

# VoodooShield 6.00



## User Guide

October 2020

Important Note: Antivirus testing labs should run VoodooShield in AutoPilot mode when testing VoodooShield with traditional antivirus methodologies, since this mode emulates as closely as possible traditional antivirus. Software reviewers and pen testers should run VoodooShield in Smart (Default) mode when testing VoodooShield to truly appreciate all of the benefits that our proprietary technology has to offer.

## **Table of Contents**

1. Welcome to VoodooShield
  - a. The Concept
  - b. How VoodooShield is different
  - c. How to use VoodooShield
2. How to use VoodooShield
  - a. Left click on shield or tray icon
  - b. Right click on shield or tray icon for menu
3. VoodooShield Modes
  - a. Disable / Install Mode
  - b. Training
  - c. AutoPilot
  - d. Smart Mode (Default)
  - e. Always ON
4. User Prompts
  - a. Mini Prompt
  - b. Full User Prompt
5. VoodooShield Settings
  - a. Basic Settings
  - b. Advanced Settings
  - c. Web Apps
  - d. User Interface Tweaks
  - e. Custom Folders
  - f. Utility Settings
  - g. Whitelist Editor
  - h. User Log
  - i. Command Lines
  - j. Quarantine
  - k. VoodooShield Rules
  - l. Registration
  - m. WhitelistCloud
  - n. Web Management
  - o. Other Buttons
6. Proprietary / Special VoodooShield Features
  - a. VoodooAi
  - b. Drag and drop to VoodooShield to scan a file
  - c. Local Sandbox
  - d. Cuckoo / Remote Sandbox

## **Welcome to VoodooShield**

### **The Concept**

Although VoodooShield is extremely user-friendly, it is quite different from traditional blacklist antivirus, so it is vital that the user understands how it works in order to use it properly. Please keep in mind, VoodooShield is not intended to replace your current security solution, but rather to compliment it by adding an additional initial layer of protection that acts as a lock, rather than a traditional blacklist filter.

Traditional antivirus software can no longer keep up with the 300,000+ new viruses and malware created daily, so VoodooShield locks your computer and blocks all new, non-whitelisted executable code (including viruses and malware), while your computer is running a web app (browser, email, etc.).

Since most viruses and malware attack through web browsers and email attachments, VoodooShield simply locks your computer when you are browsing the web or checking email. It also protects the user space when not at risk. When used properly, VoodooShield will effectively block all browser and email based viruses and malware. VoodooShield does not remove existing viruses.

VoodooShield uses a proprietary proactive whitelist snapshot approach to virus and malware protection. VoodooShield is a patented toggling Desktop Shield Gadget / Computer Lock that automatically toggles to ON and locks your computer when you start a web app.

There is never a good reason to let new, non-whitelisted executable code run while a web app is running.

**Important Note:** If you are installing VoodooShield for the first time because you were recently infected with malware and have decided to start locking your computer while it is at risk, and are concerned with pre-existing malware, then it is recommended that you reset your whitelist once a week until you are certain that the infection is clean. This will ensure that pre-existing malware is not inadvertently whitelisted.

## **How VoodooShield is different**

VoodooShield is the only patented tangible toggling computer lock in the industry, and it is designed to complement your antivirus (including Windows Defender). There are other deny-by-default / zero trust products, but only VoodooShield functions as an actual computer lock with dynamic levels of protection (dynamic security postures). If it does not toggle, it is not a lock.

The Achilles' heel of all security products is that they are only able to offer a single static level of protection, so at any given time their security posture is likely either too aggressive or too relaxed, resulting in false positives and breaches. VoodooShield solves this issue by dynamically adjusting its security posture on the fly, based on the end-user's current activity and behavior. Because of our dynamic security postures feature, VoodooShield is able to offer a tighter and more robust lock than is possible with any other product.

Cybersecurity experts agree that application whitelisting is by far the most effective security mechanism on the market, but no one ever bothered to make this technology user-friendly enough for the masses, until we created VoodooShield. Before VoodooShield, all application whitelisting products were active full-time, often when it did not make sense to be active, which most users and administrators found to be annoying and untenable, so they would choose to forgo application whitelisting altogether. Our patented snapshot technology automatically builds the tiny, customized whitelist for the end-user, resulting in the smallest possible whitelist and attack surface in the industry.

VoodooShield does not force the end-user to respond to dangerous affirmative user prompts, which eliminates the possibility the end-user inadvertently allows an unknown item. Instead, VoodooShield displays a mini prompt prior to asking the end-user to make a decision on whether to allow a new item or not.

Through our WhitelistCloud technology, VoodooShield is the only product in the industry that scans our proprietary tiny, customized whitelist specifically for safe / clean files and automatically creates firewall rules for unknown items. In other words, traditional antivirus scans for malware while WhitelistCloud scans for safe / clean files. As a result, Administrators are continually aware that only safe items are running on the endpoints. With traditional AV engines, Administrators are somewhat certain that malware is not executing on the endpoints, but with WhitelistCloud, they are essentially certain that only safe items are executing at any moment in time.

VoodooShield considers the entire attack chain in the parent / child process creation relationship. Not only does this make VoodooShield more secure, our mechanism is flexible so that blacklisting vulnerable items globally is not required. For example, VoodooShield is not required to blacklist PowerShell globally in order to protect against PowerShell attacks. VoodooShield considers the entire attack chain so that benign scripts that need to execute are able to do so, while blocking malicious PowerShell attacks.

VoodooShield includes extremely robust ransomware, script, LOLBins and fileless malware protection capabilities.

VoodooShield created the anti-exploit mechanism that many vendors utilize today, but chose not to patent it. VoodooShield is also the only deny-by-default product that protects the entire Windows system, as opposed to only protecting the Windows components that are currently being exploited by

malware authors. With VoodooShield, there is no need to update our mechanism when malware authors discover a new Windows component to exploit, which tends to happen every 3-4 months.

VoodooShield utilizes ML/Ai (VoodooAi) and reputation based file insight (WhitelistCloud) that provides the end-user with file insight so they are able to make an informed decision, while offering an end-user recommendation based on the provided file insight.

Unlike products that utilize legacy / deprecated Software Restriction Policy (SRP) that operates in user-mode, VoodooShield utilizes a modern kernel-mode monolithic blocking mechanism that does not require patches, hacks or tweaks to protect against new or undiscovered vulnerabilities and threats. In addition, unlike other products in its class, VoodooShield is refined to the point that it does not require vendor co-management of the Web Management Console.

VoodooShield Pro is highly customizable through its settings, allowing Administrators to fine tune the overall security posture for each end-user.

## How to use VoodooShield

**The golden rule of VoodooShield:** If VoodooShield blocks something that you asked or intended to run, then allow it (assuming that there are no warnings from VoodooAi or WhitelistCloud). Otherwise, if VoodooShield blocks something out of the blue, then just ignore it and assume it was a malware or a virus.

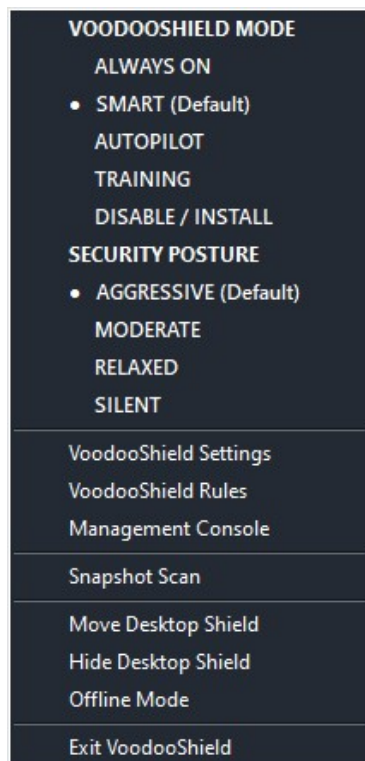
### Left click on shield or tray icon

VoodooShield is a toggling desktop shield gadget / computer lock, and the whole concept is to lock your computer whenever a web app is running, since it is at risk. If VoodooShield is ON, you can left click on the desktop shield gadget or tray icon to turn it OFF. If VoodooShield is in Always ON or Smart mode (with a web app running), you can left click on the desktop shield gadget or tray icon to turn it back ON. VoodooShield is smart and will do its best to ensure that it is ON whenever a web app is running, even if you temporarily turn it OFF.

After installation, VoodooShield will automatically take a quick whitelist snapshot of your system and place VoodooShield in Smart mode. You can keep VoodooShield in Smart mode full time, or you can change to one of the other modes described below.

### Right click on shield or tray icon for menu

The user can right click on the desktop shield gadget or tray icon to display the following menu.



Left clicking the VoodooShield Settings option will display the settings window where you can adjust advanced settings, choose web apps and custom folders, and view / edit the whitelist, user logs, command lines and quarantine items. If you have purchased a VoodooShield Pro license, you can also register your VoodooShield Pro account in the settings window, which will unlock all of the advanced settings and features.

