



AppGuard™

Release Notes Version 3.2

October, 2011

Blue Ridge Networks, Inc.
14120 Parke Long Court
Chantilly, VA 20151

Contents

1.0	Introduction.....	3
2.0	AppGuard Hardware and Software Requirements	3
3.0	AppGuard Release Features.....	3
3.1	AppGuard Release 3.2 – (October 2011).....	3
3.2	AppGuard Release 3.1 – (August 2011)	3
3.3	AppGuard Release 3.1.3 – Beta (July 2011).....	4
3.4	AppGuard Release 3.0 (March 2011)	9
3.5	AppGuard Beta Release 3.0.7 (December 2010).....	11
3.6	AppGuard Beta Release 2.0.10 (September 2010).....	14
3.7	AppGuard Beta Release 2.0 (August 2010).....	16
3.8	AppGuard Beta Release 1.5 (July 2010).....	17
3.9	AppGuard Release 1.4 (March 2010)	18
3.10	AppGuard Release 1.3 (October 2009)	18
3.11	AppGuard Release 1.2 (May 2009)	20
3.12	AppGuard Release 1.1 (February 2009).....	20
3.13	AppGuard Release 1.0 (November 2008).....	21
4.0	Known Anomalies.....	23

1.0 Introduction

The release notes highlight the new features and major defect fixes in AppGuard. A more complete description of AppGuard's capabilities can be found in the AppGuard Administrative Guide.

Note: AppGuard is not compatible with Blue Ridge's EdgeGuard and USA Connect products. Uninstall these products prior to installing AppGuard.

2.0 AppGuard Hardware and Software Requirements

Software

1. Microsoft Windows XP SP2 and above (32 Bit).
2. Microsoft Windows VISTA, Service Pack 1 and above (32 Bit*).
3. Microsoft Windows 7, Service Pack 0 and above (32 and 64 Bit).

*Blue Ridge did confirm that this release will operate on 64 Bit Windows Vista. However, Blue Ridge will not guarantee future compatibility with 64 bit Windows Vista.

Hardware

1. Minimum 1.80 GHz 1.00 GB of RAM
2. 10 MB Hard Disk free space.

3.0 AppGuard Release Features

3.1 AppGuard Release 3.2 – (October 2011)

AppGuard no longer checks the digital signatures in files launched from System Space. Also, an intermittent crash that occurred when validating the license has been fixed in this release.

3.2 AppGuard Release 3.1 – (August 2011)

The following enhancements have been made in this release:

1. AppGuard now checks the signature of files launched from Network shares.
2. Protection for Virtual EdgeGuard was added to this release.

The following defects which were found during Beta testing of the 3.1.3 release were fixed in this release:

1. Performance related to signature checking was improved.
2. Default settings for the publisher list were not being defined correctly.
3. Blocked registry settings were causing the AppGuard icon to blink.

3.3 AppGuard Release 3.1.3 – Beta (July 2011)

The following sections summarize the new features incorporated in the 3.1 Beta version of AppGuard.

3.3.1 New Protection Level Definitions

AppGuard's Protection Levels have been modified as follows:

1. **Locked Down:** Only user-space programs explicitly specified in the Guard List are permitted to run. All programs in the Guard List are automatically Memory Guarded and run in Privacy Mode regardless of the settings. Only Microsoft install files are permitted.
2. **High:** User-space programs published by trusted publishers will be protected as defined in the Trusted Publishers List (see Section 3.3.2). All other digitally signed applications will be permitted to run, but they will be automatically Guarded, Memory Guarded, and executed in Privacy Mode. Rundll32.exe is removed from the Guard List and only Trusted Publisher's install files will be permitted.
3. **Medium:** All user-space programs will be permitted to execute, but will run in Privacy Mode. Applications that are digitally signed will not be Guarded or Memory Guarded. Unsigned applications will be Guarded. Rundll32.exe is removed from the Guard List and all signed installation files are permitted. User-space scripts are also permitted.
4. **Install:** All user-space programs and scripts will be permitted to execute and are not Guarded. Rundll32.exe, Regsvr32.exe, cmd.exe and all browsers are removed from the Guard List. All install files are permitted.

The Protection Levels are summarized in the table below.

	Off	Install Mode	Medium	High	Locked Down
User-Space Protection					
Application/Script Launch Policy (not in Guard List):					
• Microsoft	UnGuarded	UnGuarded	UnGuarded	Pub. List policy	Not allowed
• Pub.List	UnGuarded	UnGuarded	UnGuarded	Pub. List policy	Not allowed
• Dig. Signed	UnGuarded	UnGuarded	UnGuarded	Guarded	Not allowed
• Un-signed	UnGuarded	UnGuarded	Guarded	Not allowed	Not allowed
• Scripts	UnGuarded	UnGuarded	Not allowed	Not allowed	Not allowed
• Autorun.inf	UnGuarded	Not allowed	Not allowed	Not allowed	Not allowed
MemoryGuard	No	No	No	Yes	Yes***
Privacy Mode	No	No	Yes	Yes	Yes***
System-Space Protection					
Guard List Apps	UnGuarded	Guarded*	Guarded**	Guarded**	Guarded
MemoryGuard	No	No	No	As conf.	Yes
Privacy Mode	No	As conf.	As conf.	As conf.	Yes
Other Protections					

InstallGuard	All allowed	All allowed	Signed only	Publisher List	Microsoft only
MBRGuard	As conf.	As conf.	As conf.	As conf.	As conf.

*Browsers, cmd.exe, regsvr32.exe and rundll32.exe are removed from the Guard List.

**rundll32.exe is removed from the Guard List.

***If a user-space application is launched while in another protection level, and then the protection level is switched back to “Locked Down”, then those programs will become protected (i.e. Guarded, MemoryGuarded and execute in Privacy Mode).

3.3.2 Trusted Publishers List

Execution and Guard policies can now be specified for User-space applications based on the publisher. When AppGuard is first installed, it includes Microsoft, Adobe, Google, Mozilla and Sun Microsystems as trusted publishers, but additional publishers can be added through the AppGuard Configuration Interface.

