



AppGuard™

Release Notes Version 1.4

March, 2010

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

1.0 Introduction

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

2.0 AppGuard Hardware and Software Requirements

Software

1. Microsoft Windows XP Service Pack 2 and above.
2. Microsoft Windows VISTA, Service Pack 0 and above.
3. Microsoft Windows 7, Service Pack 0 and above.

Hardware

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

3.0 AppGuard Release Features

3.1 AppGuard Release 1.4 (March 2010)

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

3.1.1 Drive-by Download Protection for Script Files

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

3.1.2 Removable Media Launch Protection for Script Files

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

3.1.3 Additional Guarded Applications

The following applications are now guarded by AppGuard:

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

3.1.4 Defect Fixes

The following defects were fixed in this release:

1. When making multiple changes on the settings page that includes the suspension timeout value, all changes are now saved.

2. User space drive-by download protection is now effective after a fast user switch.
3. 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).
4. Intermittent problem where Exception folders were not recognized has been fixed.

3.2 AppGuard Release 1.3 (October 2009)

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

3.2.1 Windows 7 Support

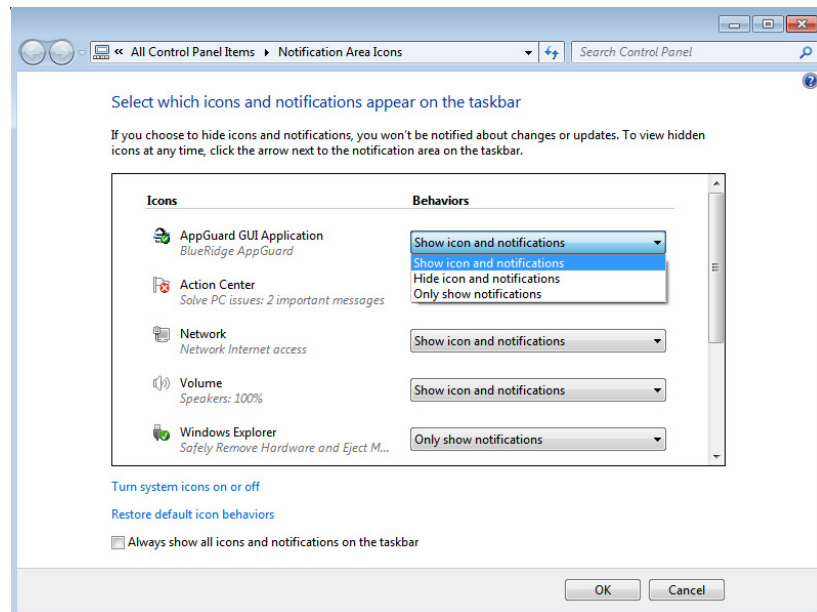
AppGuard will now install and execute on Windows 7.

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.

3.2.2 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.

3.2.3 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.

3.3 AppGuard Release 1.2 (May 2009)

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

3.3.1 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).

3.3.2 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.

3.3.3 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.

3.3.4 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.

3.4 AppGuard Release 1.1 (February 2009)

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

3.4.1 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.

3.4.2 Improved AppGuard Notifications

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

3.4.3 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.

3.4.4 Enhanced USB Malware Protection

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

3.5 AppGuard Release 1.0 (November 2008)

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

3.5.1 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.

3.5.2 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).

3.5.3 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.

3.5.4 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).

3.5.5 AppGuard Help

AppGuard has a help feature.

3.5.6 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.

3.5.7 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

4.1 Release 1.4

None.

4.2 Release 1.3

1. When changing the suspension timeout value on the settings tab any other changes that are also made will not be saved.
2. User Space Drive-by Download protection was ineffective after fast user switch occurred. This defect did not effect extended drive-by download protection.
3. Suspension of Drive-by Download protection does not suspend extended user-space protection (i.e. launches from non-system volumes are still prohibited when drive-by download protection is suspended).
4. There is an intermittent problem where “Exception” folders are not recognized. An Exception folder is a folder designated such that guarded applications are allowed to access this folder. In some cases AppGuard prevents a guarded application from accessing these folders. A work-around is to temporarily suspend protection for the application that is accessing the Exception folder.

4.3 Release 1.2

1. To activate the license the user must have administrative privileges.
2. When adding a private folder or more drive-by-download folders, you must browse to the folder. You cannot simply type in the path.
3. Terminal Services must be running.

4.4 Release 1.1

1. To activate the license the user must have administrative privileges.
2. On VISTA the tray icon will not blink to alert the user of a change in status (the icon will change states, but it will not blink).
3. The ‘Enable All’ menu option only enables USB Protection and Drive-by Download Protection. It does not enable the protection for the Guarded Applications. Protection of the guarded applications will resume after the timeout period.

4.5 Release 1.0

1. None.