## **VoodooShield Modes**

### **Disable Protection (VoodooShield will remain OFF):**

Disable Protection mode is similar to Training mode, except new items are not added to the whitelist, so it is typically used when you are installing new software, but do not want the installer items to be automatically added to the whitelist. The computer is not protected in Disable Protection mode.

### **Training (VoodooShield will remain OFF):**

Training mode is typically used when you initially install VoodooShield, or when you are installing or running new software. VoodooShield will remain OFF and will allow all new items and automatically add them to the whitelist, so they will not be blocked once VoodooShield turns back ON. The computer is not protected in Training mode.

### **AutoPilot Mode (VoodooShield will remain in AutoPilot Mode):**

AutoPilot mode will remain in AUTO Mode and automatically allow and whitelist any file that is determined to be Safe by VoodooAi and WhitelistCloud. If a non-whitelisted process is spawned that is determined to be Not Safe by VoodooAi or WhitelistCloud, VoodooShield will block the item and prompt the user so they can decide whether to allow the item or not.

AutoPilot mode is a great choice for users who want the power and performance of application whitelisting, without the hassle of constantly being bombarded by affirmative user prompts. Gamers and software testers typically use this mode.

### **Smart / Default (VoodooShield will toggle between ON and OFF):**

Smart mode will toggle VoodooShield between ON and OFF, depending on if the computer is at risk of infection or not, which is mainly determined by whether a web app is running or not. Web apps such as Internet Explorer, Outlook and Firefox all expose the computer to significant risk while they are running, so when a web app is launched, VoodooShield automatically toggles to ON to lock the computer, and anything that was previously whitelisted is allowed, but all new non-whitelisted executable code is blocked.

Likewise, if no web apps are running, there is no reason to lock the computer, so VoodooShield automatically toggles to OFF so that it can automatically and safely build the whitelist while the computer is not at risk. VoodooShield's proprietary toggling severely limits the quantity of dangerous affirmative user prompts that the user is required to respond to.

### **Always ON (VoodooShield will remain ON):**

Always ON mode is typically used after a few days or weeks, once the whitelist is sufficiently built so that VoodooShield knows what to block and what to allow. Although a lot of users prefer to run VoodooShield in AutoPilot or Smart mode full time.

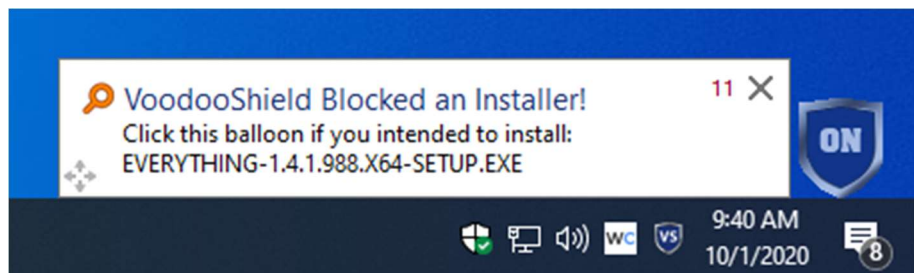


## User Prompts

In its default settings, VoodooShield utilizes a deny-by-default method so that dangerous affirmative user prompts are avoided as much as possible. That is, for security reasons the user should not be required to make a decision on whether to block or allow a new non-whitelisted item that VoodooShield has blocked. There is no reason to take a chance that a blocked item might be malicious, especially when the user does not need or want to run the blocked item.

### Mini Prompt

VoodooShield accomplishes this by initially displaying a mini prompt when a new non-whitelisted item is blocked, and the mini prompt will automatically close after 20 seconds, requiring no user interaction if the blocked item is not required to run. If the user wishes to run the blocked item, they can click on the mini prompt, and the full user prompt will be displayed, providing the user with relevant information about the blocked item, along with buttons to allow the user to allow, block, sandbox or quarantine the blocked item.



## Full User Prompt

Upon clicking the mini prompt, the full user prompt will be displayed, along with relevant information about the file, so the user can make the decision on whether to allow, block or quarantine the blocked item.

In the three scenarios provided below, the user can also click the Sandbox button to run the file with limited rights, or to run the file in a remote sandbox, while viewing the execution in a Remote Desktop session. The Remote Desktop session allows the user to see first-hand the implications of running the blocked file, safely, on a remote machine before they choose to allow the file.

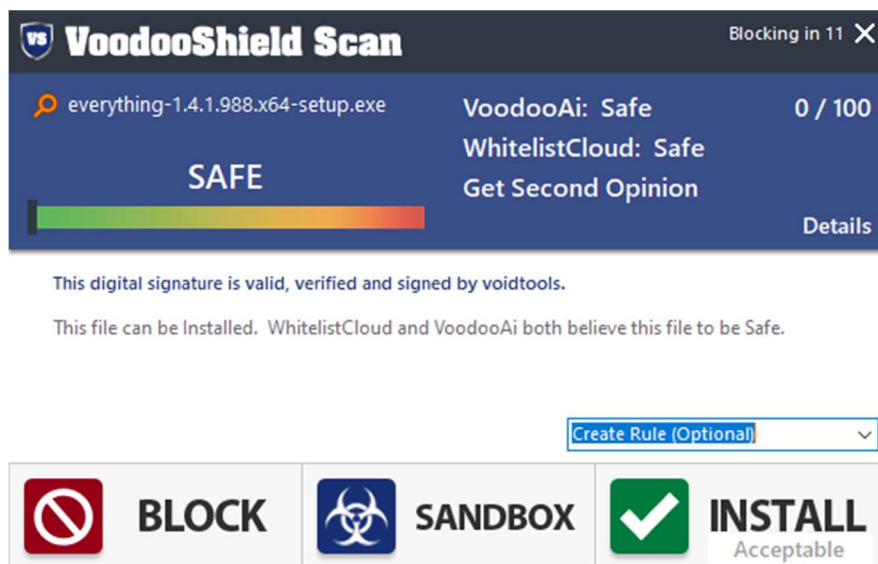
**Block (Button):** This button will block the item and ensure that it is not executed or whitelisted.

**Sandbox (Button):** This button will display the Sandbox screen and will give the user the option to run the file in a Local Sandbox or in the Cuckoo Sandbox.

**Allow (Button):** This button will allow and whitelist the item.

**Install (Button):** This button will be displayed in place of the Allow button if the blocked item is detected as an installer file. Clicking the Install button will toggle VoodooShield to OFF so that installation of the new software can complete without interruption, and it will allow and whitelist the item.

## Safe Blocked Item



VoodooAi and WhitelistCloud have both determined that this item is Safe, so it is recommended that the user click the Allow button to allow the item to add it to the whitelist, assuming this is an item they wish to allow.

## Unsafe Blocked Item

 **VoodooShield Alert** Blocking in 11 X

 malware.exe

**UNSAFE**

VoodooAi: Unsafe 100 / 100  
WhitelistCloud: Not Safe  
Get Second Opinion

Details

This file is not digitally signed!

This file should be Blocked. WhitelistCloud determined this file to be Not Safe, and VoodooAi believes this file to be Unsafe.

☐ Report False Positive


Create Rule (Optional) 

 <b>BLOCK</b> Recommended	 <b>QUARANTINE</b>	<b>SANDBOX</b>
		<b>ALLOW FALSE POSITIVE</b>

VoodooAi and WhitelistCloud have both determined that this item is Unsafe / Not Safe, so it is recommended that the user click either the Block or Quarantine button to safely handle this item.

## Suspicious Blocked Item

 **VoodooShield Alert** Blocking in 11 X

 applicationname test.exe

**SUSPICIOUS**

VoodooAi: Suspicious 77 / 100  
WhitelistCloud: Not Safe  
Get Second Opinion

Details

This file is not digitally signed!

This file should be Blocked. WhitelistCloud determined this file to be Not Safe, and VoodooAi believes this file to be Suspicious.

