

RANSOMWARE DEFENDER

User Manual



**RANSOMWARE
DEFENDER**

Ransomware Defender Operation Manual
ShieldApps Software Innovations.
All Rights Reserved 2012 - 2017



Table of Contents

Welcome.....	3
Compatibility.....	3
Installation Guide.....	5
Registration.....	6
Overview.....	7
Scan.....	8
Manage.....	13
History.....	14
Quarantine.....	15
Always Allowed.....	16
Schedule Scans.....	17
Ransomware Defender Updates.....	19
System Tools.....	20
History Cleaner.....	21
Secure File Eraser.....	22
Start-Up Manager.....	23
Settings.....	24
General.....	24
Scan Options.....	25
Uninstall.....	27
Help & Support.....	28

Welcome to ShieldApps' Ransomware Defender

This guide is devised to lead you through the installation process and general usage of the software. ShieldApps' **Ransomware Defender**, is designed for detecting and blocking ransomware prior to any damage. The software proactively stands guard to detect threats and works alongside all main antiviruses and anti-malware products.

Compatibility

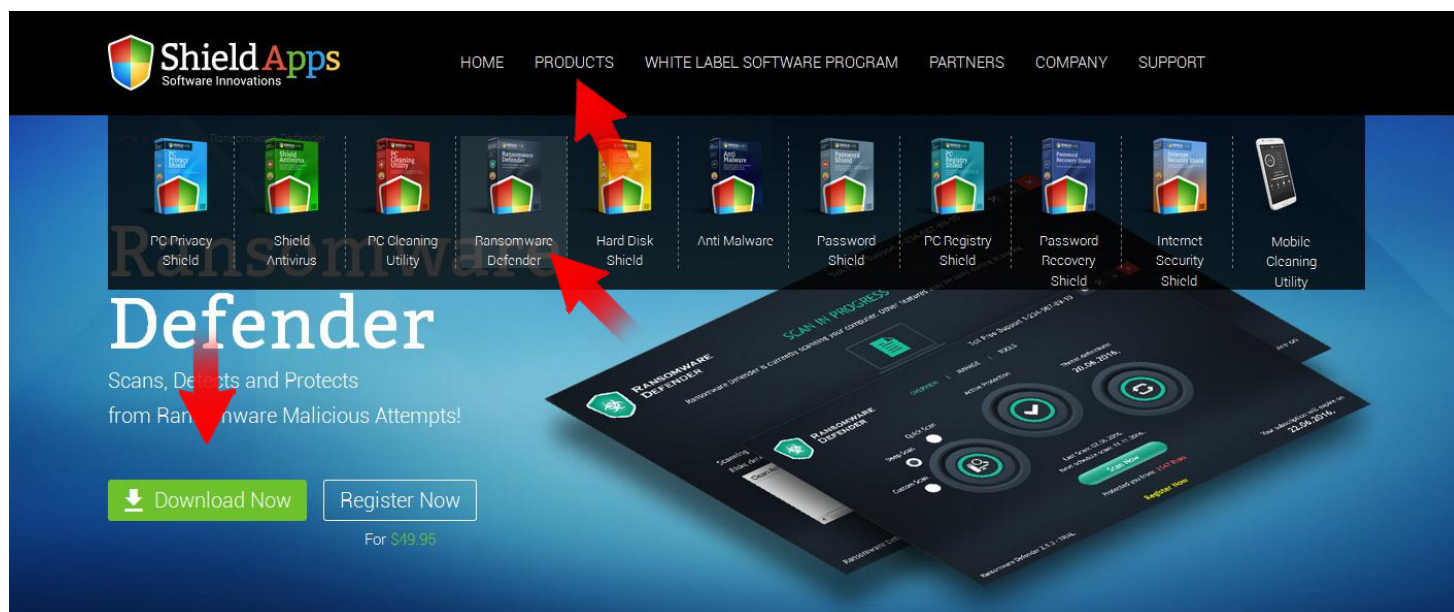
Ransomware Defender supports Windows versions:



Installation Guide

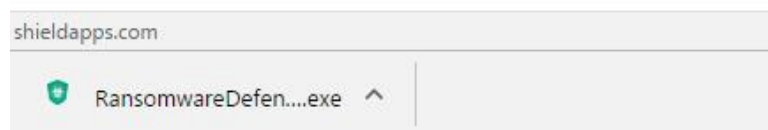
To obtain your copy of Ransomware Defender, please follow the steps below:

- ✓ Go to ShieldApps.com
- ✓ Under the **"Products"** menu, choose Ransomware Defender
- ✓ Click the **"Download Now"** button and save the product on your computer



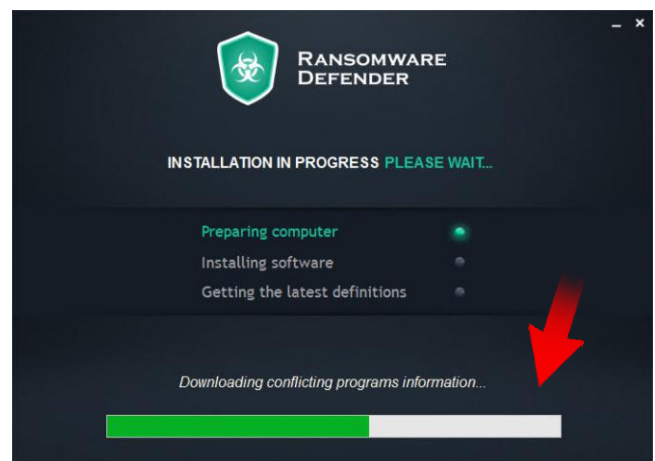
Installation Guide

To initiate the installation process,
double-click the downloaded file icon.
Ransomware Defender's installation process will start promptly.



