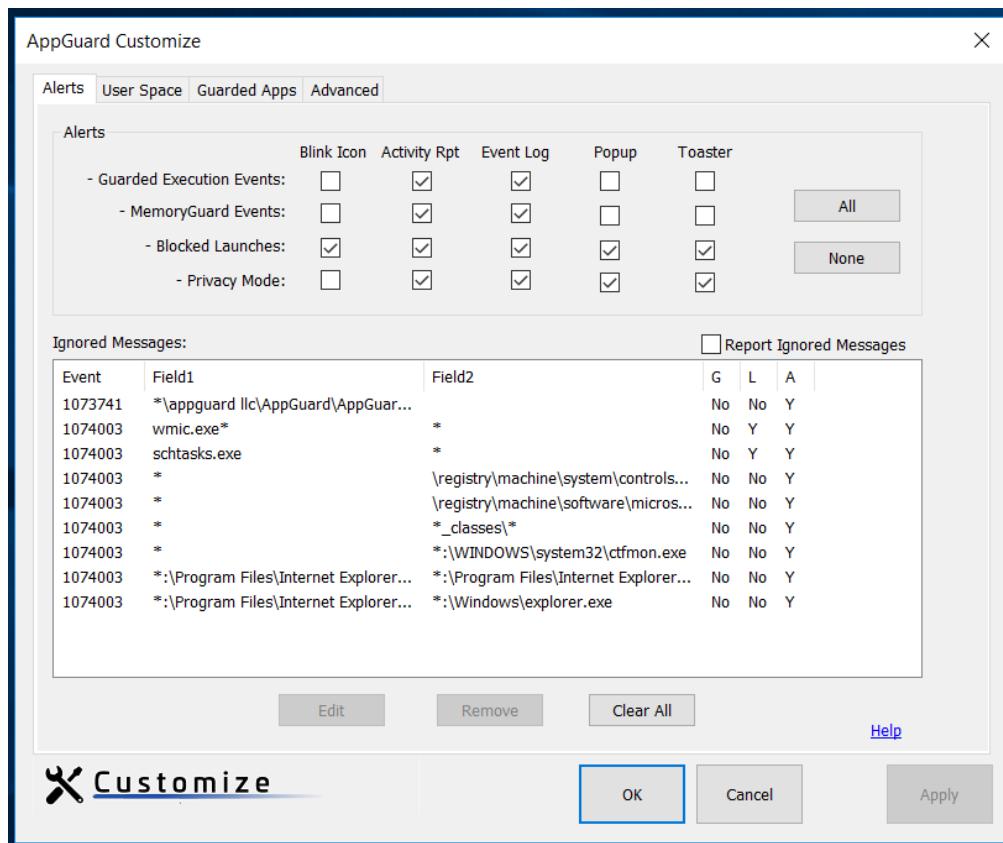
### Alerts Tab

AppGuard Solo reports events in multiple ways:

- The AppGuard Solo tray icon **blinks**.
- Status reports are sent to the **AppGuard Solo Activity Report** user interface.
- The event is sent and saved to the **Windows Event Log**.
- Both **toaster** and **popup** messages alert the user about events.

AppGuard Solo reports the following types of events:

- Guarded Execution Events:** These events occur whenever AppGuard Solo prevents an application from performing a risky operation.
- MemoryGuard Events:** These events occur whenever AppGuard Solo prevents an application from reading from or writing to the memory of another process.
- Blocked Launches:** These events occur whenever AppGuard Solo blocks an application or installation file from running.
- Privacy Events:** These events occur when AppGuard Solo blocks an application from accessing a private folder.



**Popup** messages must be acknowledged by the user; **toaster** messages are displayed in the bottom right corner for a bit and then disappear. To get the alerts for any of the types of events described above, simply check the box for the alert(s) and then click **Apply** or **OK**. It can be unchecked at any time.

To change any of the Alerts settings, simply check or uncheck the setting as desired and click the **Apply** or **OK** button.

- To quickly turn on all alerts, click the **All** button followed by the **Apply** or **OK** button.
- To turn off all alerts, click the **None** button followed by the **Apply** or **OK** button.
- To restore the Alerts setting to the default settings, enable Privileged Mode on the Advanced Settings tab and click the **Reset all settings to default** button.

The Alerts tab also contains the controls for managing the Ignored Messages list.

- To Un-Ignore a message, select the message in the Ignored Message list and click the **Remove** button.
- To display Ignored Messages without removing them from the Ignored list, check the **Report Ignored Messages** checkbox.

## User Space Tab

User Space refers to the computer storage space that is typically accessible by non-admin Windows users. It contains the user's profile directory (which includes the My Documents folder and Desktop), removable storage devices, network shares, and all non-system hard drives such as additional external and internal disk drives. AppGuard Solo will either block or protect the execution of any programs contained in User Space directories.

AppGuard Solo protects a computer from User Space attacks by stopping the launch of executables from User Space (e.g., My Documents, Desktop, etc.), non-system internal or external hard drives (D:\, E:\, etc.), removable media, and network drives. These initial directories included in the AppGuard Solo protection cannot be deleted, but other folders can be added.

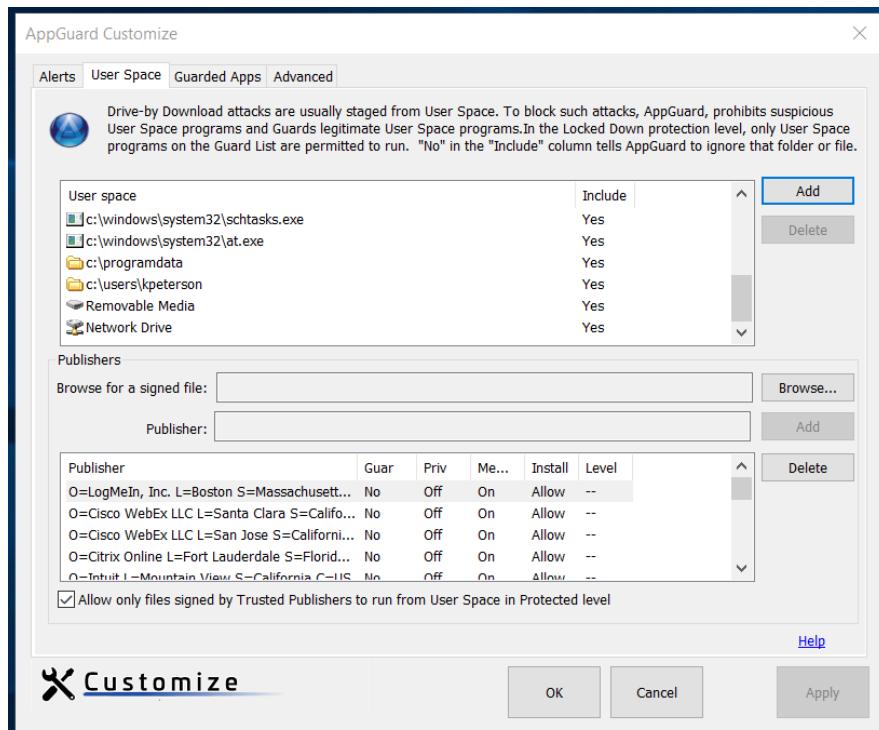
### Adding User Space Folders

You can define your own set of directories to protect by including them in the User Space definition. When you specify a folder to include in User Space, all sub-folders will be protected as well. To add a User Space folder, click the **Add** button and either type or navigate to the directory name.