☐ Report False Positive

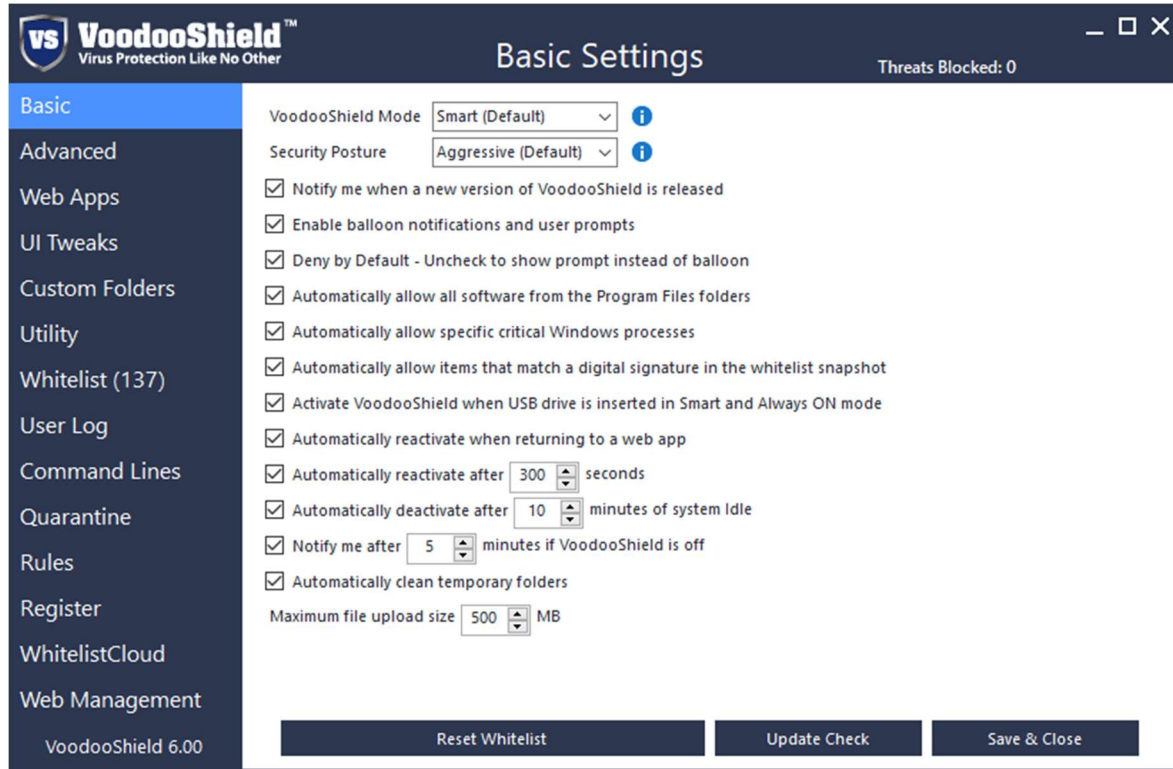
Create Rule (Optional) 

 <b>BLOCK</b> Recommended	 <b>QUARANTINE</b>	<b>SANDBOX</b>
		<b>ALLOW FALSE POSITIVE</b>

VoodooAi has determined that this item is Suspicious and WhitelistCloud has determined that the item is Not Safe, so it is recommended that the user click the Block button to safely handle this item.

# VoodooShield Settings

## Basic Settings



The Basic Settings tab allows the user to adjust various basic settings, according to their preferences.

**VoodooShield Mode:** This option will allow the user to change VoodooShield's Mode to Always ON, Smart (Default), AutoPilot, Training or Disable / Install.

**Security Posture:** This option will allow the user to change VoodooShield's Security Posture to Aggressive (Default), Moderate, Relaxed or Silent.

**Notify me when a new version of VoodooShield is released:** When enabled, VoodooShield will automatically alert you for program updates and new releases. VoodooShield does not rely on technologies such as blacklisting that require frequent updates, so updates are released every few months to add new features and fix minor bugs.

**Enable balloon notifications and user prompts:** When enabled, VoodooShield will display a mini prompt or full user prompt when a new non-whitelisted item is blocked. System administrators might wish to disable this feature and add a password in the Utility tab to ensure the user does not add new items to the whitelist without permission.

**Deny by Default - Uncheck to show prompt instead of balloon:** When enabled, VoodooShield will display the mini prompt notification that does not require a response or user interaction. If the user

wishes to allow a new item, they can click on the mini prompt and the full user prompt will be displayed. When disabled, VoodooShield will display a full user prompt that the user is able to respond to, instead of initially displaying the mini prompt.

**Automatically allow all software from the Program Files folders:** When enabled, all items in Program Files and Program Files (x86) directories are automatically allowed. While on the surface this option may not appear to be safe, these directories are Windows Protected Folders, so it is actually safe.

**Automatically allow specific critical Windows processes:** When enabled, all items in specific Windows directories are automatically allowed. While on the surface this option may not appear to be safe, these directories are Windows Protected Folders, so it is actually safe.

**Automatically allow items that match a digital signature in the whitelist snapshot:** Allowing items by digital signature in general can be dangerous. When enabled, once a new item is allowed and whitelisted, any child process of the newly whitelisted item is allowed, assuming that the digital signature matches. Allowing by digital signature is temporary, and only one digital signature of a parent process is allowed at any given time. Once a new item is allowed, the temporary digital signature changes to the digital signature of the newly allowed parent process.

**Activate in smart mode when USB drive is inserted in Smart and Always ON mode:** When enabled, VoodooShield will automatically toggle to ON when a USB drive is inserted.

**Automatically reactivate when returning to a web app:** When enabled, VoodooShield will automatically toggle to ON when a web app gains focus of the screen (after prompting the user to do so), assuming the user manually turned VoodooShield OFF at some point.

**Automatically reactivate after 300 seconds:** When enabled, VoodooShield will prompt the user to turn VoodooShield back on after 5 minutes of being OFF, assuming the user manually turned VoodooShield OFF at some point.

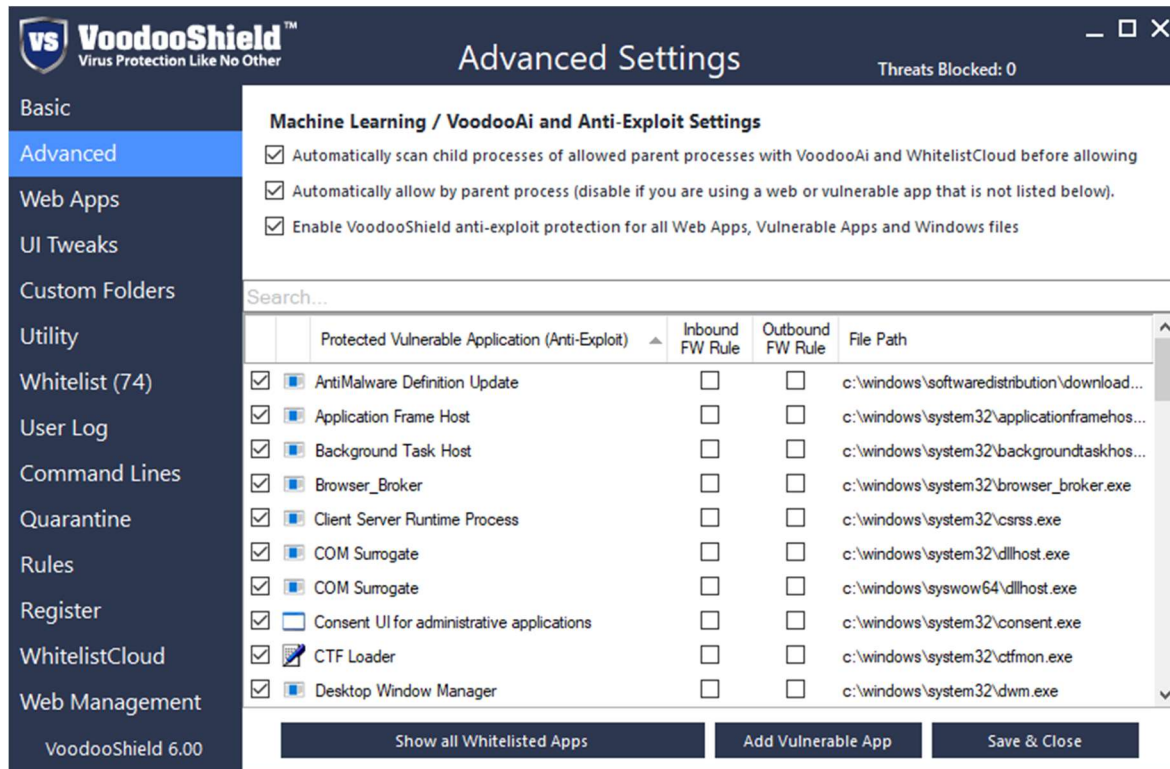
**Automatically deactivate after 10 minutes of system idle:** When enabled, VoodooShield will automatically deactivate after 10 minutes of system idle, in order to allow background processes and updates to run properly. When the user returns to the computer, VoodooShield will automatically reactivate upon mouse or keyboard use.

**Notify me after 5 minutes if VoodooShield is off:** When enabled, if the user temporarily disables VoodooShield, they will be notified after 5 minutes to turn VoodooShield back ON.

**Automatically clean temporary folders:** When enabled, VoodooShield will automatically clean user and system temporary folders.

**Maximum file upload size 500 MB:** This option will set the maximum file upload size for new files that are not currently in the WhitelistCloud database and need to be uploaded to WhitelistCloud for analysis.

## Advanced Settings



The Advanced Settings tab allows the user to adjust various advanced settings, according to their preferences. Protected Vulnerable Apps are listed with checkboxes and the user can choose which vulnerable applications are protected by VoodooShield from potential exploits spawning malicious payloads. VoodooShield automatically manages these settings and they should only be changed by advanced users who understand vulnerable applications, otherwise unnecessary blocks or bypasses can result if these settings are not configured properly. Inbound and Outbound Firewall Rule checkboxes allow the user to quickly create Windows Defender Firewall rules for any item on the list.

**Automatically scan child processes of allowed parent processes with VoodooAi and WhitelistCloud before allowing:** When enabled, VoodooShield will automatically scan the blocked item with VoodooAi and WhitelistCloud and block the item if it is not determined to be Safe.