Please note: before you confirm the installation process,
we urge you to read product's terms and conditions ("**End User License Agreement**")
by clicking on the relevant link, as shown below.


The installation process includes a vast ransomware database download,
and thus takes a while. Once downloaded Ransomware Defender's database will be
up to date and provide maximum protection.





Once all the files are downloaded and unpacked, Ransomware Defender will launch automatically, and an installation confirmation page will open to confirm a successful installation.



SHIELD APPS
Software Innovations

HOMEPRODUCTSWHITE LABEL SOFTWARE PROGRAMPARTNERSCOMPANYSUPPORT

Home > post install > Ransomware Defender successful installation

Ransomware Defender successful installation

How does Ransomware Defender Work?

Ransomware Defender is designed for simplicity and ease of use.

All you need to do is run the application, let it scan your PC for all threats, and then click "Clean Now" to eliminate all found issues and threats – **That's it!**

1




Scan for Threats – With a fast and advanced scan algorithm, Ransomware Defender scans the entire system with hardly any effect on CPU resources and speed. Use "Quick Scan" for a faster, more common search process.

2

Let the Scan Run – A Quick Scan should take a couple of minutes. If you choose deeper scans, it might take several minutes – let the scan run its course till it's finished.

3

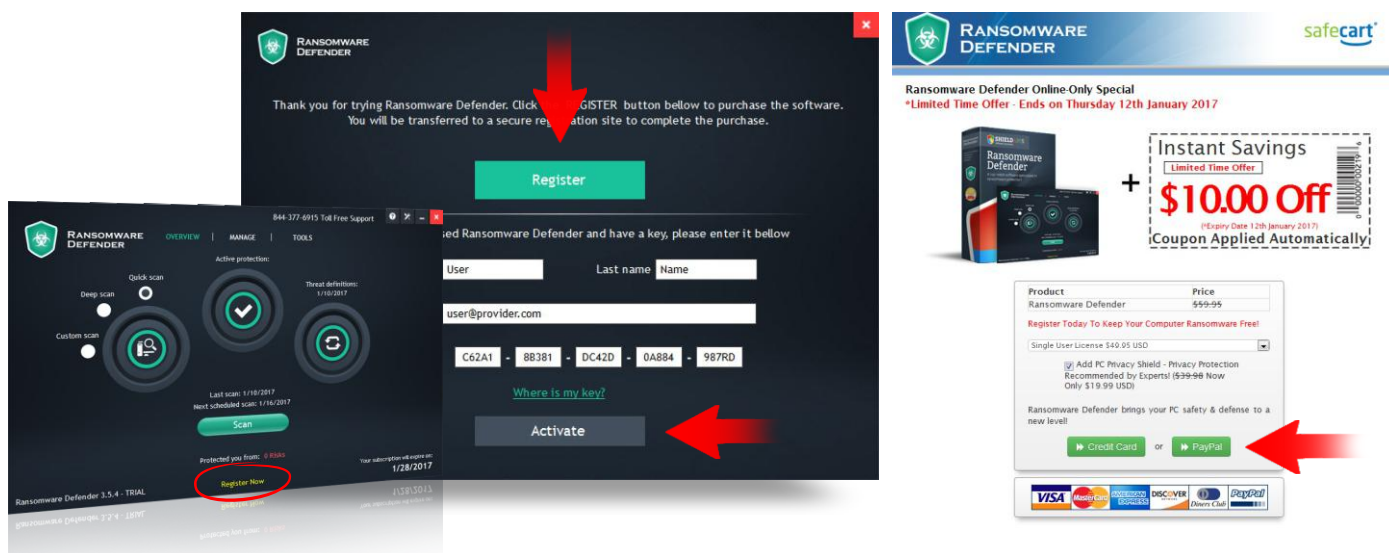
Review the Scan Results and Delete the Threats! – Review all threats found by the Scan and either manually choose which ones to delete, or simply Clean All as suggested by the Recommended Action button.





Registration

Ransomware Defender features a fully functional 30 days trial. To upgrade to a premium account, and enjoy Ransomware Defender's protection further, click the **"Register Now"** button at the bottom of the screen.



If you have already registered your copy:

- ✓ Enter your full name
- ✓ Enter the email address you have used to register your Ransomware Defender
- ✓ Copy and paste* your key in to the activation box
- ✓ Click **"Activate"**

To register your software copy and upgrade to a fully featured premium version:

