CENTRE FOR DEVELOPEMNT OF ADVANCED COMPUTING

AppSamvid

User Manual

CDAC Hyderabad

Version: 2.0.1

Contents

Prerequisites

AppSamvid software require the computer user to have significant knowledge on using the Microsoft Windows operating system as well as how security software's (such as antivirus) work. The user should have clear understanding of whitelisting and the consequences of whitelisting on the operating system. The user is informed that once whitelisting is enforced, any file which is not whitelisted will be denied execution. This affects the updating, installation and un-installation of software on the operating system and the user has to go through the defined procedures defined within AppSamvid software for doing these works after installation of this software.

1. Introduction

a. What is application/file(s) whitelisting?

It's the process of deciding on set/list of executable files as allowed (i.e. whitelisted) for execution and then allow only those files to execute on a system. Any file that is not in the allowed set/list will be treated as blacklisted and denied execution.

This way only pre-decided set/list application programs will be able to execute/run on the users operating system.

b. What AppSamvid do?

AppSamvid is application/file whitelisting software. It has ability to whitelist executables (i.e. files with .exe extension) and java files (i.e. files with .class, .war and .jar extensions).

c. How does it work?

AppSamvid software allows application/file whitelisting on Microsoft Windows based PCs. It has scans the complete hard-disk for executables, java files and stores them in the database along with some additional information about each file. Once the software is installed and initial scan of applications is done, user can whitelist any executable files using file and/or folder scan.

d. Main features:

Application Whitelisting: Whitelist windows executable files and java files. AppSamvid allows only the whitelisted files to execute on system. Whitelisting the applications this way has the ability to protect the system from malware (virus, Trojans etc.). In addition to this it *may* protect the system from zero day malware.

Whitelist Management: Graphical Interface to manage whitelisted files. This allows the user to manage whitelist from user interface for easy administration of whitelist.

Scan System: Scanning includes all the executables and java files present on the system's hard-disk. System scanning can be done at any point of time after the software installation and initial scan, depending upon the user requirement.

Enable Whitelist Enforcement: Whitelist is enforced and all the non-whitelisted applications are denied execution.

Installation Mode: Whitelisting of file(s) makes the system static in nature. This means that any new file on the system is regarded as blacklisted by default. When user installs software on a system, many new files are installed or copied to the system. Whitelisting will not allow these new files to be executed which may result in incomplete or corrupted software installation. To install new software, update installed software and un-install installed software, Administrator needs to put the system in Installation mode.

Trusted Updaters: AppSamvid allows automatic application updates by trusted updaters, even if whitelist enforcement is enabled. Any updates by these trusted updaters will be added to the database as *allow* and thus whitelisted.

Java Files Whitelisting: Java files whitelisting is enforced based on the JRE (Java Runtime Environment), JDK (Java Development Kit) versions used by java applications in the system. In order to enforce the java files whitelisting, user need to configure the JRE/JDK versions with AppSamvid.

Note: This software does NOT support java files whitelisting on windows XP/server 2003 systems.

2. User-Interface

I. AppSamvid user interface

AppSamvid user interface has the following major components:

a.Home Menu

Under Home menu, the description of applications and current status of software is displayed.

I. Scan options

1. **Initial Scan:** This option is active, only if initial scan is not performed during the installation. Once initial scan is completed, this option will remain disabled.
2. **Folder Scan:** Allows scanning a folder or a drive to add to database.
3. **File scan:** Adds a single file to the database.
4. **Add as:** This option allows adding the applications to the database as Allow (i.e. whitelisted) or Block (i.e. non-whitelisted/blacklisted).

II. AppSamvid features

1. **Enable Whitelist Enforcement:** Enables the AppSamvid's application whitelisting enforcement.
2. **Suspend Whitelist Enforcement till next reboot:** Disables AppSamvid's application whitelist enforcement until system reboots. After system reboot, whitelist enforcement starts automatically.
3. **Disable Whitelist Enforcement:** Disables AppSamvid's application whitelist enforcement permanently. Whitelist enforcement will remain in disabled state even after system reboot.