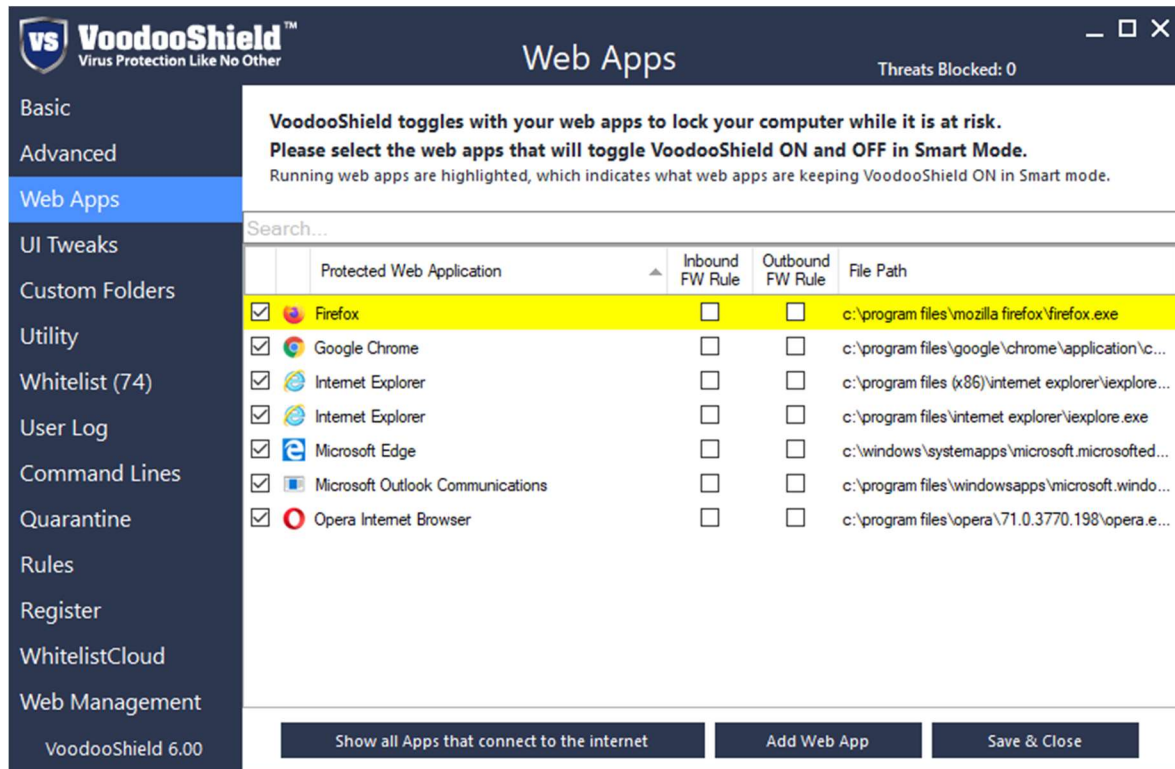
**Automatically allow by parent process (disable if you are using a web app that is not listed below):** When enabled and a new item is allowed, child processes of the newly allowed parent process are allowed, assuming certain conditions and checks are met.

**Enable VoodooShield anti-exploit protection for all web apps in all file / folder locations:** When enabled, this feature automatically blocks all child processes of web app parent processes. In other words, this feature effectively blocks payloads dropped by exploits.

**Show all Whitelisted Apps / Show only Vulnerable Apps (Button):** This button will allow the user to toggle between displaying all Whitelisted Apps and displaying only Vulnerable Apps.

**Add Vulnerable App (Button):** This button will allow the user to add a vulnerable app that is not already listed.

## Web Apps



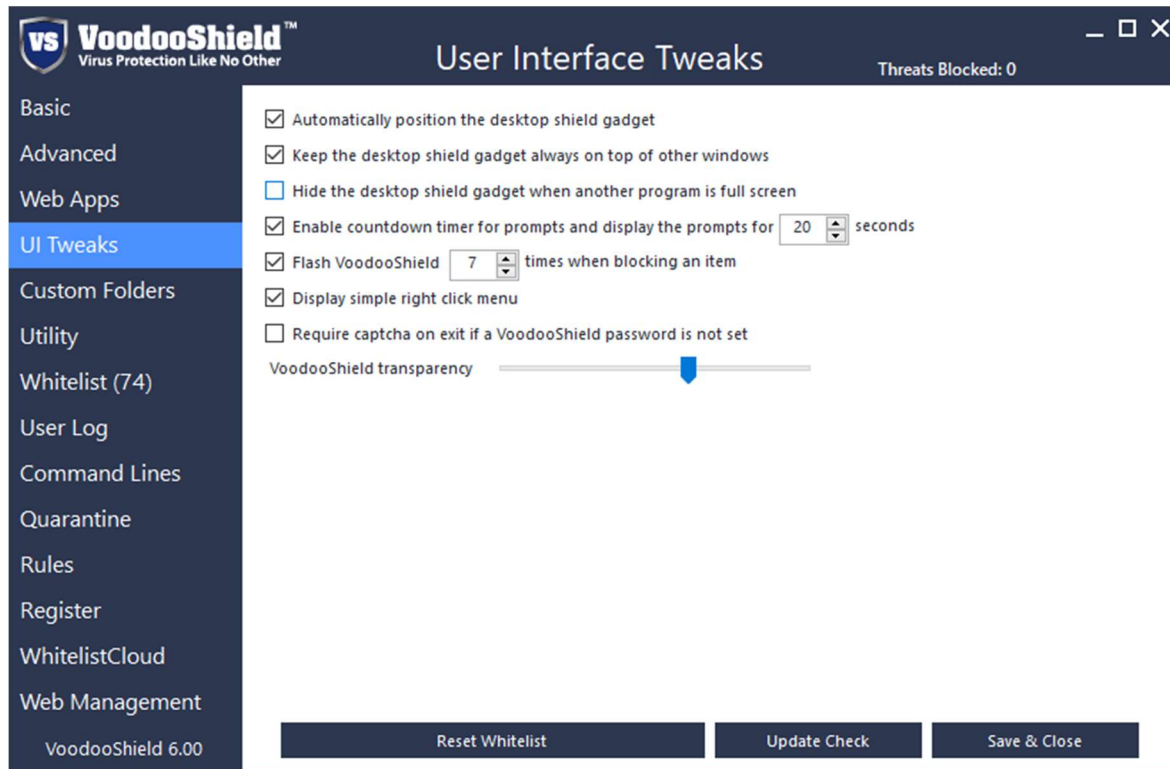
VoodooShield toggles with your web apps to lock your computer while it is at risk. The Web Apps tab allows the user to choose and customize which web apps toggle VoodooShield from OFF to ON while in Smart mode. Running web apps are highlighted, which indicates what web apps are keeping VoodooShield ON in Smart mode. Inbound and Outbound Firewall Rule checkboxes allow the user to quickly create Windows Defender Firewall rules for any item on the list.

**Show all Apps that connect to the internet / Show only Common Web Apps (Button):** This button will allow the user to toggle between displaying all Apps that connect to the internet and displaying only Common Web Apps.

**Add Web App (Button):** This button will allow the user to add a web app that is not already listed.



## User Interface Tweaks



The User Interface Tweaks tab allows the user to adjust the various user interface features of VoodooShield.

**Automatically position the desktop shield gadget:** When enabled, the desktop shield gadget will automatically be positioned in the default lower right location of the screen. If the user right clicks on the desktop shield gadget or tray icon and selects “Move”, this feature will automatically become disabled, thereby allowing the user to reposition the desktop shield gadget to their desired location.

**Keep the desktop shield gadget always on top of other windows:** When enabled, this feature will keep the desktop shield gadget on top of all other windows, so the user knows the status of the lock at all times, and is able to quickly turn VoodooShield ON or OFF.

**Hide the desktop shield gadget when another program is full screen:** When enabled, VoodooShield will automatically hide behind any window that is displayed in full screen mode. This feature is helpful for users who wish to, for example, hide the desktop shield gadget while watching full screen videos on their computer.

**Enable countdown timer for prompts and display the prompts for 20 seconds:** For security reasons, it is vital that the user is not forced to respond to affirmative prompts, so a countdown timer is included to automatically dismiss the mini prompts and full user prompts after the specified time period.