The default entries cannot be deleted or modified.

### Defining User Space Exclusions

Select “No” in the **Include** column to specify any drives, sub-folders or files within a protected folder where you might want to allow launches (be sure to click **Apply** or **OK** after making any changes). This applies only to directories you have added, not to the default AppGuard Solo directories.



This feature might be helpful to facilitate Google updates, for example. If you exclude the Google Update directory (C:\Documents and Settings\<username>\Local Settings\Application Data\Google\Update\ Download) from User Space, AppGuard Solo will allow the updates to install while still protecting the rest of User Space.

## Network Drives

AppGuard Solo includes all network drives in User Space to prevent malware from attacking your PC. If you want to allow programs to execute from a particular network drive, explicitly exclude that network drive from the User Space definition by adding it to the folder list and select “No” in the **Include** column. See [Folder Settings](#) for more information on how to do this.

## White-listing User Space Executables

User Space executables can be “white-listed” by excluding them from User Space. An example of a User Space executable is putty.exe on a desktop. Click the **Add** button and browse to the executable.

Add the file and set the Include column to **No** (note when browsing to a file, select the file and click the **OK** button – do NOT double-click the file). The executable will no longer be considered part of User Space and will be allowed to execute in all protection levels. These executables will not be protected unless they are launched (or loaded) by a protected application.

## Publishers List

When not in the Locked Down protection level, AppGuard Solo’s default policy will allow User Space applications and installations to execute if they are digitally signed by a publisher contained in the Publisher list. It is possible (though not recommended) to allow *any* digitally signed application to run by unchecking the “Allow only files signed by Trusted Publishers to run from User Space in Protected level” box.

## Default Publisher List

This is the list of publishers included in AppGuard Solo by default. You can add, delete, and specify protections by following the directions below.

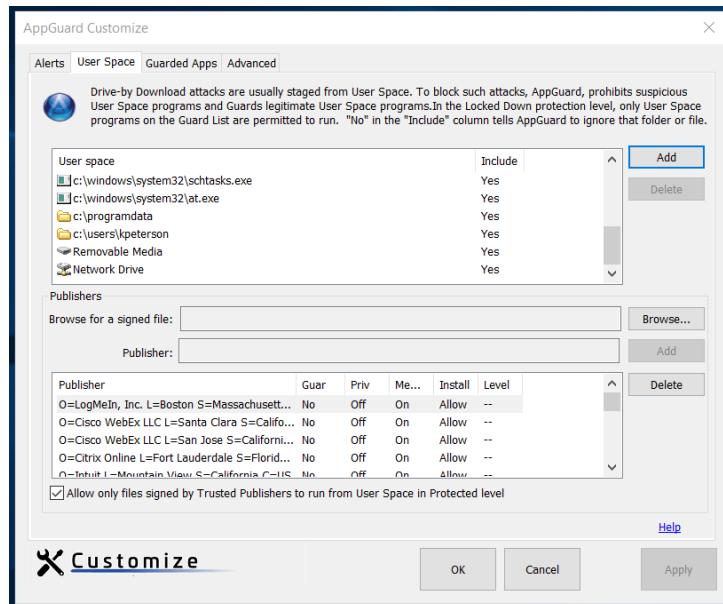
Publisher	Guarded	Privacy	Memory	Install	Level
Adobe	No	Off	On	Allow	
Apple	No	Off	On	Allow	
Blue Ridge Networks	No	Off	Off	Allow	Install
Citrix	No	Off	On	Allow	
Cisco WebEx	No	Off	On	Allow	
Google Chrome	No	Off	On	Allow	
Internet Explorer	No	Off	On	Allow	
Intuit	No	Off	On	Allow	
LogMeIn	No	Off	On	Allow	
McAfee	No	Off	Off	Allow	Install
Microsoft	No	Off	On	Allow	
Mozilla Firefox	No	Off	On	Allow	
Oracle	No	Off	Off	Allow	Install
Sun Microsystems	No	Off	On	Allow	
Symantec Corporation	No	Off	On	Allow	

For each publisher, the following can be specified:

- **Guarded:** Indicates whether a User Space program published by this publisher should be protected when it executes.
- **Privacy:** Indicates whether a User Space program published by this publisher should execute in privacy mode.
- **MemoryGuard:** Indicates whether a User Space program published by this publisher should be prevented from accessing another program's memory when it executes.
- **Install:** Indicates whether installation programs published by this publisher should be permitted, including updates.
- **Level:** indicates AppGuard Solo will automatically lower the level to Install for that publisher when a program digitally signed by that publisher is executed from User Space.

Click the **Browse** button to browse for a signed executable or use the **Delete** button to remove a publisher.

When AppGuard Solo is first installed, several publishers are contained on the Publisher List as noted. AppGuard Solo will also allow Publishers on this list to automatically install updates for their products, such as Windows, Microsoft, Quicken (Intuit), and Java (Oracle).