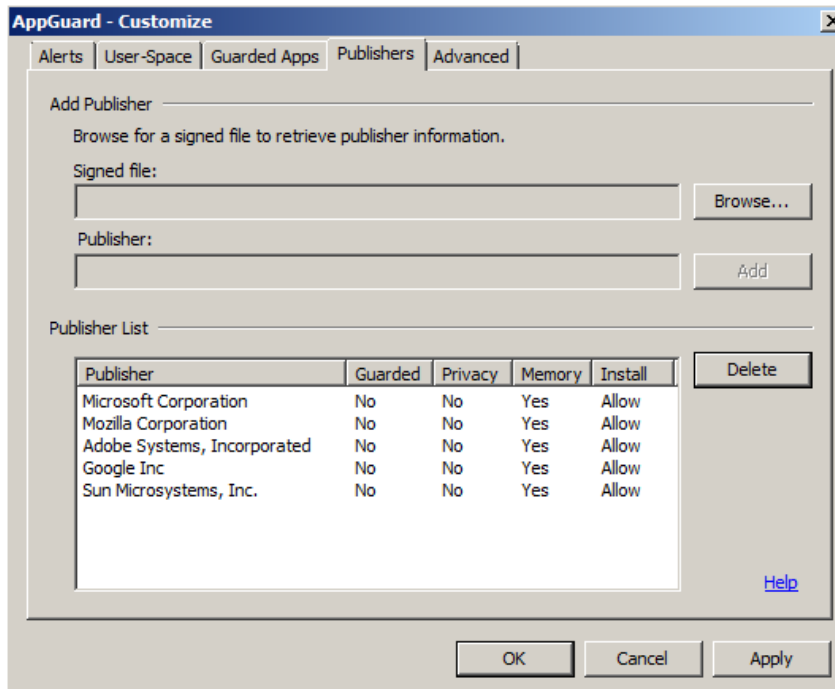
For each publisher the following can be specified:

- **Guard:** Indicates whether a user-space program published by this publisher should be Guarded 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 MemoryGuarded when it executes.
- **Install:** Indicates whether installation programs (*.msi and *.msp) published by this publisher should be permitted.

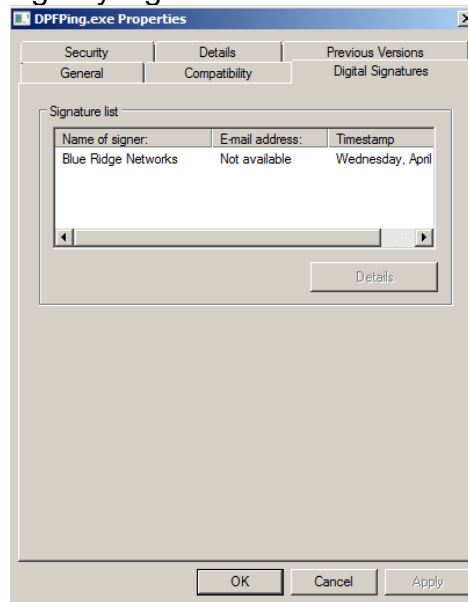
When AppGuard is first installed, the Trusted Publisher Policy is as follows:

Publisher	Guard	Privacy	Memory	Install
Microsoft	No	No	Yes	Allow
Google	No	No	Yes	Allow
Mozilla	No	No	Yes	Allow
Adobe	No	No	Yes	Allow
Sun Microsystems	No	No	Yes	Allow

To modify the Trusted Publisher Policy, click on the “Customize” button on the main AppGuard display and select the “Publishers” tab:



To add a publisher, click on the “Browse” button and navigate to a file that is digitally signed by the desired publisher. The “Digital Signatures” tab will appear in the properties of files that are digitally signed as shown below:



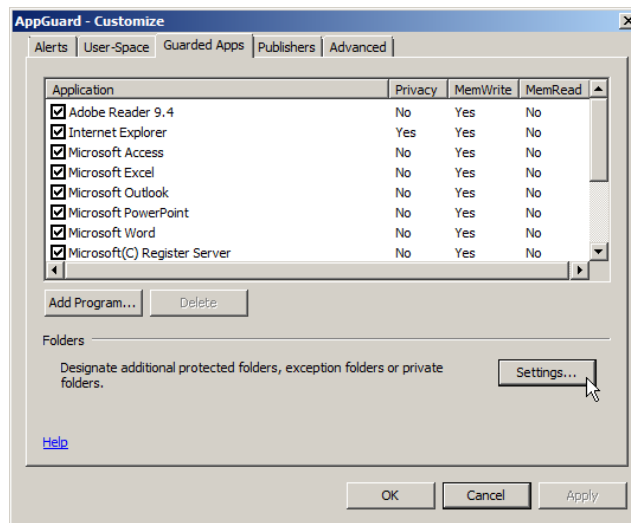
3.3.3 Adding Protected Folders

AppGuard prevents Guarded Applications from writing to a set of Protected Folders and Registry Settings. By default, AppGuard prevents applications from writing to all folders on the System Drive (usually C:\) except for the user profile directory and the program data directories:

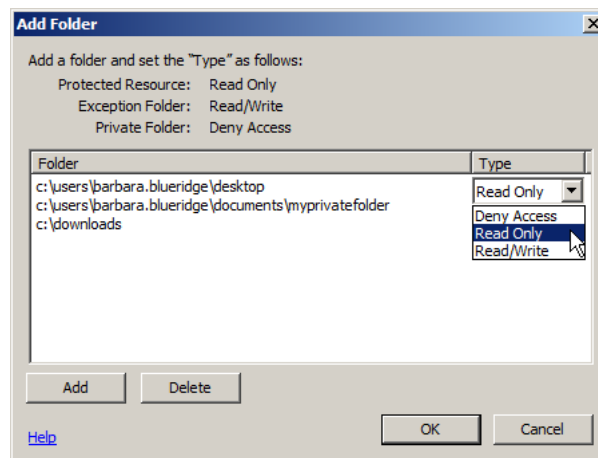
Folder	XP Folder	Win7 or VISTA Folder
User Profile	C:\Documents and Settings\John	C:\Users\John
Program Data	C:\Documents and Settings\All Users\Application Data	C:\ProgramData

Some users like to install software applications elsewhere such as a separate partition or hard drive. These locations are not regarded as system-space by default. Hence, malware or hackers could theoretically, maliciously modify these applications, transforming them into harmful tools.