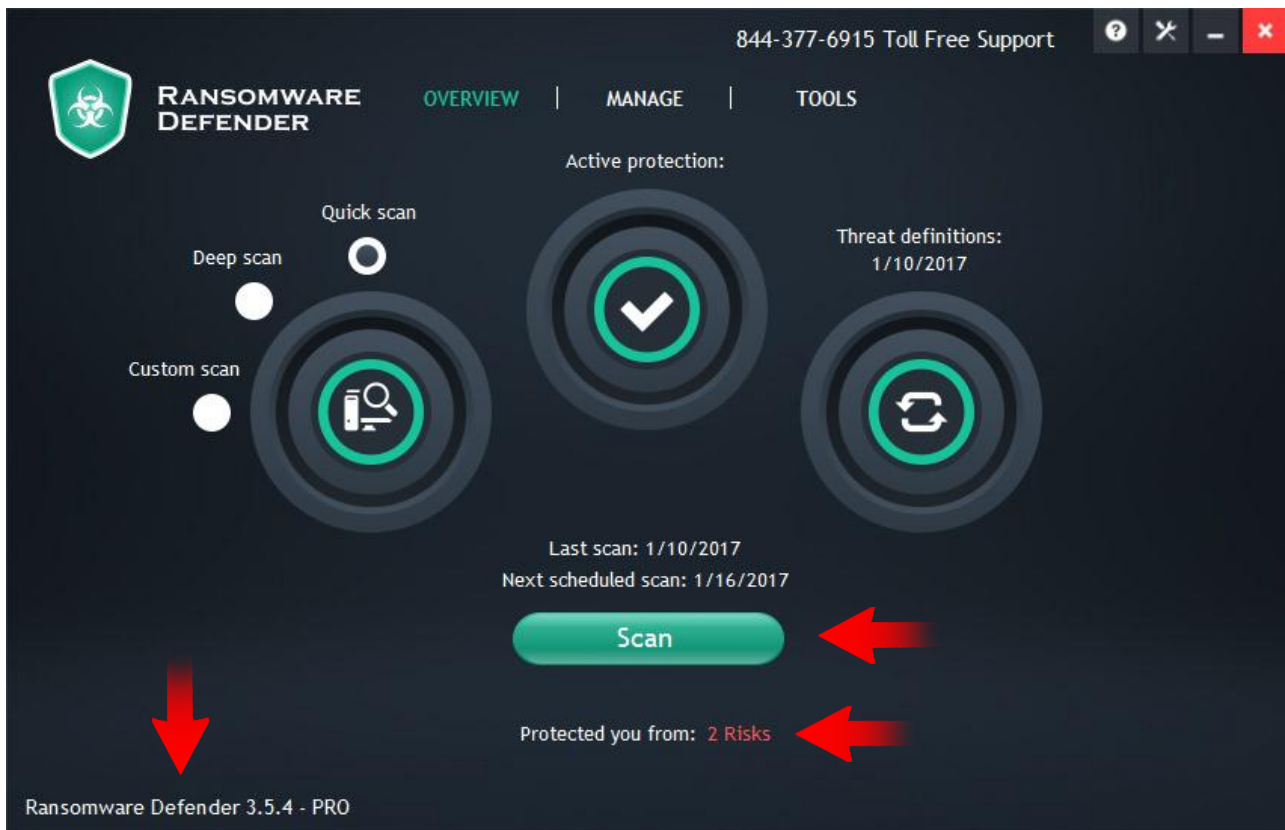
- ✓ Click the **"Register"** button
- ✓ Follow the registration process prompts
- ✓ Upon successful registration, a license key will be delivered to your email address
- ✓ Enter your full name
- ✓ Enter the email address you have used to register your Ransomware Defender
- ✓ Copy and paste it to the activation box
- ✓ Click **"Activate"**

*Hover over the license key with holding left-click to highlight it. Click right-click and select **"Copy"**. Go back to the registration box, right-click, choose **"Paste"** from the menu.

Overview

The Overview page displays the main information needed for the every-day use of Ransomware Defender.

Everything from a basic scan, the software version, the number of threats detected and prevented infections will be displayed here.