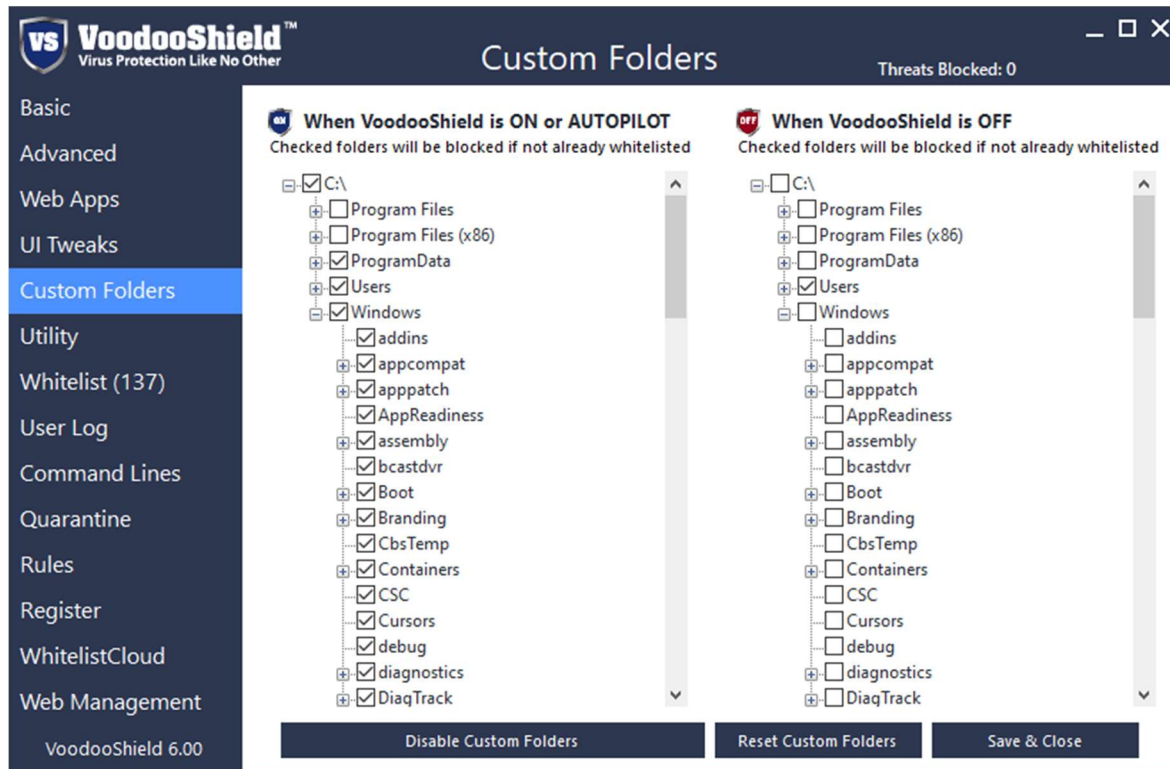
**Flash VoodooShield 7 times when blocking an item:** When enabled, VoodooShield will flash after it has blocked an item that is not on the whitelist, for the specified number of times.

**Display simple right click menu:** When enabled, VoodooShield will display the commonly used items on the right click menu, otherwise if disabled, additional items will be displayed.

**Require captcha on exit if a VoodooShield password is not set:** As a security precaution, when enabled, VoodooShield will require the user to enter a correct captcha when they exit VoodooShield.

**VoodooShield transparency:** This feature allows the user to adjust the transparency / opacity of the desktop shield gadget.

## Custom Folders



The Custom Folders tab allows the user to specify which folders are allowed and blocked as VoodooShield toggles from ON to OFF.

To use this feature, you need to enable it first by clicking the Enable Custom Folders button below.

**Enable / Disable Custom Folders (Button):** This button will enable or disable the Custom Folders feature.

**Reset Custom Folders (Button):** This button will reset the Custom Folders feature to the default settings, and all custom folder settings are cleared.

After enabling the Custom Folders feature, the following settings will become unavailable and will be controlled by the custom folders feature.

- Automatically allow all software from the Program Files folders
- Automatically allow specific critical Windows processes
- Automatically scan user space items when VoodooShield is OFF in Smart or Always ON mode

## Utility Settings

The screenshot shows the 'Utility Settings' window of VoodooShield. The interface includes a sidebar with the following menu items: Basic, Advanced, Web Apps, UI Tweaks, Custom Folders, **Utility** (selected), Whitelist (137), User Log, Command Lines, Quarantine, Rules, Register, WhitelistCloud, and Web Management. The version 'VoodooShield 6.00' is displayed at the bottom of the sidebar. The main content area features a grid of buttons: 'Backup Whitelist to Desktop', 'Backup Settings to Desktop', 'Restore Whitelist from File', 'Restore Settings from File', 'Upload Whitelist to Cloud', and 'Upload Settings to Cloud'. Below these is a section titled 'Set VoodooShield password' with three input fields labeled 'Password:', 'Password:', and 'Create Hint:', followed by a 'Set Password' button. At the bottom of the window are three buttons: 'Use individual settings for each user', 'Update Check', and 'Save & Close'.

The Utility tab allows for various backup and restore operations within VoodooShield, and allows the user to set or clear the VoodooShield password.

**Backup Whitelist to Desktop (Button):** This button will backup the whitelist data file to the desktop.

**Backup Settings to Desktop (Button):** This button will backup the settings data file to the desktop.

**Restore Whitelist from File (Button):** This button will restore the whitelist data file from the specified location.

**Restore Settings from File (Button):** This button will restore the settings data file from the specified location.

**Restore Default Settings (Button):** This button will restore all of the VoodooShield settings to their default values.

**Clear Threats Blocked Count (Button):** This button will reset the Threats Blocked Count to zero.

**Set VoodooShield password:** This feature will allow the user or system administrator to set a password for VoodooShield which limits what functions are available to the user. This feature is particularly helpful in the enterprise, where system administrator wish to lock the computer down as tightly as possible.

## Whitelist Editor

**VoodooShield™**  
Virus Protection Like No Other

Whitelist Editor

Red = System File  
Threats Blocked: 0

Search...

Time Stamp	Action	Process	Process Path
9/30/2020 11:08 PM	Auto Allowed	accessiblehandler.dll	c:\program files\mozilla firefox\accessiblehandler.dll
9/30/2020 11:08 PM	Auto Allowed	accessiblemarshal.dll	c:\program files\mozilla firefox\accessiblemarshal.dll
9/30/2020 11:05 PM	Auto Allowed	am_delta.exe	c:\windows\softwaredistribution\download\install\ar
9/10/2020 1:15 AM	Snapshot	applicationframehost.exe	c:\windows\system32\applicationframehost.exe
9/30/2020 11:08 PM	WhitelistCloud	assistant_installer.exe	c:\program files\opera\assistant\assistant_installer.e
9/30/2020 11:08 PM	WhitelistCloud	assistant_installer.exe	c:\program files\opera\assistant\assistant_installer.e
9/30/2020 11:12 PM	Auto Allowed	assistant_installer.exe	c:\program files\opera\assistant\assistant_installer.e
9/10/2020 1:27 AM	Snapshot Sync	audiodg.exe	c:\windows\system32\audiodg.exe
9/10/2020 1:16 AM	Auto Allowed	backgroundtaskhost.exe	c:\windows\system32\backgroundtaskhost.exe
9/30/2020 11:07 PM	Auto Allowed	backgroundtransferhost.exe	c:\windows\system32\backgroundtransferhost.exe
9/30/2020 11:08 PM	WhitelistCloud	browser_assistant.exe	c:\program files\opera\assistant\browser_assistant.x
9/30/2020 11:08 PM	WhitelistCloud	browser_assistant.exe	c:\program files\opera\assistant\browser_assistant.x
9/10/2020 1:31 AM	Snapshot Sync	browser_broker.exe	c:\windows\system32\browser_broker.exe
9/30/2020 11:07 PM	Auto Allowed	browser_broker.exe	c:\windows\system32\browser_broker.exe
9/30/2020 11:09 PM	Auto Allowed	chrome.exe	c:\program files\google\chrome\application\chrome

Reset Whitelist    Update Check    Save & Close

VoodooShield 6.00

The Whitelist editor tab allows the user to view and edit the whitelist, by right clicking on a whitelisted item and choosing “Delete”. System files are displayed in red and non-system files are displayed in black.

## User Log

**VoodooShield™**  
Virus Protection Like No Other

**User Log**

Red = Blocked / Quarantined  
Threats Blocked: 0

Search...

Time Stamp	Action	Process	Process Path
9/30/2020 11:08 PM	WhitelistCloud	googleupdate.exe	c:\program files (x86)\google\update\googleupdate
9/30/2020 11:08 PM	WhitelistCloud	googleupdatecomregistershell64.exe	c:\program files (x86)\google\update\1.3.35.451\gc
9/30/2020 11:08 PM	WhitelistCloud	googleupdate.exe	c:\program files (x86)\google\update\googleupdate
9/30/2020 11:08 PM	WhitelistCloud	googleupdate.exe	c:\program files (x86)\google\temp\gum613c.tmp\g
9/30/2020 11:08 PM	Auto Allowed	msi5576.tmp	c:\windows\installer\msi5576.tmp
9/30/2020 11:08 PM	Auto Allowed	googlechromestandaloneenterpris...	c:\users\voodoo\appdata\local\temp\b05618~2\g
9/30/2020 11:08 PM	Auto Allowed	unsecapp.exe	c:\windows\system32\wbem\unsecapp.exe
9/30/2020 11:08 PM	WhitelistCloud	launcher.exe	c:\program files\opera\launcher.exe
9/30/2020 11:08 PM	WhitelistCloud	browser_assistant.exe	c:\program files\opera\assistant\browser_assistant.x
9/30/2020 11:08 PM	WhitelistCloud	browser_assistant.exe	c:\program files\opera\assistant\browser_assistant.x
9/30/2020 11:08 PM	WhitelistCloud	assistant_installer.exe	c:\program files\opera\assistant\assistant_installer.e
9/30/2020 11:08 PM	WhitelistCloud	assistant_installer.exe	c:\program files\opera\assistant\assistant_installer.e
9/30/2020 11:08 PM	WhitelistCloud	assistant_installer.exe	c:\users\voodoo\appdata\local\temp\opera\opera
9/30/2020 11:08 PM	WhitelistCloud	installer.exe	c:\program files\opera\71.0.3770.198\installer.exe
9/30/2020 11:08 PM	WhitelistCloud	installer.exe	c:\program files\opera\71.0.3770.198\installer.exe