4. **Switch to Installation Mode:** Enables the Installation mode. In this mode, whitelist enforcement will be disabled automatically.
5. **Disable Installation Mode:** Disables the Installation mode and switches back the Appsamvid software state to "**Suspend Whitelist Enforcement till next reboot**". User can enable the whitelist enforcement manually if he wants.

b. Edit Whitelist Menu

Users can allow/block/remove the application from whitelist using this menu.

a. **Search:** Enables searching for file in the database, based on integrity hash or name etc.
b. **System Drive Applications:** This option lists all the scanned executable files on the system-drive i.e. the drive on which windows operating system is installed.

Note:

- During "Initial scan" only windows system drive is scanned for executable files.
- System protected applications cannot be deleted from the scanned files list/database. Protected applications are critical Windows system files and protected by WFP (Windows File Protection) feature of windows operating system.

c. **Remaining Applications:** Executable files that are on the hard-disk other than system drive (this is the drive on which Windows operating system is installed) are shown with this option.

c. Settings Menu

a. **Java Settings:** This option allows configuring and viewing JDK and JRE installed on the system. This option is for use when user wants to whitelist java files.
b. **Change AppSamvid Administrator Password:** This option allows changing the AppSamvid software's administrator password.
c. **Check for updaters:** This option allows user to evaluate/calculate for the potential updater application(s) of third-party software. This is done by analysing the logs generated by AppSamvid software. This helps the user to easily identify executable file(s) that can be marked as trusted updater(s).

d. Logs Menu

Logs menu displays logs which are generated by AppSamvid software. Logs will have the action column as:

a. Block_Unknown i.e. for application file which is NOT found in AppSamvid database,
b. Block_known i.e. for application file which is found in Appsamvid database and explicitly blocked by the user.
c. Allow i.e. for application file which is found in Appsamvid database allowed by the user.

II. AppSamvid user interface password dialog box

To access AppSamvid user interface, password is required. This is the AppSamvid software Administrator user password that was given during the installation of the software or set using the change administrator password option of AppSamvid user interface. This password needs to

be entered using AppSamvid user console password dialog box which pops-up when user tries to get access to AppSamvid user interface.

3. Scanning System

Under Home menu, scan system option allows scanning the system for the executable and java files. Scan option allows user to perform 'Initial Scan', 'Folder Scan' and 'File Scan'. User has to select the ***Add as Allow or Block*** during the scanning. Once the folder/file is selected and Add as Allow or Block option is decided, select the ***Start*** button to start the scanning. The software will notify the user once scan completes by giving the notification in taskbar.

4. Managing the executable files whitelist

Select the applications in the list box under the edit whitelist menu and allow or deny the applications using ***Allow*** and ***Block*** buttons under edit option.

5. Manage trusted updaters.

Select the application in the list box under the edit whitelist tab and make it as a trusted updater using ***make updater*** button under edit option.

To distrust an application select the application in the list box under the edit mode tab and remove it as a trusted updater using ***Un-make updater*** button under edit option.

6. Enable and Disable Whitelist Enforcement

To enable AppSamvid's whitelist enforcement, go to Home menu and under the AppSamvid features option, select the ***Enable Whitelist Enforcement*** option and click on ***Apply***.

To disable AppSamvid's whitelist enforcement, go to Home menu and under the AppSamvid features, select to ***Disable Whitelist Enforcement*** or ***Suspend Whitelist Enforcement till next reboot*** button and click on ***Apply***.

7. Executable file Analysis

AppSamvid software comes with a 'heuristic binary analysis engine' which allow user to analyse a selected file and get an information upon which user can build the consensus if the file is malicious in nature or a benign file. The output of analysis is a numeric score starting with 0. The low score value indicates that it's potentially a clean file and can be whitelisted. The high score indicates that file can be potentially malicious and needs cross-examination before whitelisting. Please note that high score for a file not always indicates that it's a malicious file. There are examples of clean files that are compressed to decrease their size and for them analysis can give a high score.