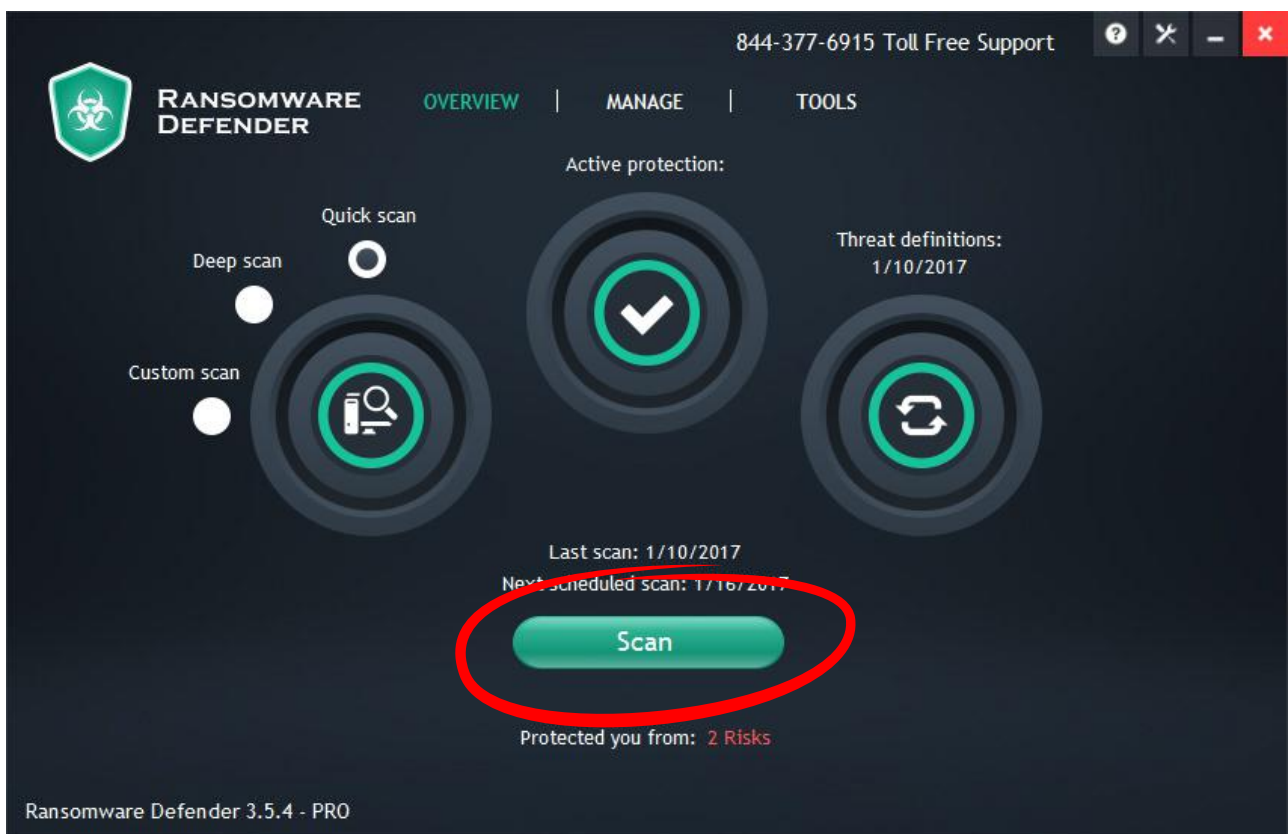


The **“Scan”** button in the overview window will start a scan when clicked.

On the left side of the overview window different scan types are placed.

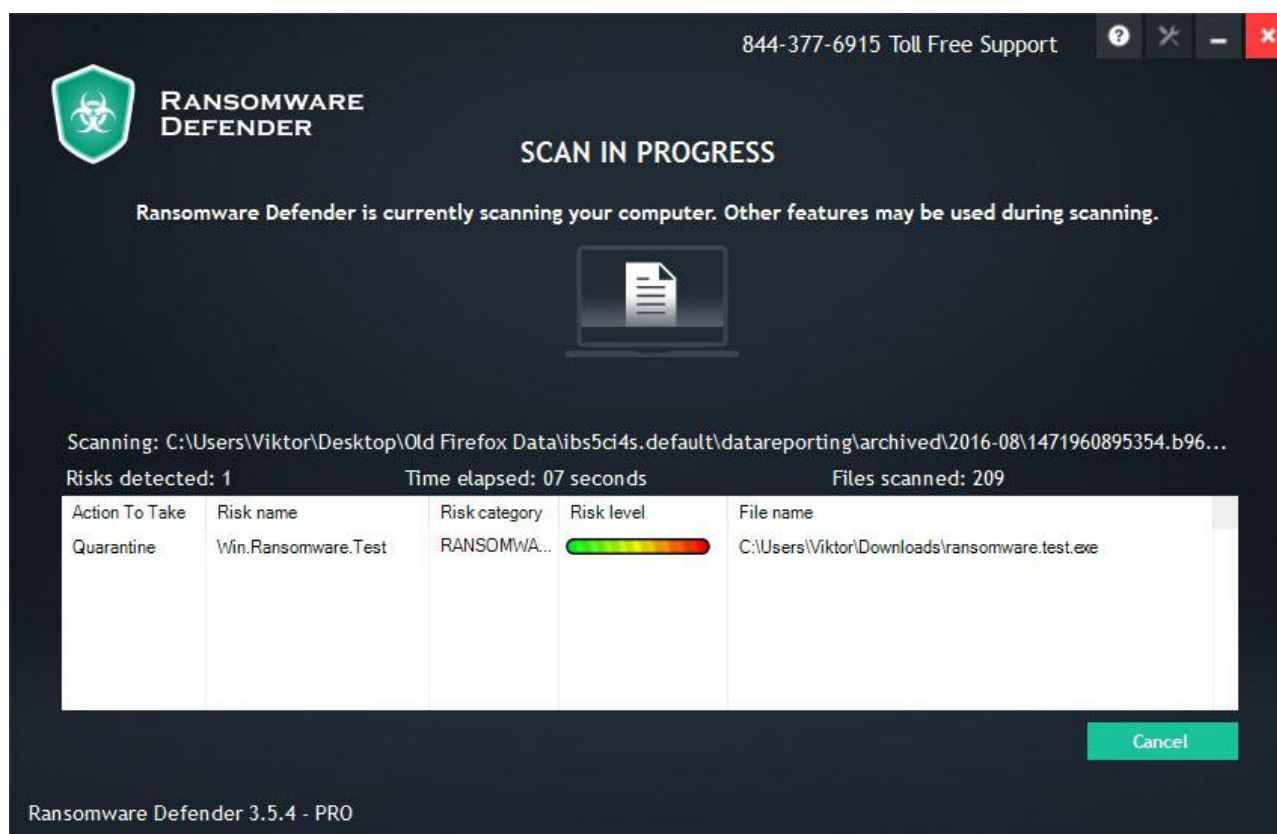
Pick either:

- ✓ **“Quick Scan”**
- ✓ **“Deep Scan”**
- ✓ **“Custom Scan”**



Quick Scan

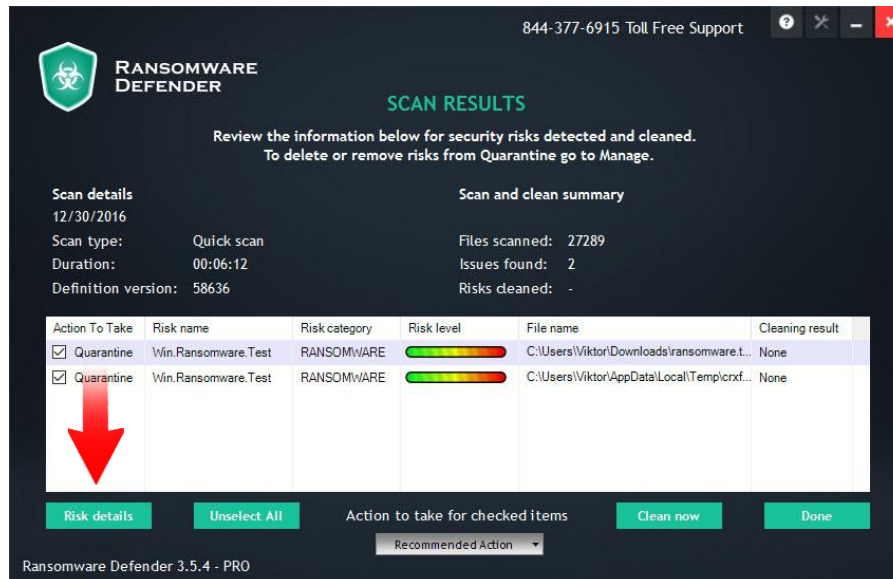
This scan will run through the system, and look for ransomware. It takes just a few minutes before a full report to display with relevant concerns and suggested actions.