So, additional directories can be added to the Protected Folder list by clicking the Folders "Settings" button on the Guarded Applications Tab:



The following dialog will be displayed from which you can add or remove Protected Folders:

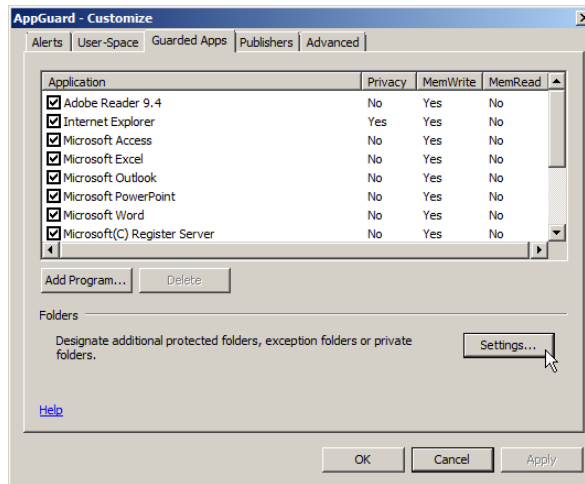


After the folder is added, change the "Type" to "Read Only."

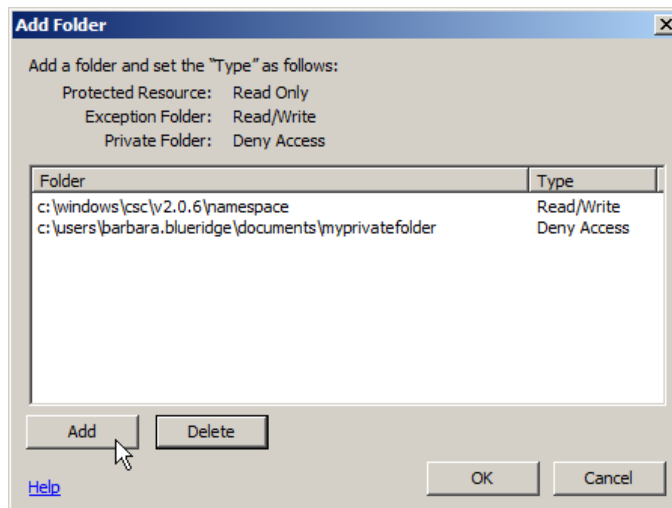
3.3.4 Exception/Private Folders Interface

The interface for adding and modifying Exception and Private Folders has changed. Exception Folders are folders that are normally within system space (such as C:\Downloads) that AppGuard prohibits Guarded Applications from writing. Private Folders are folders that AppGuard forbids any application that is running in privacy mode from accessing.

To specify Exception and Private Folders, click on the "Settings" button on the Guarded Applications Tab:



The following dialog will be displayed from which you can add or remove Exception and Private Folders, in addition to Protected Folders. To Add a folder, click on the Add Button:

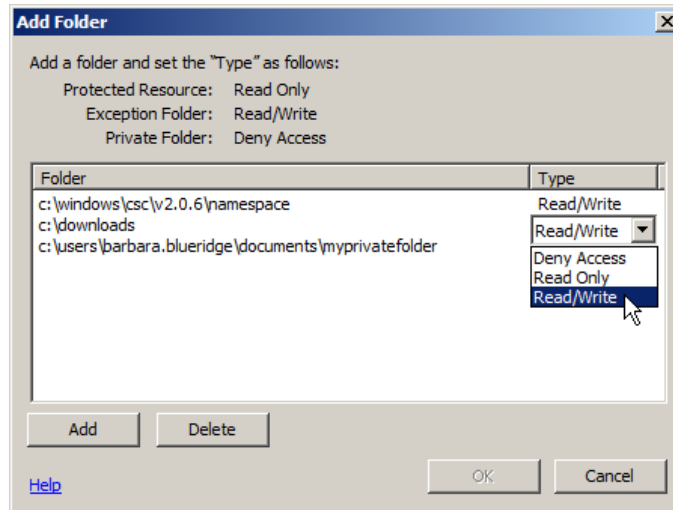


Once the folder is added change the Access "Type" field as follows:

Folder Type	Access Type
Exception Folder	Read/Write

Private Folder	Deny Access
Protected Folder	Read Only

In the following example, c:\windows\csc\v2.0.6\namespace and c:\downloads are Exception Folders, while c:\users\barbara.blueridge\documents\myprivatefolder is a Private Folder:



3.3.5 Additional Enhancements and Defect Fixes

1. An intermittent crash that occurred due to a timing issue when rebooting has been fixed in this release.
2. Self Diagnostics: The AppGuard User Interface will notify the end-user if the AppGuard service is not running.
3. Network Shares are now included in User Space.

3.4 AppGuard Release 3.0 (March 2011)

The following sections summarize the new features incorporated in the 3.0.14 version of AppGuard.

3.4.1 New Licensing Mechanism

AppGuard now uses a new licensing mechanism. Versions previously licensed under the UniLock license will need to be updated. Contact Blue Ridge Networks to request a new license key.

3.4.2 New Status Icons

AppGuard now has the following status icons:



Protection Level is set to "Install" – User-space protection is turned off.



Protection Level is set to “Off” – all AppGuard protections are turned off.

