AppSamvid

User Manual

Centre for Development of Advanced Computing (C-DAC) – Hyderabad

Version 2.1

DISCLAIMER: The APPSAMVID SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you. In no event shall CENTER FOR DEVELOPMENT OF ADVANCED COMPUTING, Hyderabad be liable for any special, consequential, incidental or indirect damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information and loss of time) arising out of the use of or inability to use this product, even if CENTER FOR DEVELOPMENT OF ADVANCED COMPUTING, Hyderabad is aware of the possibility of such damages and known defects.

C-DAC Hyderabad

Contents

Caution 4
1. Introduction 4
1. What is application/file(s) whitelisting? 4
2. What AppSamvid do? 4
3. How does it work? 4
4. Main features: 4
Application Whitelisting: 4
Whitelist Management: 4
Scan System: 4
Enable Whitelist Enforcement: 5
Installation Mode: 5
Trusted Updaters: 5
Java Files Whitelisting: 5
2. User-Interface 5
I. AppSamvid user interface 5
I. Home Menu 5
II. Edit Whitelist Menu 6
III. Settings Menu 6
IV. Logs Menu 7
II. AppSamvid user interface password dialogue box 7
3. Scanning System 7
4. Managing the executable files whitelist 7
5. Manage trusted updaters. 8
6. Enable and Disable Whitelist Enforcement 8
7. Executable File Analysis 8
8. Configure Java Settings 8
9. Installation Mode 8
10. Change AppSamvid Password 9

©2024, Centre for Development for Advanced Computing – Hyderabad

C-DAC Hyderabad

10. Context Menu Option 9
11. Check for Potential Updaters 9
12. Important Notes 9
a. Application Updates 9
b. Windows Updates 10
c. Whitelisting Applications 10

C-DAC Hyderabad

©2024, Centre for Development for Advanced Computing – Hyderabad

Caution

The AppSamvid software may break/freeze/crash the Microsoft Windows Operating system and 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 it on a production system.

1. Introduction

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

It's the process of deciding on a set/list of executable files as allowed (i.e. whitelisted) for execution and then allowing 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 user's operating system.

2. What AppSamvid do?

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

3. How does it work?

AppSamvid software allows application/file whitelisting on Microsoft Windows-based PCs. It scans the complete hard disk for executables, and Java files and stores them in the database along with some additional information about each file. Once this software is installed and the initial scan of applications is done it presents the user with the option to whitelist executable files and enforce the user-decided whitelist on the system.

4. Main features:

Application Whitelisting: Whitelist Windows executable files and Java files. AppSamvid allows only the whitelisted files to execute on the system. Whitelisting the applications this way can protect the system from malware (Viruses, 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 the whitelist from the 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 in time after the software installation and initial scan, depending upon the user's requirement.

©2024, Centre for Development for Advanced Computing – Hyderabad

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

Installation Mode: Whitelisting of the file(s) makes the system static (i.e. no new changes to the system are allowed by installing new applications etc.). This means that any new file on the system is regarded as blacklisted by default. When the 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, the 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 file whitelisting is enforced based on the JRE (Java Runtime Environment), and JDK (Java Development Kit) versions used by Java applications in the system. To enforce the Java files whitelisting, the user needs 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:

I. Home Menu

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

1. Scan options

a. **Initial Scan:** This option is active, only if the initial scan is not performed during the installation. Once the initial scan is completed, this option will remain disabled.

b. **Folder Scan:** Allows scanning a folder or a drive to be added to the database.

c. **File scan:** Adds a single file to the database.

d. **Add as:** This option allows adding the applications to the database as Allow (i.e. whitelisted) or Block (i.e. non-whitelisted/blacklisted).

2. AppSamvid features

a. **Enable Whitelist Enforcement:** Enables the AppSamvid application whitelisting enforcement.