Once the scan is complete, a full list of threats, their name, risk level and location on the computer will be displayed.

To see details for any of the found threats:

- ✓ Click on a threat
- ✓ Click **“Risk Details”**

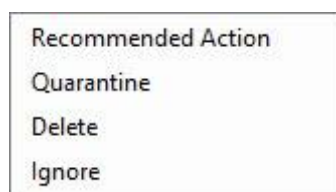


Malicious software designed to restrict computer system access to the user. In order lift the restriction, one must pay to the hacker which created the ransomware. Some ransomware simply locks the system, while other can encrypt files on the hard drive.

Cleaning methods are placed below. By default, if **“Clean Now”** button is pressed a recommended action is taken.

To change the default settings:

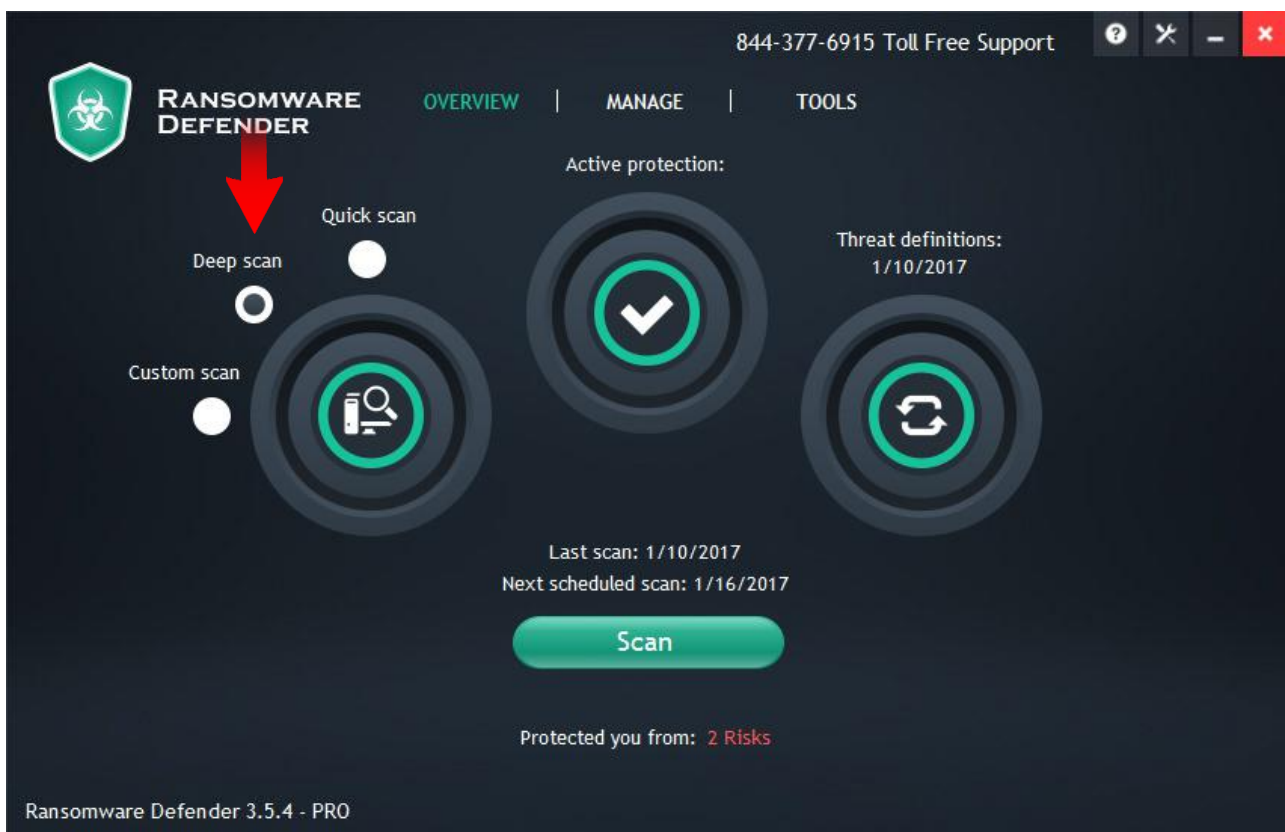
- ✓ Click on the drop-down menu
- ✓ Choose between: **“Recommended Action”**, **“Quarantine”**, **“Disinfect”**, **“Delete”** and **“Ignore”**.



Pick an action and click **“Done”**. The software will return to the Overview page.

Deep Scan

This option provides a deeper, more thorough scan of the system. Thanks to advanced algorithms, the software is able to look into deeper levels for possible dormant threats. This scan takes a bit longer, as each level of folders includes thousands of files to be scanned. Once the scan is complete, the results and actions will appear.