To add a Publisher, click the **Browse** button in the middle of the screen and navigate to a digitally signed file (\*.exe, \*.dll, or \*.ocx). If it is digitally signed, AppGuard Solo will automatically populate the Publisher field. The **Add** button will be enabled if the publisher is not already contained in the publisher list (if the publisher is already in the list, the **Add** button will remain disabled). The defaults for publishers are:

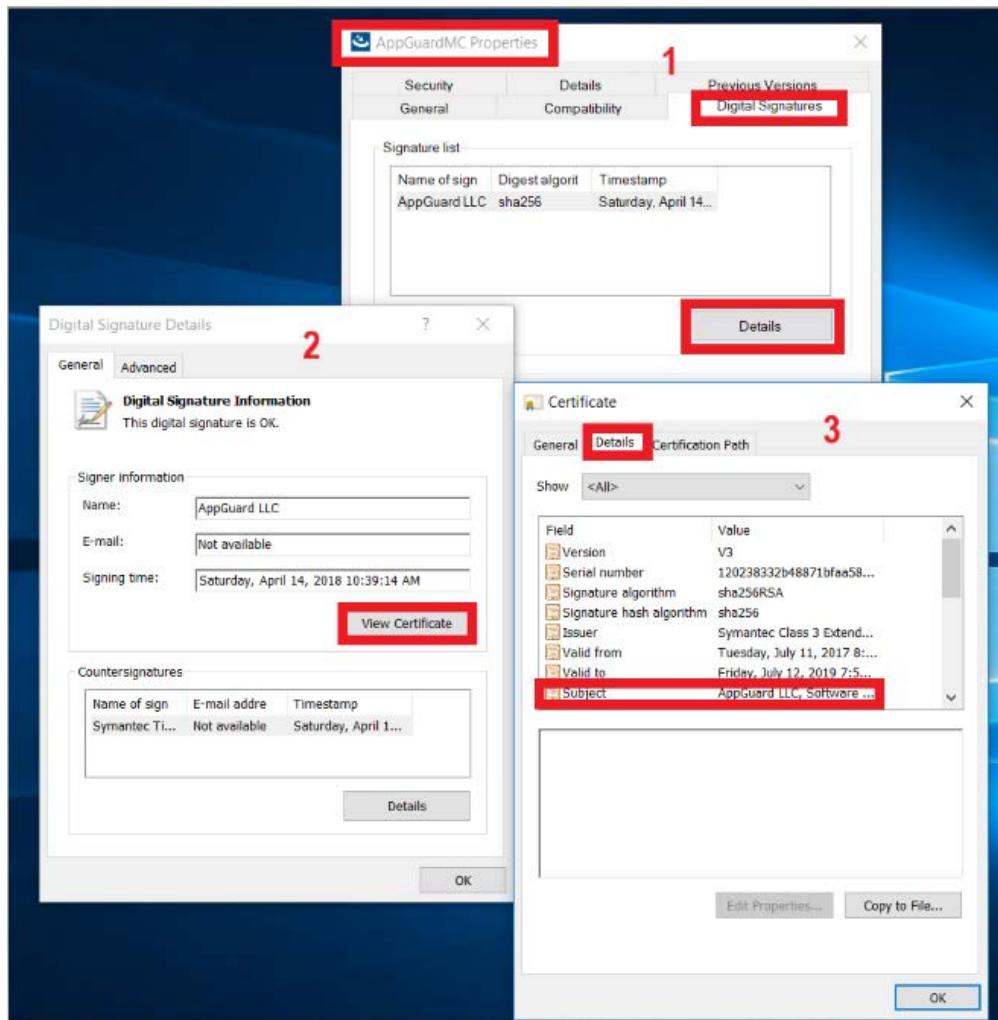
1. Guard an application.
2. Privacy mode is off.
3. MemoryGuard is on, except for some security applications.
4. Install (including updates) is Allowed.
5. Level is not applicable.

Make any changes required by clicking on the column and selecting the right response.

Not all files are digitally signed. To verify if a file has a digital signature, select the file, right-click on it and select "Properties". The file properties will have a Digital Signatures tab if it is digitally signed. Follow the steps in the picture below to verify the certificate information.

## Automatic Updates

If an application is digitally signed, and you would like to allow automatic updates, add the publisher using the directions above, but do not Guard the publisher.



## Guarded Apps Tab

The Guarded Apps tab provides a list of the currently guarded applications. On this tab, you can alter the Privacy and MemoryGuard settings for a protected application. You can also disable protection as well as add additional

applications to the Guarded Apps list if you find that protecting the application is interfering with its normal behavior. You may also remove any applications included by AppGuard Solo as default.

Note that not all the Guarded Apps listed in the chart below will be displayed; AppGuard Solo only displays those applications currently installed on your computer.

### Guarded Apps List

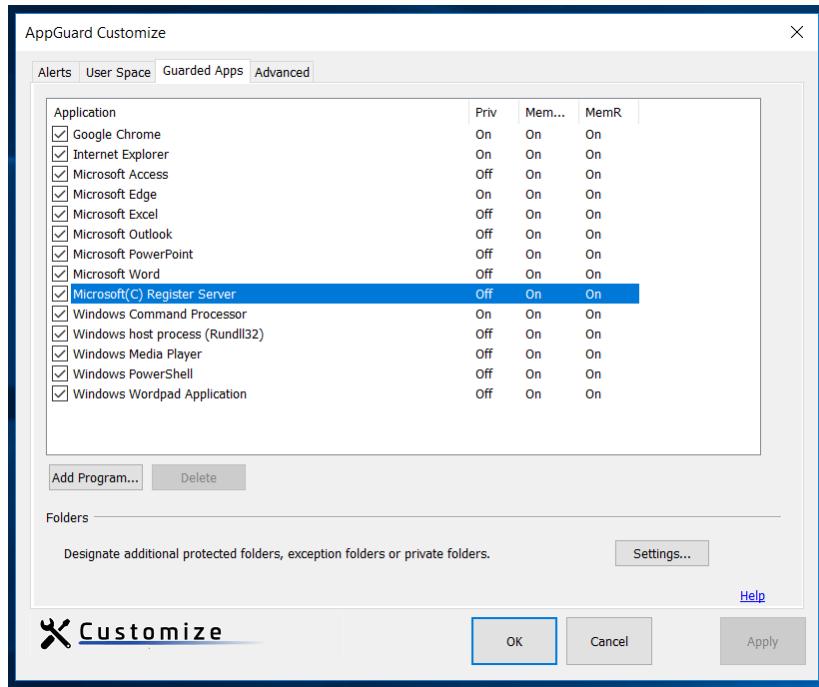
AppGuard Solo prevents applications on the Guarded Apps list from performing high-risk activities that might be exploited by malware. The Guarded Apps tab can be accessed through the **Customize** button on the main user interface.

Most widely deployed applications are automatically protected by AppGuard Solo, as are several programs that are commonly used as attack vectors. The following programs are configured to be protected. This is a comprehensive list; please note that only those applications actually installed on your computer will show up in your own Guarded Apps list. Note that the MemoryGuard functions are separated into Memory Read and Memory Write.