3.4.3 Defect Fixes and Minor Enhancements

The following defect fixes and minor enhancements were made in this release:

1. The registry protection problem on Vista and Windows 7 (see section **Error! Reference source not found.**) has been fixed in this release.
2. In the previous version, when switching the Protection Level to High from a lower level, any user-space application that was currently running became UnGuarded. This defect is fixed in this release.
3. In previous versions of AppGuard, Google Chrome would not launch if MemoryGuard was enabled. With this version of AppGuard, Chrome should run with MemoryGuard enabled in most cases. The exception is for Chrome that is installed in User-space (i.e. not Program Files directory) on Vista or Windows 7. In that case the following folder must be added to the User-Space exception list so that Chrome can operate with MemoryGuard enabled:
C:\Users\<UserName>\AppData\Local\Google\Chrome\Application
Refer to the Help topic, Customizing User-space Protection for more information.
4. There was a timing issue in the previous version of AppGuard so that sometimes the user interface would not display the correct protection status. This defect has been fixed in this release.
5. In the previous version of AppGuard, sometimes a message would be displayed to “Please enter an integer between 1 and 0.” This defect has been fixed in this release.
6. In the previous version, AppGuard was not saving the MemoryGuard exceptions. This defect has been fixed in this release.
7. On 64 bit systems, Microsoft Office applications were not showing up in the Guard list.

3.4.4 Special Notes

Anomalies when running in High Protection Level:

1. When running in the High Protection Level, the PC’s time zone cannot be changed. In order to change the time zone, switch the Protection Level to Medium or Low.
2. When running in the High Protection Level audio drivers cannot be viewed in the control panel on Windows 7 64 bit platforms. Although the audio drivers cannot be viewed in the control panel, they are still operational. Switch to Medium level if you need to view the audio drivers in the control panel.
3. In order to use Google Chrome in the High Protection Level on Windows 7 64 bit PCs do *either* of the following:
 - Install Google Chrome in the Program Files directory (preferred).

or

 - Exclude the following directories from the User-space protection definition:

- C:\Users\\AppData \Local\Google\Chrome\Application
- C:\Users\\AppData \Local\Google\Update

Anomalies with MemoryGuard Protection:

1. Sometimes, PowerPoint attachments cannot be opened from Outlook 2007 and 2010 when MemoryGuard is on. Instead save the file to your “My Documents” folder and open the file from that location.
2. Sometimes, when MemoryGuard is enabled, clicking on an email link from Internet Explorer or Office Applications will not result in the default mail client being launched.

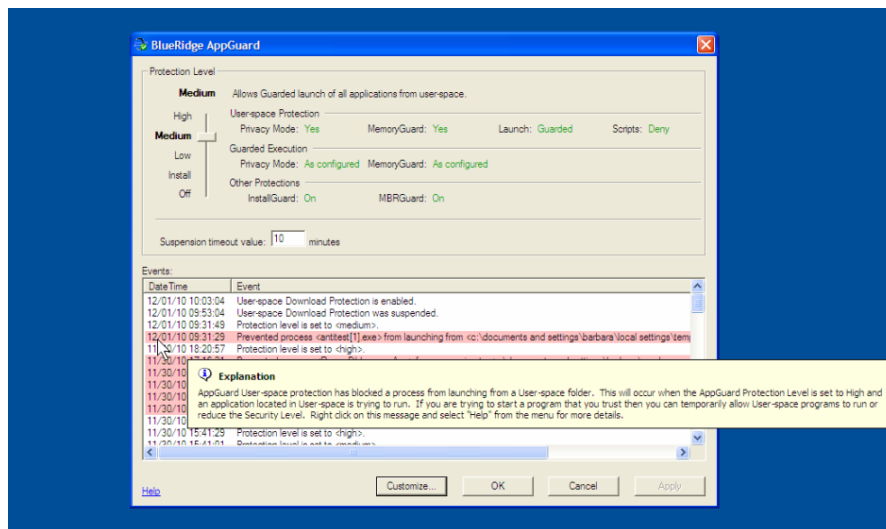
3.5 AppGuard Beta Release 3.0.7 (December 2010)

The following sections summarize the new features incorporated in the 3.0 version of AppGuard.

3.5.1 New User Interface

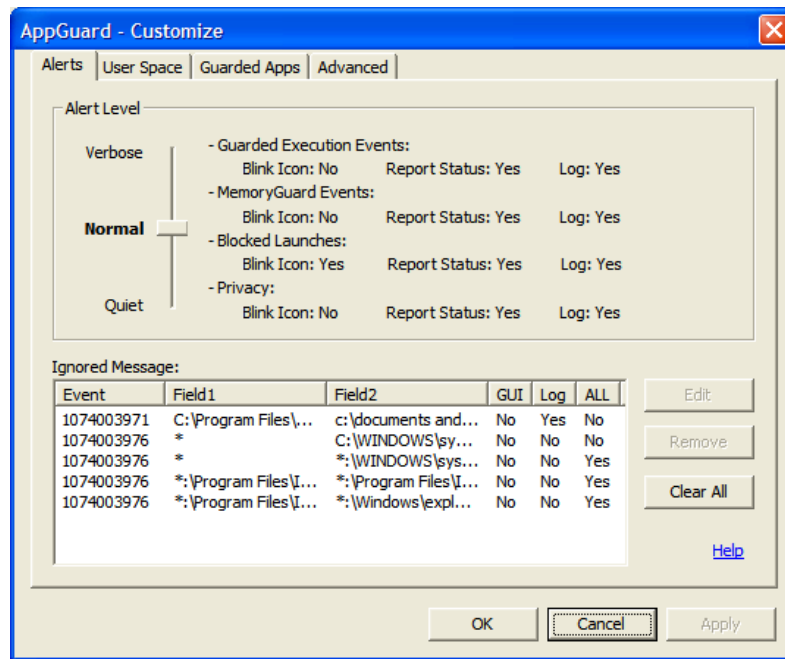
The AppGuard User Interface has changed significantly. This section will provide a brief overview of the changes; refer to the new Help file for more details.