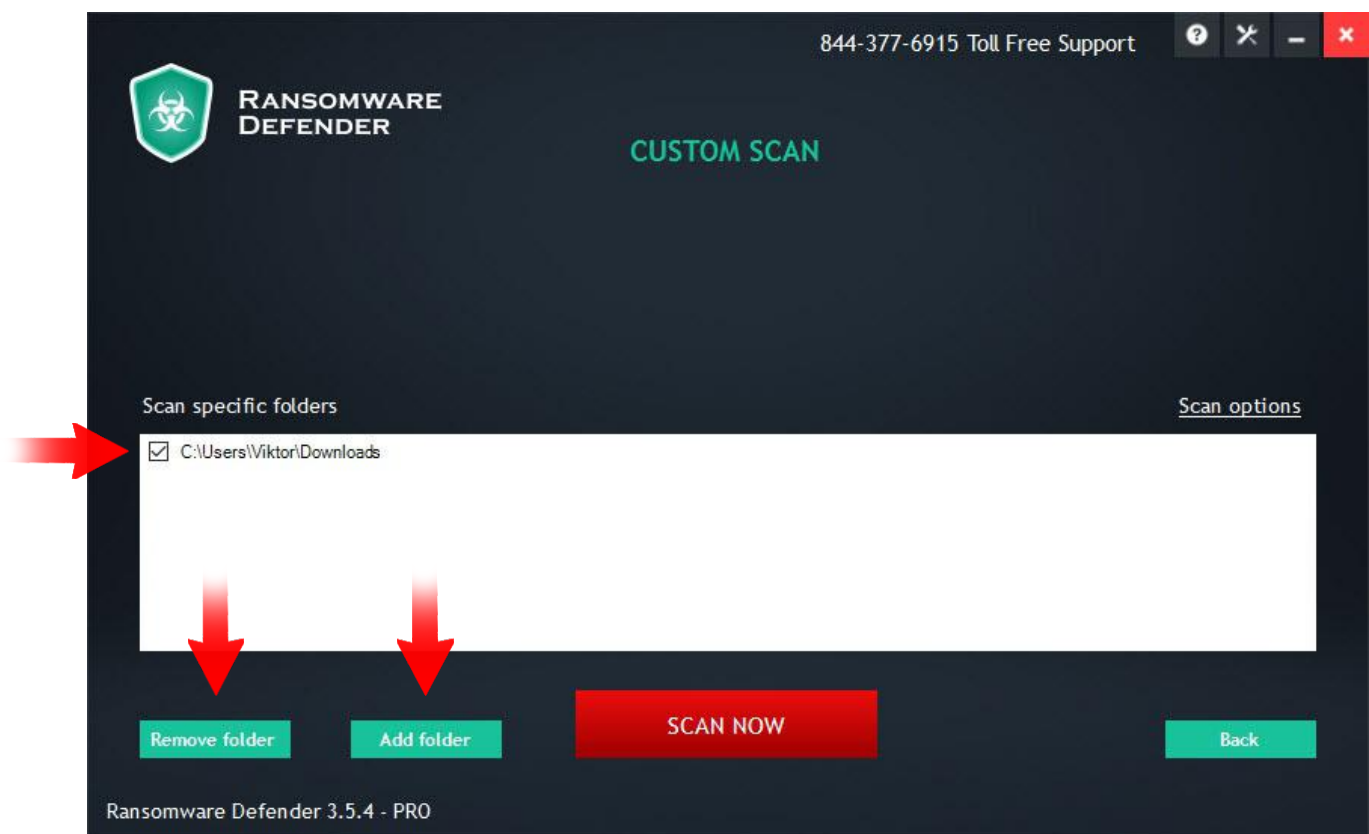


Custom Scan

This option is devised for special scans. If some file or folder are suspected to be infected, click **“Add Folder”** and that specific folder will be scanned for threats.

To create a custom scan:

- ✓ Click **“Add Folder”**
- ✓ Choose a folder
- ✓ Pick an action



There's no limitation on a number of files and folders that can be added. To remove a folder from the list, check the box next to its name, and click **“Remove Folder”**.

The Manage tab provides additional tools and information. Each feature has its own page and settings.



Manage tab contains:

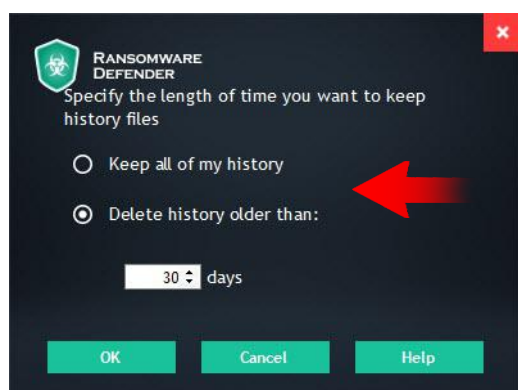
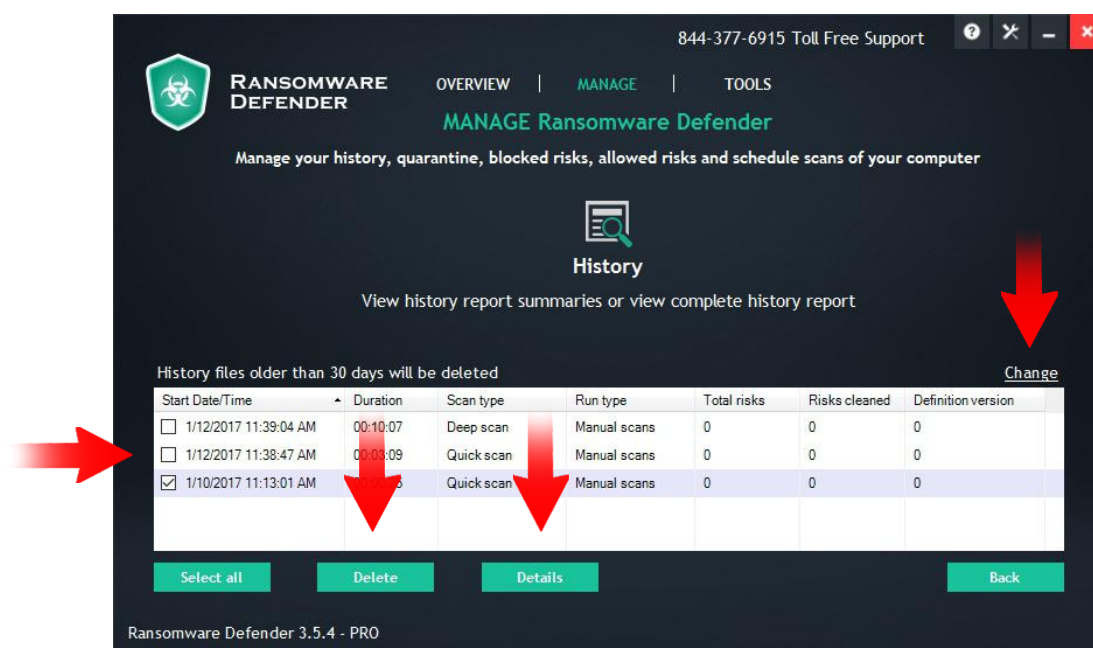
- ✓ "History"
- ✓ "Quarantine"
- ✓ "Always Allowed"
- ✓ "Scheduled Scans"
- ✓ "Ransomware Defender Updates"

History

This feature contains information about the history of scans and cleaning actions. To check the details of any scan, click on the **“Details”** button.

Each history log can be manually removed:

- ✓ Check the box next to the log
- ✓ Click the **“Delete”** button



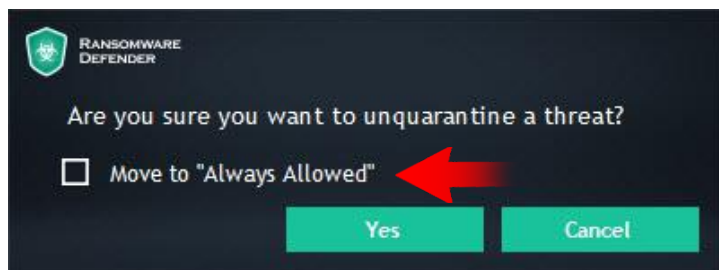
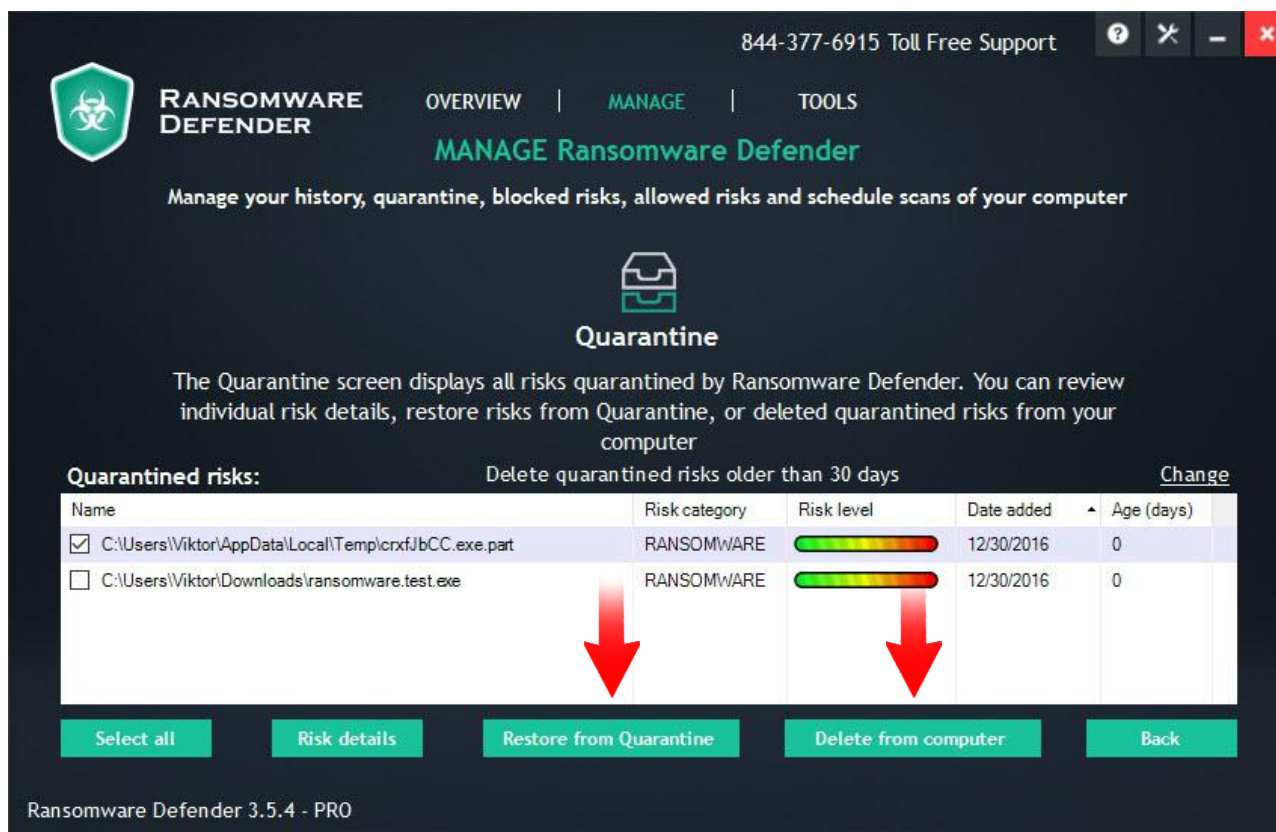
To automate this operation:

- ✓ Click **“Change”** (right side of the list)
- ✓ Choose to keep the entire history or remove anything older than specified number of days

Quarantine

This feature holds the information about every malicious file that has been in the quarantine.