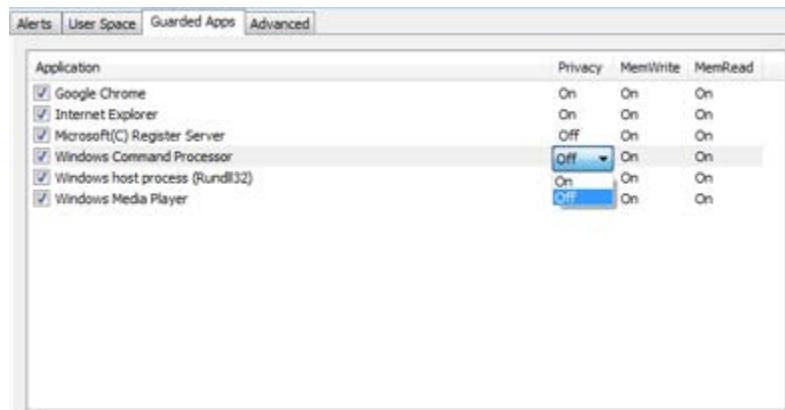
Application	Privacy	Memory Write	Memory Read
Acrobat Reader	Off	On	On
AOL Desktop (Browser)	On	On	On
AOL Instant Messenger	On	On	On
Google Chrome	On	On	On
Internet Explorer	On	On	On
Mozilla Firefox	On	On	On
Opera	On	On	On
Microsoft Office Access	Off	On	On
Microsoft Office Excel	Off	On	On
Microsoft Office Outlook	Off	On	On
Microsoft Office PowerPoint	Off	On	On
Microsoft Office Word	Off	On	On
Microsoft Register Server	Off	On	On
Power DVD	Off	On	On
Windows Host Process (Rundll32)	Off	On	On
Outlook Express	Off	On	On
Windows Command Processor	Off	On	On
Windows Media Player	Off	On	On
VLC Media Player	Off	On	On

### Folders Settings

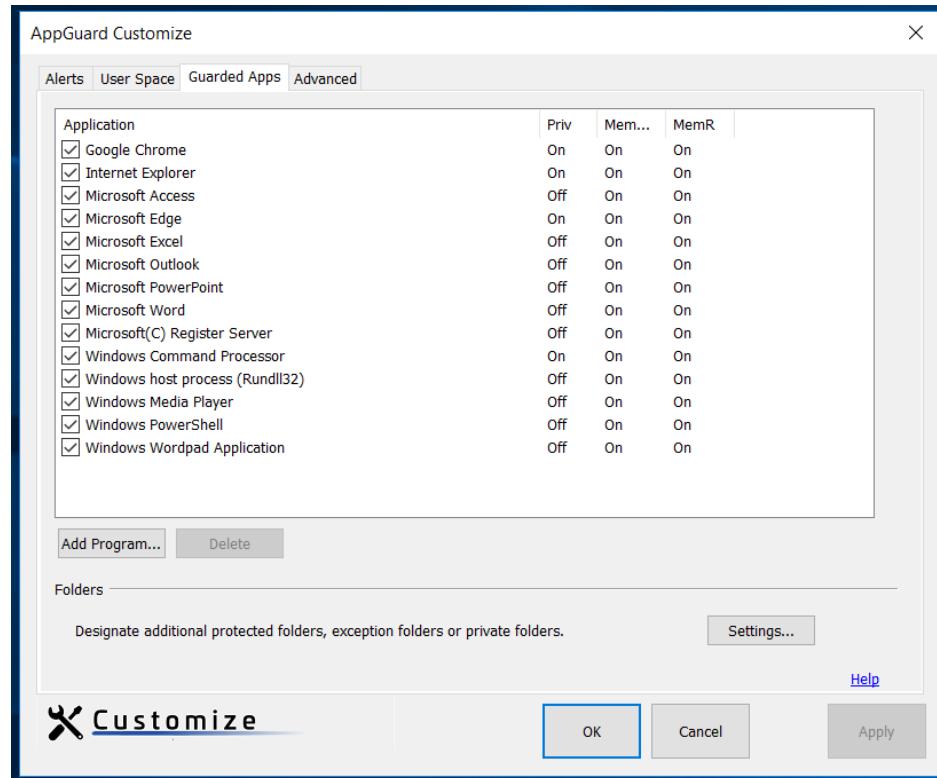
From the Guarded Apps tab, you may add additional Protected Folders, Private Folders, Exception Folders and Files.



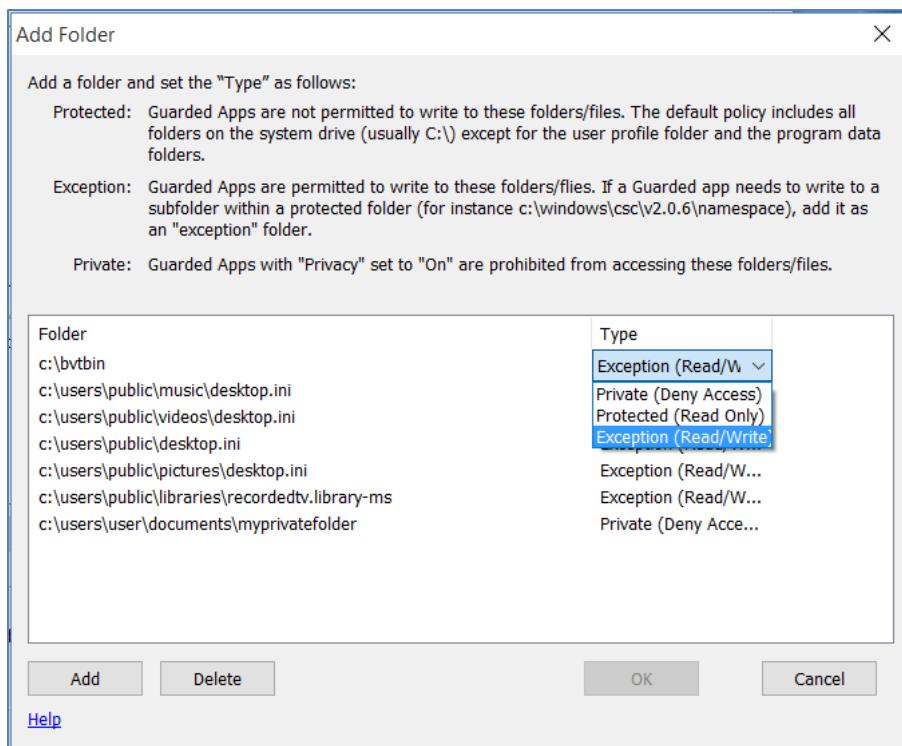
To change the Privacy Mode or Memory settings, select the Application and change the appropriate column to **On** or **Off**:



To add additional Protected Folders, Private Folders or Exception Folders and Files click the **Settings...** button.