The main interface allows the user to change the protection level (refer to Section 3.5.4) and view AppGuard events. Moving the Cursor over a particular message will provide a brief explanation of the message and further information:

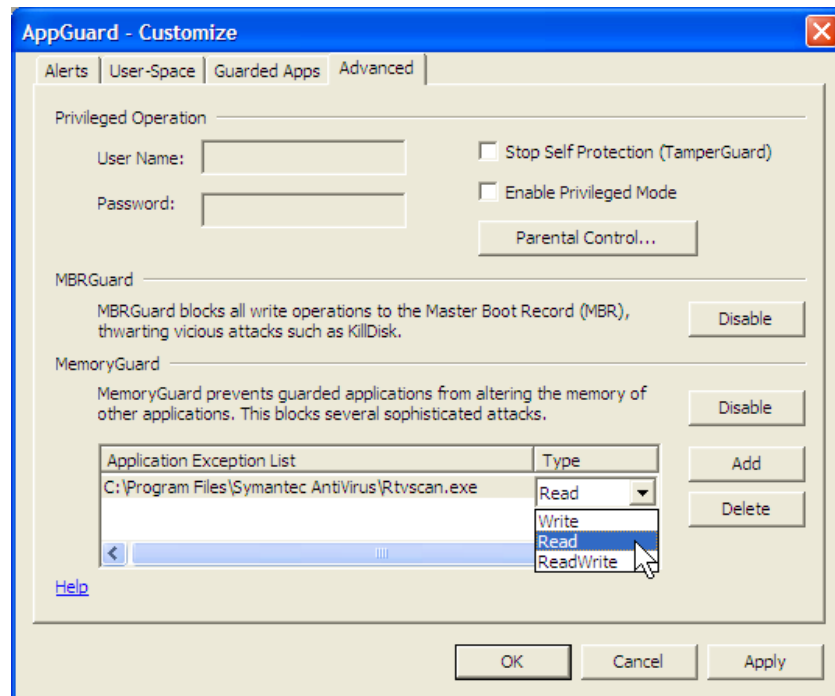


The **Customize** button will display the AppGuard Configuration Interface. The Configuration Interface has four tabs:

1. **Alerts:** This tab is used for setting the alert level (refer to Section 3.5.7) and managing the “Ignored Messages” list. Ignored Messages can now be reinstated (i.e. “Unignored”) by removing them from the Ignored Messages list.



2. **User-Space:** User-space is comprised of the folders where non-administrators can save files. By default, AppGuard considers the user's profile directory (i.e. My Documents, Desktop, etc.), USB memory devices, all non-system hard drives and network drives as User-space. The User-Space tab is used to specify additional user-space folders and exceptions.
3. **Guarded Apps:** This tab is used to add and delete applications from the Guard List. Exception Folders, Private Folders, and protection settings (MemoryGuard, Privacy Mode and Memory Read Protection) are also specified on this tab. **Caution:** With previous versions of AppGuard, unchecking an Application's checkbox resulted in a *temporary* suspension of protection. With this release, the protection will only be reinstated when the user re-checks the box.
4. **Advanced:** The Advanced Settings tab allows the user to:
 - a. Set Parental Controls.
 - b. Disable/enable MemoryGuard and Memory Read Protection.
 - c. Disable/enable MBRGuard.
 - d. Add MemoryGuard exception processes: Previous beta releases revealed that several software applications (especially Security products) require the ability to write into other processes memory. If MemoryGuard (refer to Section 3.8.3) or Memory Read Protection (refer to Section 3.5.5) interferes with a legitimate process it should be added to this list. If MemoryGuard is interfering with the process, set the "Type" column to "Write". If Memory Read Protection is interfering with the process, set it to "Read". If both protections are interfering, set it to "ReadWrite".



3.5.2 Context Sensitive Help for Blocking Events

Moving the Cursor over a particular message will provide a brief explanation of the event and further information. If more information is required, right-click on the event, and select “Help” from the drop-down menu.

3.5.3 AutoGuard

AppGuard can now be configured to allow User-space applications to launch and AppGuard will automatically Guard them so that the risk associated with potentially allowing unknown software to run is mitigated.

3.5.4 Protection Levels

With this release, there are four Protection levels:

1. High: All User-space and USB Launches are denied. All Guarded Applications are MemoryGuarded and run in Privacy Mode. InstallGuard is on. This is the Recommended and Default setting.
2. Medium: User-space and USB executables (*.exe files) are allowed to launch but they are Guarded, MemoryGuarded and run in Privacy Mode. User-space and USB scripts are denied. Guarded Applications' MemoryGuard and Privacy Mode settings are as configured. InstallGuard is on. RunDll32.exe is not Guarded at the Medium level.
3. Low: Same as medium except User-space scripts are allowed to be launched and MemoryGuard is turned off. RunDll32.exe is not Guarded at the low level.
4. Install: User-space protection, MemoryGuard and InstallGuard are all turned off. Also, the following programs are UnGuarded when the Install Protection level is invoked:
 - a. Microsoft Register Server (regsvr32.exe)

- b. Run a DLL as an App (rundll32.exe)
- c. Windows Command Processor (cmd.exe)

The Protection Level can be changed on the AppGuard User Interface.

3.5.5 Memory Read Protection

Memory Read protection prevents any malicious application from reading and copying the content of an AppGuard protected process's memory. The default AppGuard Policy does not enable Memory Read Protection for any of the Guard List applications, but setting the AppGuard protection level to High will automatically turn Memory Read Protection on for all applications in the Guard List.

3.5.6 Guarded Execution Suspension

Temporary Suspension of Guarded Execution is now done from the AppGuard Tray Menu. Protection will resume after the "Suspension timeout value" (found on the AppGuard GUI) has expired.

Caution: Unchecking the application checkbox on the Guarded Apps tab will now disable protection until the checkbox is re-checked.