8. Configure Java Settings

To whitelist Java files (i.e. .class, .war and .jar) information on installed JDK and JRE is required. To get this information 'Configure Java Settings' option is required.

To configure java settings, go to ***Settings Tab*** and select ***Auto-Detect Java Settings*** under Java Settings. This will detect the current version of *JDK* and *JRE*.

9. Installation Mode

The purpose of Installation Mode is to allow for proper installation of new software's and/or un-installation of installed software's. Once Installation mode enabled, the whitelist enforcement will be disabled.

To put the AppSamvid in Installation mode select the ***Switch to Installation mode*** under the AppSamvid features and click on ***Apply***.

Note: 'Windows Updates' can be automatically installed without enabling the installation mode.

10. Change AppSamvid Password

To change AppSamvid software's administrator user password, go to ***Settings tab*** and change the password by giving the old password and new password and selecting ***Confirm***.

11. Context Menu Option

This option allows user to enable or disable context menu option of "***Add to Whitelist*"** on right click event on executable icon.

When the context menu is enabled, user can select an application from system, right click and choose "**Add to Whitelist**" option to add that particular application into whitelist database. When context menu is disabled there will be no option shown during right click on an application icon.

12. Check for Potential Updaters

Analyse the information collected during file(s) execution and list file(s) that are potential updaters. Administrator user can consider the listed files for adding as trusted updaters, so to enable automatic updating of third party applications.

13. Important Notes

I. Application Updates

All the applications will be allowed to install updates only when *Installation* mode is turned **ON**.

When the whitelist is enforced on the system by switching the AppSamvid into 'Enable Whitelist Enforcement' mode, any attempt to update software by downloading and executing new (non-whitelisted) executable file(s) will fail. Sometimes it may appear that software updating process has initiated but it is highly likely that it will NOT be able to complete (except in the cases where no new executable file is downloaded during updating process).

Note: Sometimes an attempt to update a software during 'Whitelist Enforcement' ON mode but will render the software (that tries to update) unusable. In the worst case scenario (though this is highly unlikely) the operating system freezes.

II. Windows Updates

AppSamvid software has support for automatic installation of Microsoft Windows Updates that install through Microsoft Windows Update application in the Control Panel. For this some files are made as Trusted Updater(s) by default. Make sure that these files always remain as Trusted Updaters.

In some cases when Windows Updates are installed at the boot time or system shutdown/restart time and when AppSamvid's whitelist enforcement is ON, Windows may attempt to install updates but will fail.

In some cases the Windows Update service may try to install these updates every time the system boots up. In these cases the Administrator is recommended to boot in Safe Mode and switch to installation mode ON, or disable AppSamvid's whitelist enforcement to make the system boot normally and **free it from continuous loop of trying to install Windows Updates** at system boot up time.

III. Whitelisting Applications

AppSamvid is application whitelisting software and if the important operating system files are not whitelisted by the AppSamvid software Administrator, the Windows Operating system itself may not boot properly or in other words the non-whitelisted important operating system applications may not be able to execute properly. Moreover it is recommended to whitelist most of the files in the system drive (i.e. the drive on which windows is installed) until or unless user is completely aware of what he is blocking from execution.

In the case when programs may be installed on the drive other than the system drive (usually in cases when space in system drive is less), the AppSamvid software administrator has to take care of explicitly scanning and whitelisting applications on the other drives.

Caution

The AppSamvid software may break/freeze/crash Microsoft Windows Operating system and/or your application programs installed on the system. C-DAC Hyderabad is not responsible for any damage of such kind to the system. Use this software at your own risk. Please read all the documentation carefully before using the software and make sure that you understand what you are doing. It is recommended to first try this software on a non-production/spare system before deploying on a production system.