The following will be displayed. Click the **Add** button to specify a new folder. For a detailed description of each folder type refer to the description section at the top of the window.



After the folder is added, change the “Type” column as follows:

- For a Protected Folder: Read Only
- For an Exception Folder: Read/Write
- For a Private Folder: Deny Access

## Protected Folders

AppGuard Solo prevents protected applications from writing to a set of protected folders and registry settings. By default, AppGuard Solo prevents applications from writing to all folders on the System Drive (usually C:\) except for the user profile directory and the program data directory.

Folder	XP Folder	Win7 or VISTA Folder
User Profile	C:\Documents and Settings\John	C:\Users\John
Program Data	C:\Documents and Settings\All Users\Application Data	C:\ProgramData

Sometimes users require that software applications be installed elsewhere such as a separate partition or hard drive. These locations are not regarded as system-space by default; therefore, malware or hackers could maliciously modify these applications, transforming them into harmful tools.

Following the instructions above, use the **Add** button on the Guarded Apps tab to add a protected folder. After the folder is added, change the Type to **Read Only**.

## Exception Folders

If a protected application requires write access to a folder or file within a protected folder, you will need to add an exception folder or file. For example, on some operating systems Windows Media Player requires access to several files within C:\users\public.

Following the instructions above, use the **Add** button on the Guarded Apps tab to add a protected folder. After the folder is added, change the Type to **Read/Write**.

## Private Folders

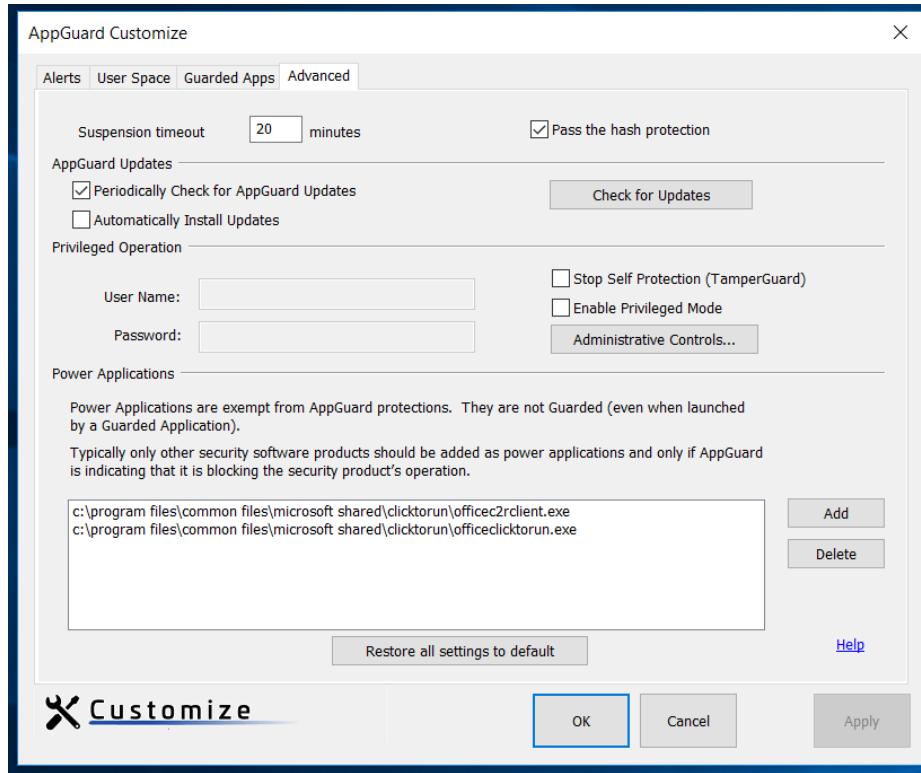
Private folders cannot be accessed by applications running in privacy mode. By default, “My Documents\MyPrivateFolder” is created during the AppGuard Solo install and included as a private folder.

Following the instructions above, use the **Add** button on the Guarded Apps tab to add a protected folder. After the folder is added, change the Type to **Deny Access**.

## Advanced Settings Tab

The Advanced Settings tab allows the user to:

- Set the suspension timeout value.
- Set the policy for AppGuard Solo Updates.
- Set Administrative Controls and Super Users.
- Disable/enable Self Protection.
- Disable/enable Privileged Mode.
- Add Power Applications.
- Restore all settings to default.



The following sections provide more details about AppGuard Solo's advanced settings.

### Suspension Timeout

When a user changes the protection level to Install, a default suspension timeout value of 20 minutes starts. After 20 minutes, the protection level will automatically return to the default Protected level.

### Pass the hash protection

When this box is checked, AppGuard is protecting against pass the hash and pass the ticket attacks.

### AppGuard Solo Updates

The user can choose to periodically check for AppGuard Solo updates, as well as whether or not to automatically install any update it finds. There is also a button to check for updates now for AppGuard Solo. The default is to periodically check for updates, but not to automatically install updates. The user will be reminded to install periodically.

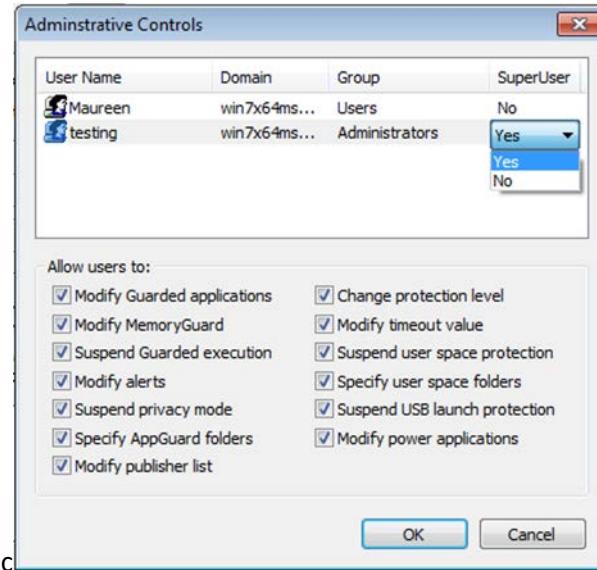
### Privileged Operation - Administrative Controls

Administrative Controls provide a way to manage how AppGuard Solo can be modified by other users of the PC.

Until a Super User is specified in the Administrative Controls dialog, all users are considered AppGuard Solo Super Users. This means that any user on the computer is able to temporarily suspend protections, and any Windows Administrator is able to uninstall AppGuard Solo. Click the **Administrative Controls** button to get started.