3.5.7 Alert Levels

With this release, there are three alert levels:

1. Quiet: AppGuard is completely quiet. The AppGuard tray icon will not alert the end-user of any blocking actions. No events are reported to the AppGuard User Interface or to the Windows Event Log.
2. Normal: The AppGuard tray icon will only alert the end-user when an application has been blocked from launching. All other blocking events are reported to the AppGuard User Interface and Windows event log, but the AppGuard icon will not flash to alert the end-user of these actions.
3. Verbose: The AppGuard tray icon will alert the end-user of all blocking events. All events, including events that have been previously set to be ignored, are reported to the AppGuard user interface and the Windows Event Log.

3.5.8 Defect Fixes and Minor Enhancements

The following defect fixes and minor enhancements were made in this release:

8. AOL Instant Messenger has been added to the Guard List.
9. Additional Registry Keys are now Guarded.
10. On XP, a Windows user that did not have a password could not be recognized as a Super User. This defect is fixed in this release.

3.6 AppGuard Beta Release 2.0.10 (September 2010)

The following sections summarize the new features incorporated in the 2.0.10 version of AppGuard.

3.6.1 User-Space and USB Protection Levels

With this release, there are two User-Space and USB Protection levels:

1. Deny all Launches
2. Allow Guarded Launches

When set to the “Deny all Launches”, AppGuard will behave as it did in previous versions. AppGuard will prevent all scripts or executables from being executed if they are located in User-Space or on a USB memory device.

When set to “Allow Guarded Launches”, AppGuard will allow executables (*.pif, *.scf, *.exe, *.com, or *.scr.) to be launched from User-Space and USB memory devices, but they will automatically be “Guarded” by AppGuard so that they cannot write to “Protected Resources” (system directories, and critical registry keys). Also, applications launched with this protection level will also be “MemoryGuarded” and will run in Privacy mode. With this level, AppGuard will still prevent scripts (including *.cmd and *.ps1 files) from being launched.

When AppGuard is first installed, the “Allow Guarded Launches” protection level is in effect. The level can be changed on the Advanced Settings dialog.

3.6.2 MemoryGuard Operation

MemoryGuard no longer applies to all applications. The end-user can select which applications are to be MemoryGuarded on the Guard List. Also any User-space and USB applications that are launched with the protection level set to “Allow Guarded launches” will be MemoryGuarded.

When AppGuard is first installed, all applications in the default Guard List are automatically MemoryGuarded. This setting can be changed on the Guarded Applications Tab.

3.6.3 Persistent Disable

AppGuard can now be disabled completely for the current user from the Advanced Settings Dialog. AppGuard will remain disabled for that user (even after a reboot) until they re-enable it.

3.6.4 MemoryGuard Support for XP

MemoryGuard is now supported on XP Service Pack 2 and above.

3.6.5 Alerts

The “Alarm” setting on the Guarded Applications Tab has been changed to “Alert.” In previous versions of AppGuard, when “Alarm” was set to “No”, the status messages were not displayed on the Status tab and the end-user was not alerted about the block. In this version, when setting “Alert” to “No”, the status message is displayed on the Status Tab, but the end-user is not alerted with the blinking icon.

When first installed, the Alert option is set to “No” for all Guarded Applications.

Note: The end-user will still be alerted about MemoryGuard events regardless of the Alert setting.

3.6.6 Additional Applications added to Default Guard List

The following applications have been added to the Default Guard List:

1. Microsoft Register Server (regsvr32.exe)
2. Run DLL as Application (rundll32.exe)
3. Windows Command Processor (cmd.exe)

3.7 AppGuard Beta Release 2.0 (August 2010)

The following sections summarize the new features incorporated in the 2.0 version of AppGuard.

3.7.1 MBRGuard Integrated with AppGuard

MBRGuard protects the Master Boot Record from being written to. It is installed and enabled with AppGuard. MBRGuard can be disabled (and re-enabled) from the AppGuard Settings tab. A reboot is required whenever MBRGuard is disabled (or re-enabled).

3.7.2 MemoryGuard GUI Controls

MemoryGuard can be disabled or enabled from the AppGuard Settings tab. When installed, MemoryGuard is disabled by default. Note: MemoryGuard is not supported on XP platforms.

3.7.3 Parental Controls

This version of AppGuard provides a mechanism for defining parental controls. Refer to AppGuard’s Help facility for more information about this feature.

3.7.4 Super User

Super Users are not affected by Parental Controls. Refer to AppGuard’s Help facility for more information about this feature.

3.7.5 Privileged Mode

Privileged Mode must be enabled by a Super User. Once in Privileged mode, one can disable any AppGuard protection even if prohibited by Parental Controls or Default Policy. Refer to AppGuard’s Help facility for more information about this feature.

3.7.6 Ignore Messages

This release allows the end-user to specify sets of messages that can be suppressed from being reported. Refer to AppGuard’s Help facility for more information about this feature.

3.7.7 User-Space Protection

“Drive-by Download” protection is now referred to as “User-space” protection. In addition to executables (.exe files), the following types of files are not permitted to launch as part of User-space protection:

1. Visual Basic Script Files (.vbs).
2. OLE Control eXtension Files (.ocx).
3. Batch files (.bat).
4. Command Files (.cmd, .com).
5. PowerShell script files (.ps1)

3.7.8 Defect Fixes and Enhancements

The following defects and enhancements were made in this release:

11. A defect which prevented a valid license from being recognized has been fixed in this release.
12. Upon installation, "My Documents" is no longer designated as a default private folder. The default private folder is now a sub-folder of “My Documents”: "MyPrivateFolder". AppGuard will create this folder. If upgrading from a previous version, the “My Documents” folder will still remain as a Private Folder, but can be deleted from the “Guarded Applications” tab.

3.8 AppGuard Beta Release 1.5 (July 2010)

The following sections summarize the new features incorporated in the 1.5 version of AppGuard.

3.8.1 64-bit OS Support for Vista and Windows 7

AppGuard now supports Windows 7 64 bit Operating Systems. Blue Ridge did confirm that the Beta agent will operate on 64 Bit Windows Vista. However, Blue Ridge will not guarantee future compatibility with 64 bit Windows Vista.