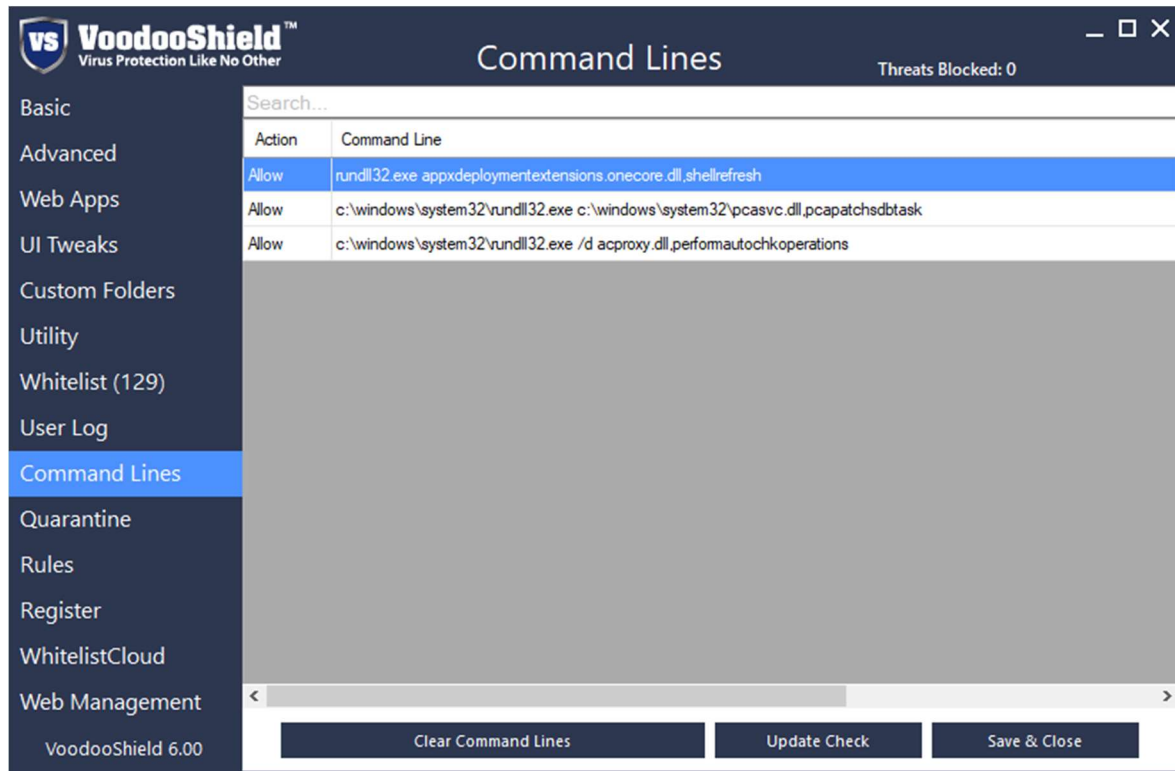
Clear User Log    Update Check    Save & Close

VoodooShield 6.00

The User Log tab allows the user to view the User Log and whitelist blocked items. The user can whitelist an item by right clicking and choosing “Whitelist Item”. Blocked and quarantined files are displayed in red and allowed files are displayed in black.

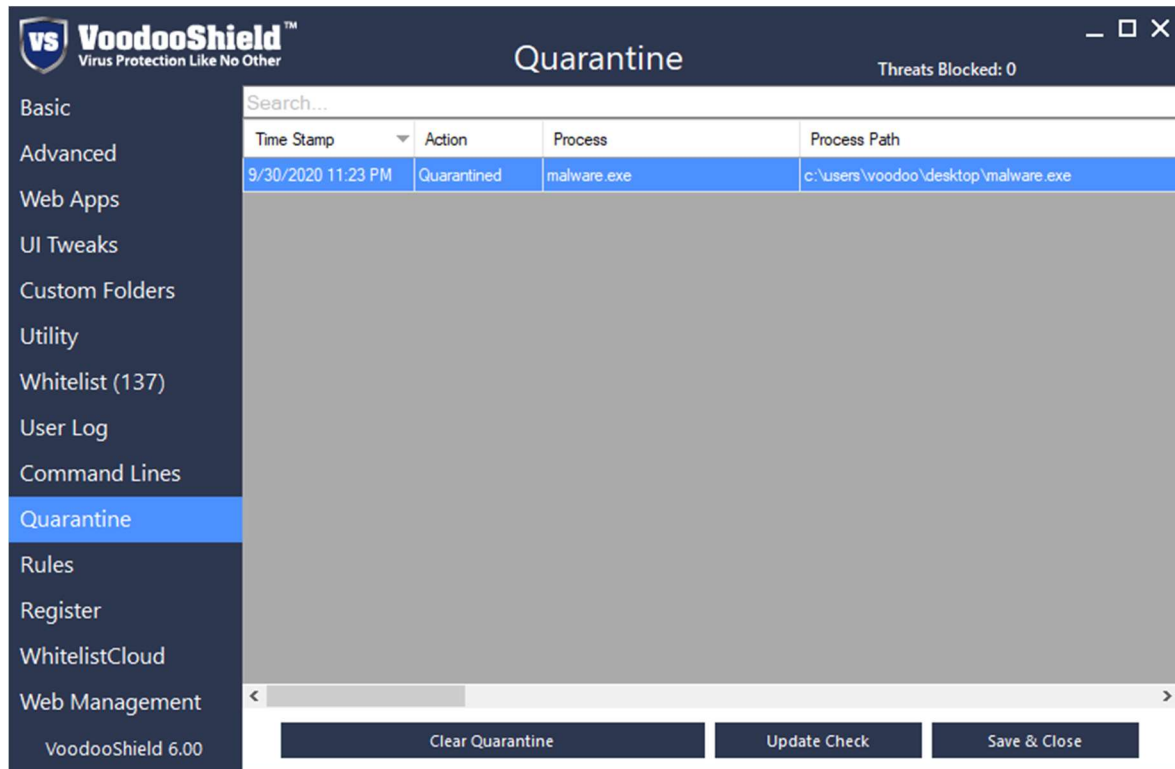
**Clear User Log (Button):** This button will clear all of the User Log items.

## Command Lines



The Command Lines tab allows the user to view and edit the Command Lines. Multiple right click functions are provided, allowing the user to Allow, Block, Add, Edit, Delete and Delete All command line items. Blocked command lines are displayed in red and allowed command lines are displayed in black.

## Quarantine

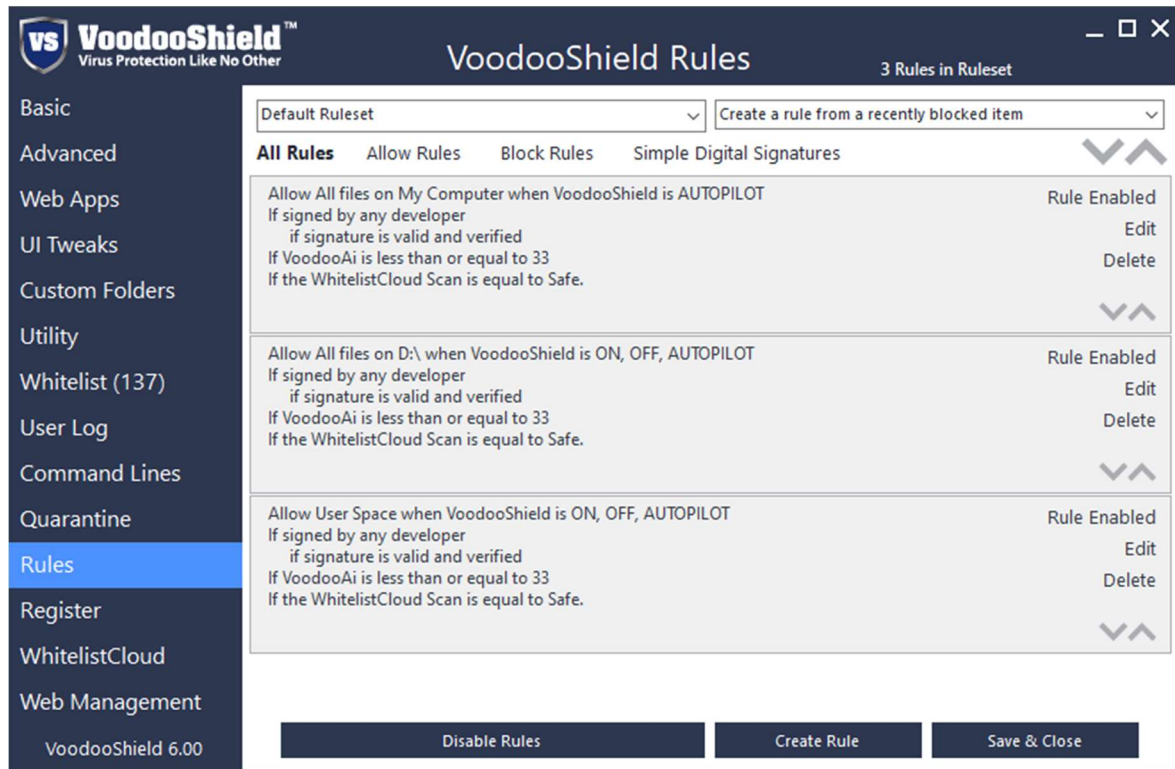


The Quarantine tab allows the user to view and edit the quarantine items. Multiple right click functions are provided, allowing the user to Restore, Delete and Delete All command line items.