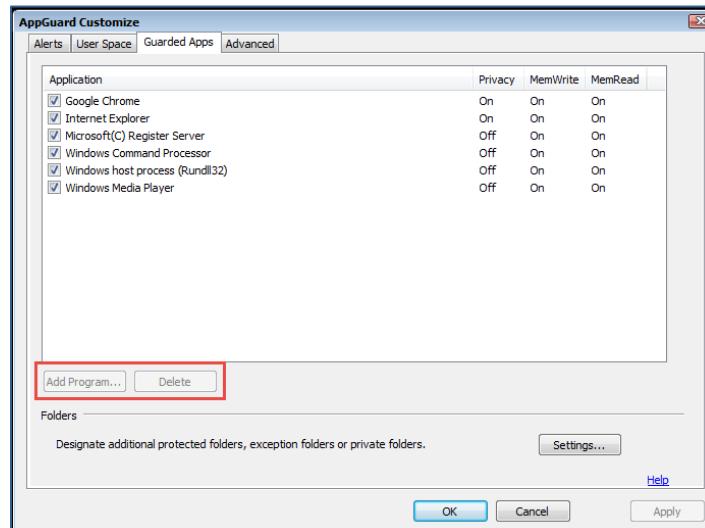
1. Designate the desired Windows login account(s) as an AppGuard Solo Super User.

2. The AppGuard Solo Super User can then designate which AppGuard Solo permissions are available to non-Super Users. Designate any user accounts that you would like to be Super Users, modify the check boxes as desired, and then click **OK**.
3. Once a Super User account has been created, only a Super User is permitted to modify the default policy or uninstall AppGuard Solo.



Important: Make sure you know the Windows credentials for at least one of the Super User accounts. Once a Super User is designated, the login credentials of a Super User are required in order to modify Administrative Controls.

If no permissions are allowed, then most of the controls on the user interface will be disabled. For example:



Additionally, the tray menu will only display those controls which are allowed:



Administrative controls will apply to all non-Super Users. A Super User can disable Administrative Controls on behalf of the non-Super Users by enabling Privileged Mode. In Privileged Mode any AppGuard Solo protection can be temporarily suspended.

To permanently remove Administrative Controls, remove all Super User designations.

### **Self-Protection**

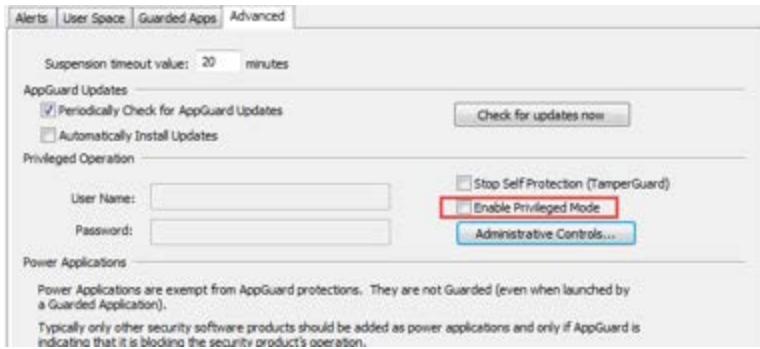
AppGuard Solo prevents end users and malware from stopping AppGuard Solo or tampering with AppGuard Solo's critical components. This ensures that AppGuard Solo is always protecting your computer.

Self-protection can be disabled from the Advanced tab by checking the box. This should be done only to uninstall AppGuard Solo, or to be able to stop the AppGuard Solo service. If Administrative Controls are activated, then only Super Users can disable self-protection. When self-protection is disabled, the AppGuard Solo service can be stopped from the Windows Services Control Panel. In addition, the AppGuard Solo default policy file can be modified when self-protection is disabled.

### **Privileged Mode**

AppGuard Solo has two modes of operation: Normal Mode and Privileged Mode. In Normal mode, all users are restricted as to which AppGuard Solo protections they can control or suspend. Super Users are restricted to the permissions specified in the default policy while regular users are further restricted by Administrative Controls (if defined). Running in Privileged Mode enables any user to temporarily suspend any AppGuard Solo protection. This is true even if Administrative Controls or default AppGuard Solo policy does not permit the suspension. Privileged Mode also enables a "factory reset" of the user's AppGuard Solo policy. This is done by clicking the **Reset all settings to default** button that appears at the bottom of the AppGuard Solo Configuration Interface when in Privileged Mode.

Privileged Mode can be enabled from the Advanced tab by checking the box. If a regular user is logged into Windows (and at least one Super User is defined), then the Windows login credentials of one of the designated Super Users is required to enable Privileged Mode. Otherwise, a regular user can check the box without restrictions.



Privileged Mode is in effect until the Privileged Mode box is unchecked. This is true even if a user logs out and another user logs in.

The following table illustrates which operations are allowed for each type of user and in privileged mode:

Operation	Super User	User	Privileged
Enforce Administrative Controls	N	Y	N
Modify Administrative Controls	Y	N	Y
Uninstall AppGuard Solo	Y	N	Y
Suspend TamperGuard	Y	N	Y
Designate Super Users	Y	N	Y
Return all settings to default	N	N	Y

Designate any user accounts that you would like to be Super Users by changing the Super User column from No to Yes and click OK.

## Power Applications

In rare cases, AppGuard Solo's protection may interfere with a program's operation. Power Applications are exempt from AppGuard Solo post-launch protections. In other words, they are not guarded or memory guarded (even if they are launched from a guarded application). Caution should be taken when adding Power Applications especially from user-space as they may not be protected by AppGuard Solo and may even become an attack vector used by sophisticated zero-day malware. Typically, only other security software products should be added as Power Applications and only if AppGuard Solo is indicating that it is blocking the security product's operation. Applications launched by a Power Application are also considered to be Power Applications.

To determine if AppGuard Solo is interfering with an application, examine the AppGuard Solo events on the main AppGuard Solo Activity Report user interface. You may see messages similar to those below:

```

Prevented < Antimalware Service Executable > from reading memory of < Microsoft Outlook >.
Prevented < Antimalware Service Executable > from writing to memory of < Microsoft Outlook >.
Prevented < Antimalware Service Executable > from reading memory of < Google Toolbar Broker >.
Prevented < Antimalware Service Executable > from reading memory of < Internet Explorer >.
Prevented < Antimalware Service Executable > from writing to memory of < Internet Explorer >.