3.8.2 InstallGuard

The primary purpose of InstallGuard is to block MSI based malware attacks:

- Prevents MSI based software installations regardless of MSI file location
- Allows Microsoft Digitally Signed MSI Installations/Patches
- User can suspend.

3.8.3 MemoryGuard

MemoryGuard is an advanced protection against sophisticated attacks whereby either a compromised legitimate process running in a process or an unauthorized process running in a PC injects code into the memory of another process, usually a legitimate one. Attackers do so to elude detection, by-pass personal firewalls restricting network access, steal information, and or many other reasons.

3.9 AppGuard Release 1.4 (March 2010)

The following sections summarize the new features incorporated in the 1.4 version of AppGuard.

3.9.1 Drive-by Download Protection for Script Files

AppGuard now prevents script files (*.bat, *.cmd, *.com) from being launched from user space.

3.9.2 Removable Media Launch Protection for Script Files

AppGuard now prevents script files (*.bat, *.cmd, *.com) from being launched from USB removable memory devices.

3.9.3 Additional Guarded Applications

The following applications are now guarded by AppGuard:

- a. Acrobat Reader (versions 7, 8 and 9).
- b. Opera
- c. Outlook Express

3.9.4 Defect Fixes

The following defects were fixed in this release:

13. When making multiple changes on the settings page that includes the suspension timeout value, all changes are now saved.
14. User space drive-by download protection is now effective after a fast user switch.
15. Suspension of Drive-by Download protection now suspends extended user-space protection (i.e. launches from non-system volumes are now allowed when drive-by download protection is suspended).
16. Intermittent problem where Exception folders were not recognized has been fixed.

3.10 AppGuard Release 1.3 (October 2009)

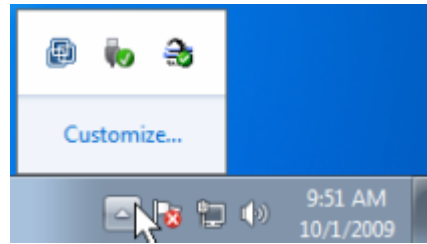
The following sections summarize the new features incorporated in the 1.3 version of AppGuard.

3.10.1 Windows 7 Support

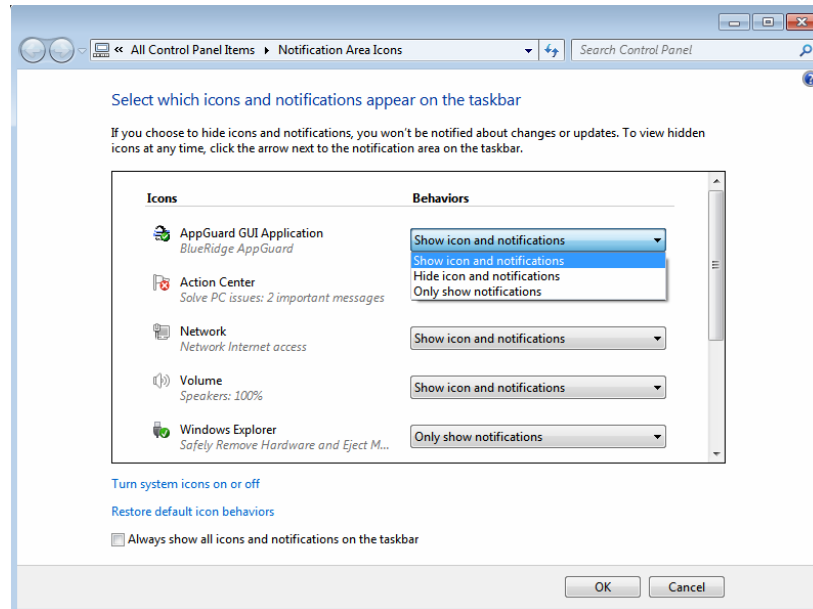
AppGuard will now install and execute on Windows 7.

Windows 7 does not display application icons in the tray or taskbar unless explicitly enabled by the end-user. To enable the AppGuard Tray Icon on Windows 7:

1. Click on the up-arrow on the left-hand side of the tray:



2. Click on "Customize"
3. The following will be displayed:



4. Locate "AppGuard GUI Application" in the icon list.
5. Select "Show icon and notifications" from the Behavior dropdown list.

3.10.2 Guarded Applications Exception Folders

The user may specify exception folders that Guarded Applications may write to. For example you may want your browser to be able to download files to c:\downloads directory. Previous versions of AppGuard did not allow this.

3.10.3 Improved User Interface

The following improvements have been made to the user interface:

1. Protection Status is now summarized on the status tab.
2. Blocking events are now highlighted in red.
3. The definition of Private Folders has been moved to the Guarded Applications tab.
4. A single timeout value now controls the time period for all protection suspensions.

3.11 AppGuard Release 1.2 (May 2009)

The following sections summarize the new features incorporated in the 1.2 version of AppGuard.

3.11.1 Privacy Mode

AppGuard enables the user to specify a set of Private Folders that are not accessible to Guarded Applications running in Privacy Mode. AppGuard is initially installed with browser Applications (Internet Explorer, FireFox and Google Chrome) set to run in Privacy Mode and the My Documents folder is specified as a Private Folder (in other words browser applications are not permitted to read or write to the My Documents folder).

3.11.2 Drive-by Download Protection Extensions

AppGuard protects a PC from drive-by downloads by suppressing the launch of executables from user-space (e.g., My Documents, Desktop, etc.) and non-system volumes such as extra internal or external hard drives (D:\, E:\ etc.). You can modify the protected areas by clicking on the Drive-by Download Protection Extension Settings button on the AppGuard Settings tab.