**Clear Quarantine (Button):** This button will clear all of the quarantine items and delete the quarantined files.



## VoodooShield Rules



The VoodooShield Rules tab allows the user to create highly customizable and powerful rules to automatically block or allow specific items based on the rule type and file insight.

**Enable / Disable VoodooShield Rules (Button):** This button will enable or disable the VoodooShield Rules feature.

**Create Rule (Button):** This button will allow the user to create a new VoodooShield Rule.

## Registration

**VoodooShield™**  
Virus Protection Like No Other

# Registration

Threats Blocked: 0

Basic  
Advanced  
Web Apps  
UI Tweaks  
Custom Folders  
Utility  
Whitelist (137)  
User Log  
Command Lines  
Quarantine  
Rules  
**Register**  
WhitelistCloud  
Web Management  
VoodooShield 6.00

**Thank you for choosing VoodooShield Pro!**

**You are currently registered, with an expiration date of 11/11/2050.**

There are 10998 days remaining in your VoodooShield Pro subscription.  
We appreciate your support in the development of VoodooShield!

Email Address OR Product Key

Purchase Additional License Online

Password (Not Required if using Product Key)

Confirm Registration

Machine Name:  
DESKTOP-7QDEHK0

Machine ID:  
1D03-5A36-E2FF-2424-E2C9-7ED6-DE84-391C

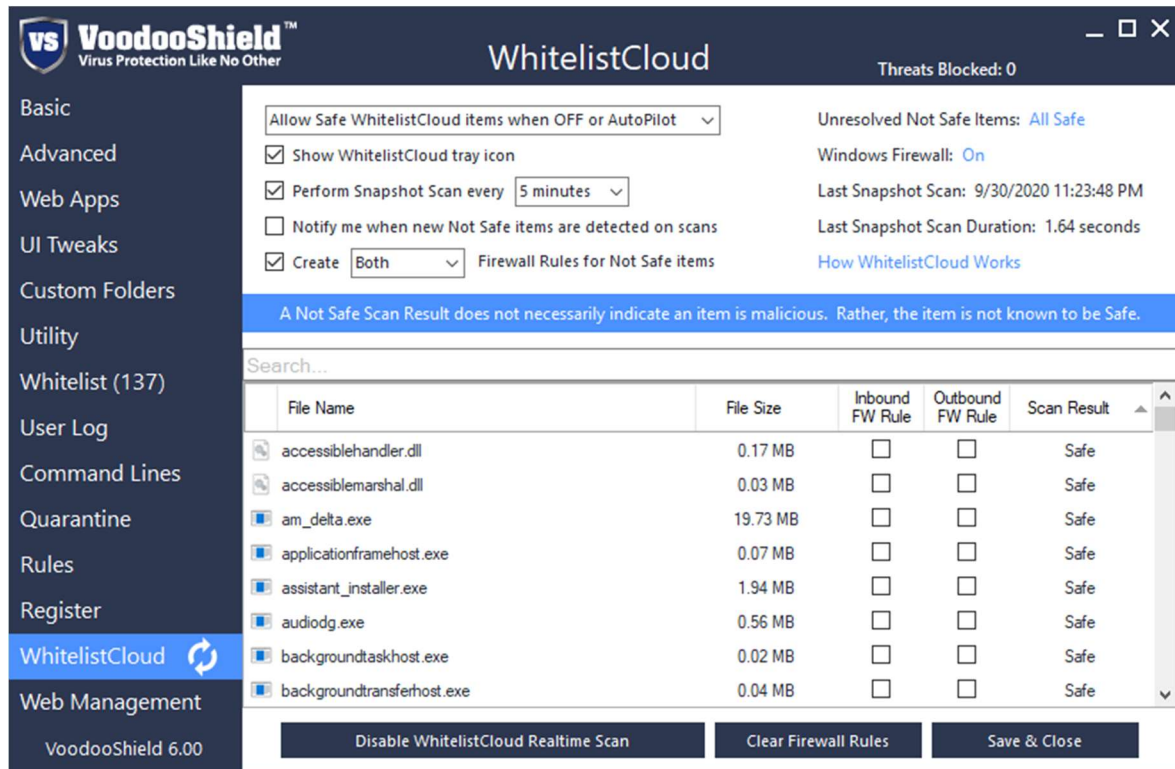
Reset Registration    Update Check    Save & Close

The Registration tab allows the user to register VoodooShield Pro to unlock all of the advanced settings and features included with VoodooShield Pro.

To register VoodooShield Pro:

1. If you have not already purchased a VoodooShield Pro license, please click the “Step 1: Purchase a License Online” button and complete the online registration.
2. Once your VoodooShield Pro account is registered, simply enter your email address and password for your VoodooShield account, then click the “Step 2: Confirm Registration” button to register VoodooShield Pro and unlock all of the advanced settings and features.

## WhitelistCloud



The **WhitelistCloud** tab allows the user to adjust various **WhitelistCloud** settings, according to their preferences, and to modify the **WhitelistCloud** list. Inbound and Outbound Firewall Rule checkboxes allow the user to quickly create Windows Defender Firewall rules for any item on the list.

**WhitelistCloud Mode:** This option allows the user to adjust when new, non-whitelisted files are automatically allowed by **WhitelistCloud**. The three options are as follows.

- Do not Automatically Allow Safe **WhitelistCloud** items
- Allow Safe **WhitelistCloud** items when OFF or AutoPilot
- Automatically allow Safe **WhitelistCloud** items Full-Time

**Show WhitelistCloud tray icon:** This option allows the user to choose whether the **WhitelistCloud** system tray icon is displayed or not.

**Perform Snapshot Scan every 5 minutes:** This option allows the user to choose when **WhitelistCloud** performs a scan.

**Notify me when new Not Safe items are detected on scans:** This option allows the user to choose whether the **WhitelistCloud** system tray icon is displayed or not.

**Create Both Firewall Rules for Not Safe items:** This option allows the user to choose whether the **WhitelistCloud** system tray icon is displayed or not.

**Unresolved Not Safe Items:** This option allows the user to choose whether the WhitelistCloud system tray icon is displayed or not.

**Windows Firewall:** This option displays the current status of the Windows Defender Firewall and if clicked, opens the Windows Defender Firewall settings so the user can make necessary adjustments.

**Last Snapshot Scan:** This option displays the date and time of the most recent WhitelistCloud scan.

**Last Snapshot Scan Duration:** This option displays the duration of the most recent WhitelistCloud Scan.

**Enable / Disable WhitelistCloud Realtime Scan (Button):** This button will allow the user to enable or disable the WhitelistCloud Realtime Scan.

**Clear Firewall Rules (Button):** This button will remove all existing Windows Defender Firewall rules that were created by WhitelistCloud.

## **How WhitelistCloud Works**

Traditional antivirus scans for malicious files. WhitelistCloud scans for safe files.

WhitelistCloud is a new patent pending feature of VoodooShield that continuously monitors all running processes and ensures only Safe items are running at any given time. If you enable WhitelistCloud, an initial Snapshot Scan will be performed and should take less than 10 minutes. There are usually a handful of files that WhitelistCloud is unable to determine to be safe during the scan. So once the scan is complete, you can manually verify the files classified as Not Safe are safe or not. You will then be continually aware that only Safe files are running on your system at any given time, as indicated by the white colored WC icon at the bottom right, by the clock.

WhitelistCloud is essentially an advanced file reputation service that classifies files as either Safe or Not Safe and will usually encounter a handful of files that it is unable to determine as being Safe. When unknown files are encountered, you can inspect the file to ensure it is a known, Safe file that is supposed to be running on your system. Once all of the files are known to be Safe, you will then be constantly aware that only Safe files are running on your system at any given time. Remember, a Not Safe Scan Result does not necessarily indicate an item is malicious. Rather, the item is not known to be Safe.