```

In the case of most applications the above events are not disruptive, but for a security product, the above blocking events may indicate that AppGuard Solo is interfering with the security product's operation. To allow a security product to operate without AppGuard Solo blocking its operation, the security product's executable should be added to the Power Applications list on the Advanced tab. If AppGuard Solo is blocking other security program operations, it is because of one of the following reasons:

- The security product has been added to the Guarded Apps list. Typically, security products should not be added to the Guarded Apps list. If that is the case, remove the security product from the list.
- The security product is located in User Space. In this case, consider installing the security program in system space (i.e. Program Files). If that is not possible, the executable should be added to the Power Applications list. Also consider adding the file's path as a protected resource folder on the Guarded Applications tab.
- The security product is being launched by a protected application. In this case the security product executable should be added to the Power Applications list.
- The security product is trying to launch a program that is not permitted by AppGuard Solo User Space policy. Adding the security application to the Power Applications list should remedy the problem.

## Restore All Settings to Default

Clicking the **Restore all settings to default** button on the Advanced tab will restore all AppGuard Solo's settings to the default settings that were installed with AppGuard Solo. Any user modifications will be lost.

## Application Notes

### Running with UAC Enabled

If the user overrides an AppGuard Solo blocking event through UAC, AppGuard Solo will not interfere.

### Click-to-Run Applications

Click-to-Run Applications (such as Office Starter) are streamed from the Internet to a virtualized disk (usually the Q: drive) on your computer. Because these applications are not always digitally signed, AppGuard Solo prevents them from running in the Locked Down protection level. They can be launched by placing the AppGuard Solo protection level back to Protected. When launched in the Protected level, these applications are automatically protected by AppGuard Solo.

Another option is to exclude the "Q" drive from User Space. This will enable these applications to be launched in the Locked Down protection level. Although AppGuard Solo will not protect these applications, Microsoft's virtualization provides some isolation of these applications from the critical components of the OS.

### Google Chrome

In order to use Google Chrome in the Locked Down protection level, do either of the following:

- Install Google Chrome in the Program Files directory (preferred).
- Exclude the following directories from the User Space protection definition:
  - C:\Users\<UserName>\AppData\Local\Google\Chrome\Application
  - C:\Users\<UserName>\AppData\Local\Google\Update

## Network Shares Anomalies

The following are known anomalies with AppGuard Solo 6.0.

1. Sometimes protected execution of an application located on a network share drive cannot be suspended from the tray menu. If you encounter this problem, suspend the application from the Guarded Apps tab on the AppGuard Solo Customize interface.
2. Using a mapped drive letter (vs. the computer name) to specify a Guarded Application path is not supported. Instead, use “<\\FullyQualifiedSharePath\shared\program.exe>” vs. “z:\shared\program.exe” to include program.exe in the Guard List.

## Support

There are multiple ways to get information or support.

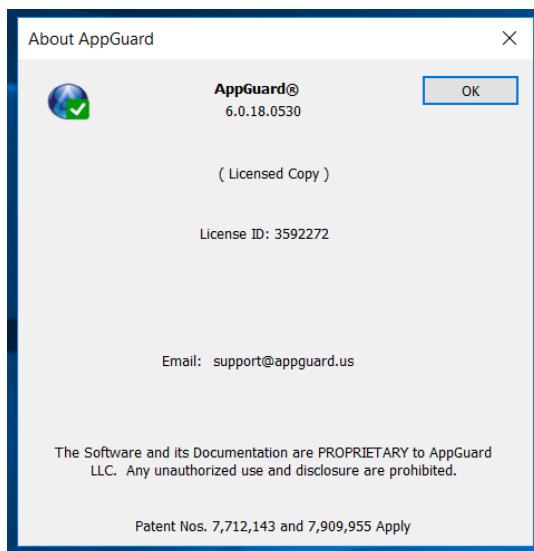
### Product Online Help

The comprehensive help menu can be accessed from any page by clicking the **Help** link in the bottom right corner. Detailed information is provided about the majority of blocking events and includes a Troubleshooting FAQ section.

### Contact Support

If you have any questions about AppGuard Solo, or require troubleshooting assistance, please contact support and include the information about your version and License ID. These are displayed in your “About AppGuard Solo” window, accessed by right-clicking on your tray icon, and selecting “About...” from the menu.

Email support: [support@appguard.us](mailto:support@appguard.us)



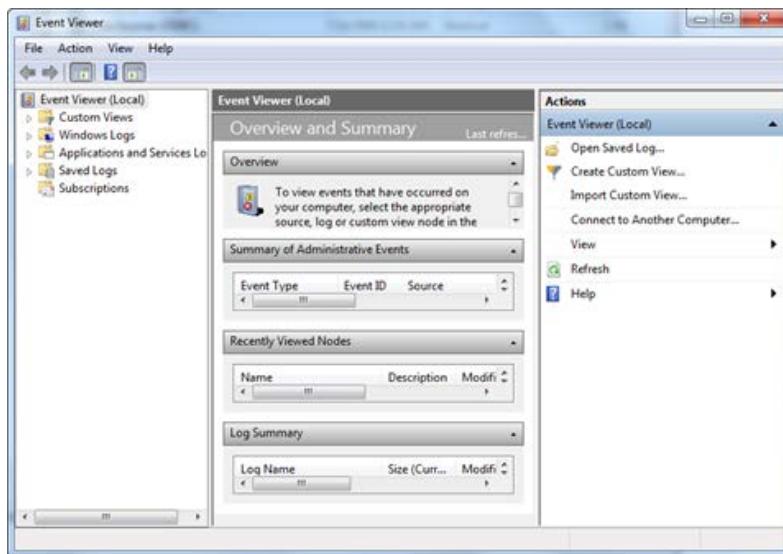
## Windows Event Viewer

All AppGuard Solo events and status messages are logged to the **Windows Event Log**, which can be reviewed with the **Windows Event Viewer**. To view or download AppGuard Solo events in the Windows Event Viewer, follow these steps.