©2024, Centre for Development for Advanced Computing – Hyderabad

b. **Suspend Whitelist Enforcement till next reboot:** Disables AppSamvid application whitelist enforcement until the system reboots. After the system reboots, whitelist enforcement starts automatically.

c. **Disable Whitelist Enforcement:** Disable AppSamvid application whitelist enforcement permanently. Whitelist enforcement will remain disabled even after the system reboots.

d. **Switch to Installation Mode:** Enables the Installation mode. In this mode, whitelist enforcement will be disabled automatically.

e. **Disable Installation Mode:** Disables the Installation mode and switches back the AppSamvid software state to "**Suspend Whitelist Enforcement till next reboot**". Users can enable the whitelist enforcement manually if they want.

II. Edit Whitelist Menu

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

a. **Search:** Enables searching for files 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:

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

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

III. Settings Menu

a. **Java Settings:** This option allows configuring and viewing JDK and JRE installed on the system. This option is for use when the user wants to whitelist java files.

Note: This setting is not allowed in XP /server 2003.

b. **Change AppSamvid Administrator Password:** This option allows changing the AppSamvid software's administrator password. Please note that once this password is changed, the AppSamvid software uninstallation password will also change to this new password.

c. **Check for updaters:** This option allows the user to evaluate/calculate the potential updater application(s) of third-party software. This is done by analysing the logs

©2024, Centre for Development for Advanced Computing – Hyderabad

generated by AppSamvid software. This helps the user to easily identify executable file(s) that can be marked as trusted updater(s).

IV. Logs Menu

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

I. Block_Unknown i.e. for application file which is NOT found in the AppSamvid database,
II. Block_known i.e. for application file found in AppSamvid database and explicitly blocked by the user.
III. Allow i.e. for application files found in the AppSamvid database allowed by the user.

Note: Some logs may be missed in the case of Windows XP/Server 2003 systems.

II. AppSamvid user interface password dialogue box

To access the AppSamvid user interface, a 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 the AppSamvid user interface. This password needs to be entered using the AppSamvid user console password dialogue box which pops up when a user tries to get access to the AppSamvid user interface.

3. Scanning System

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

Note: In the case of Windows XP and Windows Server 2003 systems whenever the user modifies the status of any application that would come into effect after the system restarts or 'whitelist enforcement' restarts.

©2024, Centre for Development for Advanced Computing – Hyderabad

5. Manage trusted updaters.

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

6. Enable and Disable Whitelist Enforcement

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

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

7. Executable File Analysis

AppSamvid software comes with a 'heuristic binary analysis engine' which allows users to analyse a selected file and get information upon which users can build the consensus if the file is malicious in nature or a benign file. The output of the 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 the file can be potentially malicious and needs cross-examination before whitelisting. Please note that a high score for a file does not always indicate 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 the ***Settings Tab*** and select ***Auto-Detect Java Settings*** under Java Settings. This will detect the current version of *JDK* and *JRE*.

Note: This setting is not available in Windows XP and Windows Server 2003 Operating Systems.

9. Installation Mode

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

©2024, Centre for Development for Advanced Computing – Hyderabad

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 the ***Settings tab*** and change the password by giving the old password and new password and selecting ***Confirm***. Please note that once the AppSamvid software's Administrator user password is changed, the uninstallation password will also change to the new password.

10. Context Menu Option

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

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

11. Check for Potential Updaters

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

Note: This option is not available in Windows XP and Windows Server 2003 Operating Systems.

12. Important Notes

a. 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 the software by downloading and executing new (non-whitelisted) executable file(s) will fail. Sometimes it may appear that

©2024, Centre for Development for Advanced Computing – Hyderabad

the software updating process has been initiated but, likely, it will NOT be able to complete (except in the cases where no new executable file is downloaded during the updating process).

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

b. Windows Updates

AppSamvid software has support for automatic installation of Microsoft Windows Updates that install through the 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 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 whitelist enforcement to make the system boot normally and **free it from a continuous loop of trying to install Windows Updates** at system boot-up time.

c. 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 the user is completely aware of what he is blocking from execution.

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

©2024, Centre for Development for Advanced Computing – Hyderabad