WhitelistCloud also includes a unique firewall feature that automatically creates Window Defender Firewall rules for new items that are not known to be Safe. Once an item that is not well known but verified as Safe, the firewall rules are automatically removed. You can also create firewall rules for Safe items, simply by clicking the Inbound or Outbound checkboxes in the WhitelistCloud settings tab. This might be useful if you have a need to block internet access to a specific app for whatever reason. The WhitelistCloud options are highly flexible and you can configure WhitelistCloud and its firewall component to your liking.

## Web Management

**VoodooShield™**  
Virus Protection Like No Other

### Web Management

Threats Blocked: 0

- ☐ Require admin approval before letting the user allow new, non-whitelisted files (disables left click of VoodooShield)
  - ☐ Analyze items the user wants to allow with Cuckoo Sandbox and post an alert in the Management Console
- ☒ Require password to login to the Web Management Console
- ☐ Synchronize and backup my whitelist to the cloud
- ☐ Synchronize and backup my settings to the cloud

On-Premise Web Management Console

On-Premise Cuckoo Sandbox Server

☐ Use custom proxy settings

Proxy Server  Proxy Port  Proxy Type

Login to the Web Management Console Update Check Save & Close

The Web Management tab allows the user to connect the endpoint to a Web Management Console which enables administrators to remotely manage whitelists and settings on each endpoint.

**Require admin approval before letting the user allow new, non-whitelisted files (disables left click of VoodooShield):** When disabled (default), the user has the ability to allow new items to be whitelisted when prompted. System administrators might wish to enable this feature and add a password in the Utility tab to ensure the user does not add new items to the whitelist without permission.

**Analyze items the user wants to allow with Cuckoo Sandbox and post an alert in the Management Console:** When enabled, VoodooShield will store a backup copy of your whitelist to the cloud so that it can be transferred to other computers on your network, or restored at a later date.

**Require password to login to the Web Management Console:** When enabled, VoodooShield will store a backup copy of your whitelist to the cloud so that it can be transferred to other computers on your network, or restored at a later date.

**Synchronize and backup my whitelist to the cloud:** When enabled, VoodooShield will synchronize the endpoint whitelist with the Web Management Console so it can be remotely managed by administrators.

**Synchronize and backup my settings to the cloud:** When enabled, VoodooShield will synchronize the endpoint settings Web Management Console so it can be remotely managed by administrators.

**On-Premise Web Management Console:** This option will allow the user to configure an On-Premise Web Management Console.

**On-Premise Cuckoo Sandbox Server:** This option will allow the user to configure an On-Premise Cuckoo Sandbox Server.

**Use custom proxy settings:** If enabled, this option will allow the user to configure a custom proxy.

**Proxy Server:** This option will allow the user to configure the custom proxy server address

**Proxy Port:** This option will allow the user to configure the custom proxy port

**Proxy Type:** This option will allow the user to configure the custom proxy port type (HTTP, SSL, FTP, SOCKS v4 or SOCKS v5)

### **Other buttons:**

**Reset Whitelist (Button):** This button will reset the whitelist and take a whitelist snapshot of the currently running processes, automatically adding them to the whitelist.

**Update Check (Button):** This button will manually check to see if the latest version of VoodooShield is installed.

**Save & Close (Button):** This button will save any changes made in the settings window.

## **Proprietary / Special VoodooShield Features**

### **VoodooAi**

VoodooAi is integrated into VoodooShield Pro and utilizes machine learning and artificial intelligence to analyze files for maliciousness. The file is then classified as Safe, Suspicious or Unsafe, and a graph indicator showing the maliciousness is displayed.

In general...

**Safe:** If a file is determined by VoodooAi to be Safe, it is most likely safe to allow, assuming WhitelistCloud has determined the file to be Safe.

**Unsafe:** If a file is determined by VoodooAi to be Unsafe and determined to be Not Safe by WhitelistCloud, then the file should be blocked or quarantined.

**Suspicious:** If a file is determined by VoodooAi to be Suspicious, the user should rely on the WhitelistCloud result to make the determination whether the file is safe to allow or not.

While machine learning and artificial intelligence will never be perfect, VoodooAi is especially adept at detecting new, unknown and zero day threats, where traditional antivirus methods tend to fail.

### **Drag and drop to VoodooShield to scan a file**

The user can drag and drop a file to the VoodooShield Desktop Gadget to analyze the file with VoodooAi and WhitelistCloud.

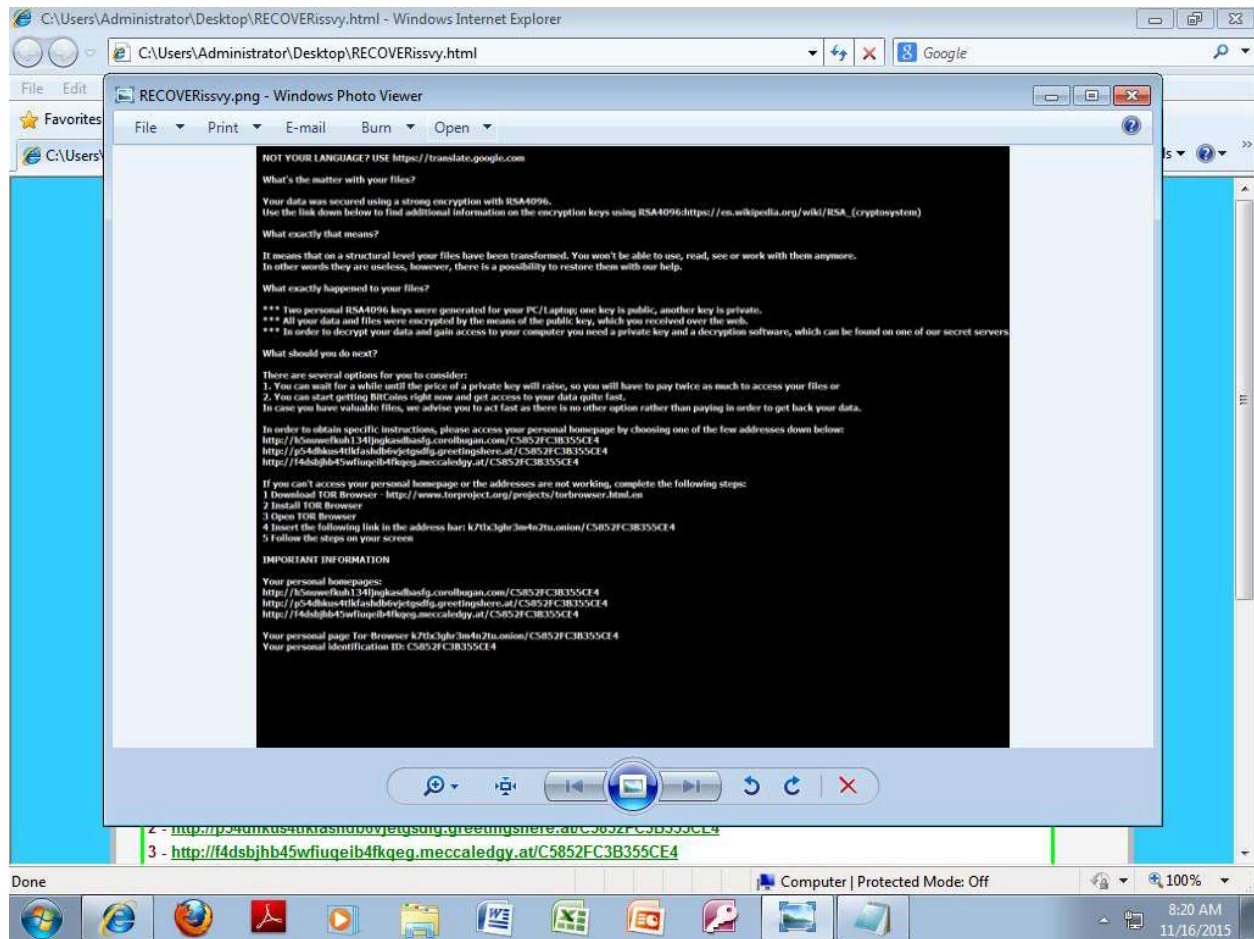
### **Local Sandbox**

Although the Cuckoo / Remote Sandbox is the preferred sandbox, VoodooShield also offers the ability for the user to execute a blocked file in a local sandbox, which runs the file with limited rights. Files that require administrator approval to perform certain tasks will typically fail in the local sandbox. But keep in mind, files that require administrator approval are capable of performing dangerous actions on the computer, so if a file fails in the local sandbox, there is a good chance that the user should not execute this file outside of the sandbox.



## Cuckoo / Remote Sandbox

VoodooShield also offers the ability for the user to execute a file in a remote sandbox, safely in a remote computer, and receiving a full detailed analysis of the file's execution, before deciding to run the file on their machine. The user also has the ability to watch the Cuckoo Sandbox analysis in real-time, in a Remote Desktop session, which allows the user to see first-hand the implications of running the blocked file, safely, on a remote machine before they choose to allow the file, as demonstrated in the ransomware sample below.



In order to view the Cuckoo Sandbox analysis in real-time, please ensure that the “Watch Cuckoo Sandbox analysis in a Remote Desktop session in real-time” option is checked in the full user prompt.