1. To view and collect events, open the Windows Event Viewer (type “Event Viewer” in the Start Menu):



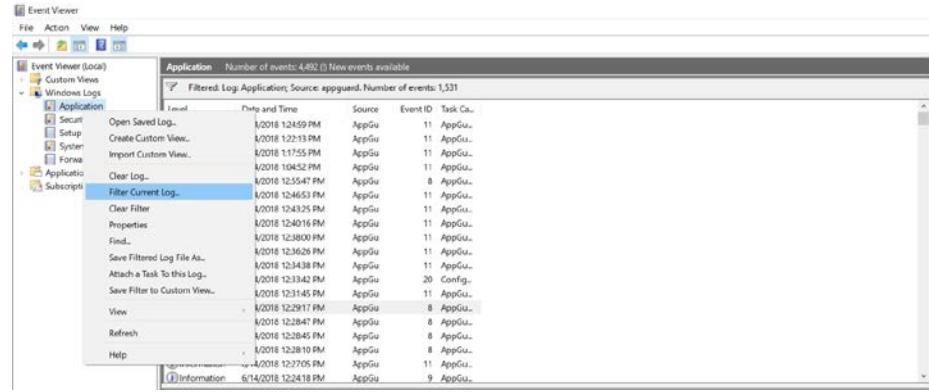
2. When you open the Windows Event Viewer you should see the following screen:



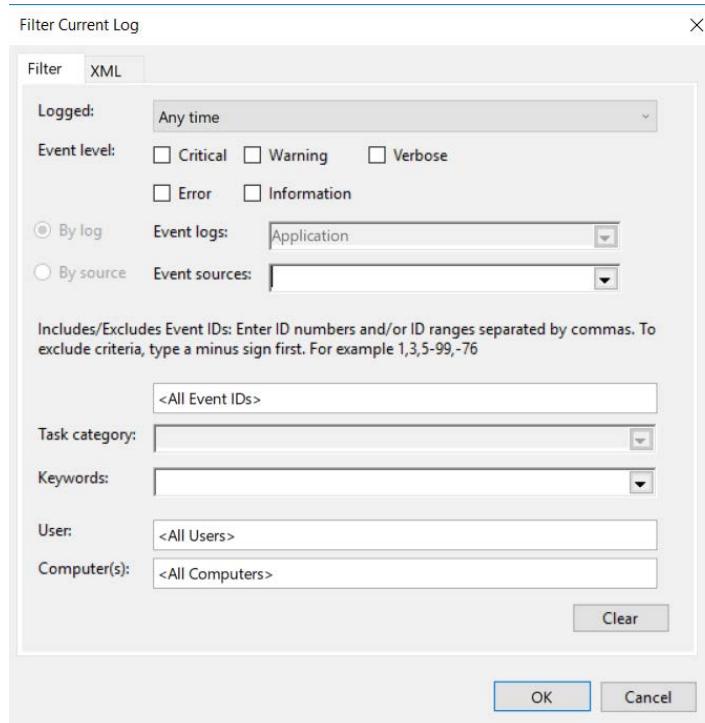
3. Open “Application Log” in the Windows Logs Folder:

A screenshot of the Windows Event Viewer application window, specifically viewing the Application Log under the Windows Logs folder. The left pane shows the log structure. The central pane displays a table of event logs with columns: Level, Date and Time, Source, Event ID, Task Ca..., and a dropdown menu. The table lists numerous "Information" level events from June 14, 2018, at various times, all originating from the "AppGu..." source. A filter bar at the top indicates "Filtered: Log: Application; Source: appguard. Number of events: 1,531".

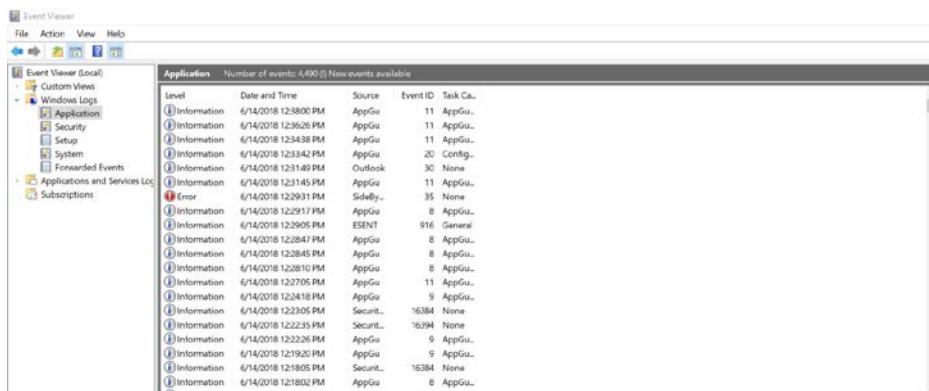
4. If there are a lot of events, right-click the **Application Log** and select “Filter Current Log” to view only the AppGuard Solo events.

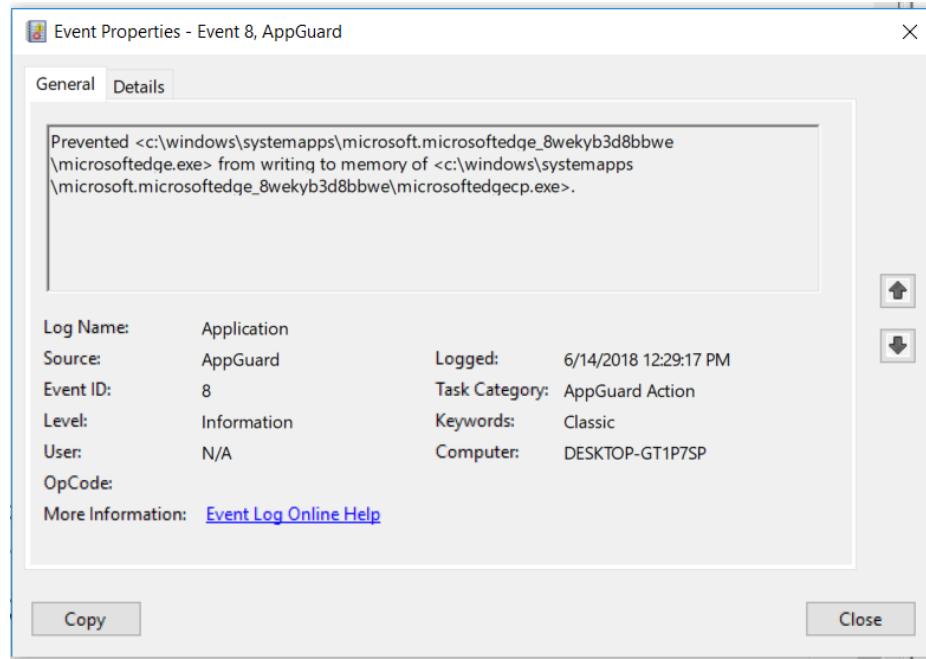


5. In the Event Sources field below, select “AppGuard” and click on OK.



6. In the filtered events, double-click an event to view more about it.





7. To get assistance with troubleshooting, right-click **Application** again and choose Save the Filtered Log File As.... Name the file and send to AppGuard Solo support – [Support@appguard.us](mailto:Support@appguard.us).