3.11.3 Improved End-User Experience

The following enhancements were made to improve the AppGuard end-user experience:

1. Previous versions of AppGuard required the user to navigate to an application's executable in order to add it to the Guard List. Now AppGuard enumerates the applications installed on the PC and the user can select from the list of applications. If the application has not been installed using Microsoft's best practices it may not show up in the application list. In that case, the user can still add the executable directly.
2. Links to the AppGuard Help file were added to the GUI.
3. Links to an AppGuard Tutorial were added to the Help file.

3.11.4 Defect Fixes

The following bugs have been fixed in this release:

1. On VISTA the tray icon will now blink to indicate a change in status.
2. The Enable All menu option now re-enables all protections.
3. When Autoplay is enabled for USB devices, version 1.1 of AppGuard reported blocks to autorun.inf files on USB storage devices even though an autorun.inf file was not present on the device. AppGuard no longer reports these blocks to the end-user.
4. Some false status indications related to temporary protection suspensions were corrected.

3.12 AppGuard Release 1.1 (February 2009)

The following sections summarize the new features incorporated in the 1.1 version of the AppGuard.

3.12.1 License Enforcement

License Enforcement has been added to AppGuard. When installed, AppGuard will support a 30 day trial. Full functionality is supported during the trial period. Whenever AppGuard is started, it will request an activation code until it has been fully activated. To activate AppGuard beyond the 30 day trial period an activation code must be obtained (either from Blue Ridge or from the Web Sales Portal). The activation code can be entered via the GUI or from a file (AppGuardLicense.txt) placed in the All User's profile directory. The end-user must have administrative privileges in order to activate the license.

Once the activation code is provided, AppGuard must connect to a license server at least once to register the product and verify the activation code. Depending on the license type setup, AppGuard may have to connect periodically to the license server.

A single activation code can be used to activate multiple seats for an enterprise deployment.

The uninstall program deactivates the license on the server and locally. If the uninstall program cannot reach the license server, it does not abort the uninstallation. If the user reinstalls AppGuard he will need to reenter the activation key. Boundary cases will be handled by Customer Support.

3.12.2 Improved AppGuard Notifications

AppGuard now notifies the end-user when it blocks guarded applications from writing to system directories.

3.12.3 Improved End-User Experience

The following enhancements were made to improve the AppGuard end-user experience:

1. Allows the end-user to suppress GUI notifications of write blocks for a specific application. The events are still logged to the Windows Event Log.
2. The default time that a protection can be suspended has been increased to 10 minutes.
3. The end-user can now suspend protections for a maximum of 1 hour.
4. A menu item has been added so that the end-user can suspend all AppGuard protections with one selection.
5. If an application specified in the default policy is not located on the PC, it will not appear in the Guard List GUI.
6. Events can now be copied (or saved) from the AppGuard Status GUI.

3.12.4 Enhanced USB Malware Protection

The Malware Protection has been enhanced to block access to autorun.inf files.

3.13 AppGuard Release 1.0 (November 2008)

The following sections summarize features implemented in release 1.0 of the AppGuard Agent.

3.13.1 AppGuard Basic Functionality

AppGuard provides three types of protection against Malware:

1. Guards applications from accessing critical OS components: When added to the AppGuard Guard list, an application is blocked from writing to system directories and critical registry keys.
2. Prevents executables from being launched from USB removable media.
3. Drive-by Download Protection: Prevents executables from being launched from user's profile space.

3.13.2 AppGuard Policy

AppGuard's configuration is driven by an XML policy located in the All User's profile directory. This policy is used to configure the following:

1. List of Protected Applications.
2. User is Allowed to Disable Application Protection (Y/N - default is Y).
3. Length of time that the protection will be disabled (default is 10 minutes).
4. Prevent User Space Launches (Y/N - default is Y).
5. User is Allowed to Enable/Disable User-Space Protection (Y/N - default is Y).
6. Prevent USB executable Launches (Y/N -default is Y).
7. User is Allowed to Enable/Disable USB Protection (Y/N -default is Y).

3.13.3 AppGuard Events

All AppGuard events are reported to the Windows Event Log. In addition when AppGuard prevents an application from being launched (either from a USB memory device or from the user's profile directory), the end-user is notified via the AppGuard GUI. The tray icon will blink and an event will be logged to the status tab of the AppGuard GUI.

3.13.4 Drive-by Download White List

If an application located in the user's profile directory is added to the Guard List, then AppGuard will allow it to be launched but in a Guarded mode (i.e. it will not be able to alter critical OS components).

3.13.5 AppGuard Help

AppGuard has a help feature.

3.13.6 AppGuard Install Package

AppGuard is installed using a setup.exe file. The setup program supports a silent install for use with common software distribution systems such as SMS.

3.13.7 AppGuard Self-Protection

The AppGuard application protects itself. The service cannot be stopped, the AppGuard Program Files directory cannot be tampered with and the AppGuard registry key cannot be accessed.

4.0 Known Anomalies

Anomalies when running with UAC enabled:

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

Anomalies when running in High Protection Level:

1. When running in the High Protection Level, the PC's time zone cannot be changed. In order to change the time zone, switch the Protection Level to Medium or Low.
2. When running in the High Protection Level audio drivers cannot be viewed in the control panel on Windows 7 64 bit platforms. Although the audio drivers cannot be viewed in the control panel, they are still operational. Switch to Medium level if you need to view the audio drivers in the control panel.
3. In order to use Google Chrome in the High Protection Level on Windows 7 64 bit PCs do *either* of the following:
 - Install Google Chrome in the Program Files directory (preferred).

or

 - Exclude the following directories from the User-space protection definition:
 - C:\Users\ \Local\Google\Chrome\Application
 - C:\Users\

Anomalies with MemoryGuard Protection:

1. Sometimes, PowerPoint attachments cannot be opened from Outlook 2007 and 2010 when MemoryGuard is on. Instead save the file to your "My Documents" folder and open the file from that location.
2. Sometimes, when MemoryGuard is enabled, clicking on an email link from Internet Explorer or Office Applications will not result in the default mail client being launched.

Anomalies with Changing Protection Levels:

1. When switching the Protection Level to High from a lower level, any user-space application that is currently running will become UnGuarded.