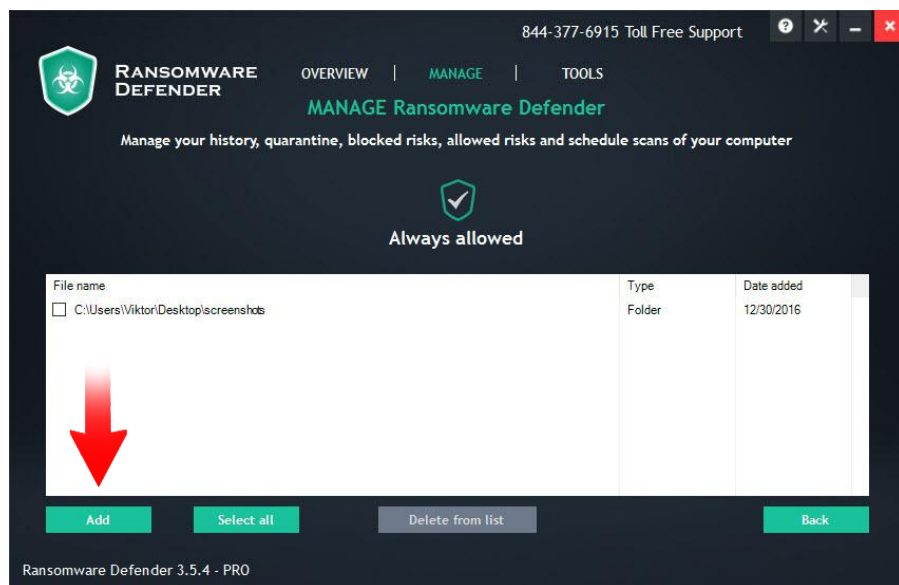
To remove it permanently, click **“Delete From Computer”**, to put it back to use click **“Restore From Quarantine”**.



When threats are restored, the software seeks action confirmation. Also, the software will offer to place the file inside the **“Always Allowed”** section.

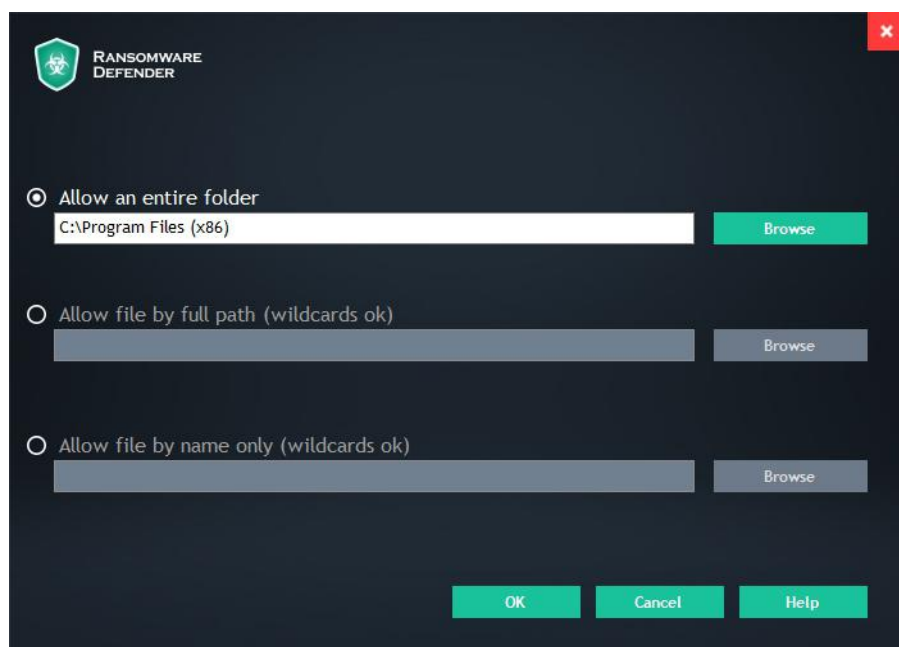
Always Allowed

This section is used to list pre-approved files and prevent their scanning and detection by Anti Malware's engine.



To exclude files from being scanned:

- ✓ Click **"Add"** button
- ✓ Find the file's location
- ✓ Confirm



There is no limit to the list and files can be added or removed at all times.

Schedule Scans

This feature allows the software to be fully automated. Numerous schedules can be created with the precisely defined time, date and type of scan.


844-377-6915 Toll Free Support

RANSOMWARE DEFENDER

OVERVIEW | **MANAGE** | TOOLS

MANAGE Ransomware Defender

Manage your history, quarantine, blocked risks, allowed risks and schedule scans of your computer



Schedule scans

Configure and schedule automated scans

Scheduled scans [Scan options](#)

Type	Status	Time	Days
<input checked="" type="checkbox"/> Deep scan	Enabled	6:27 AM	Monday

Delete

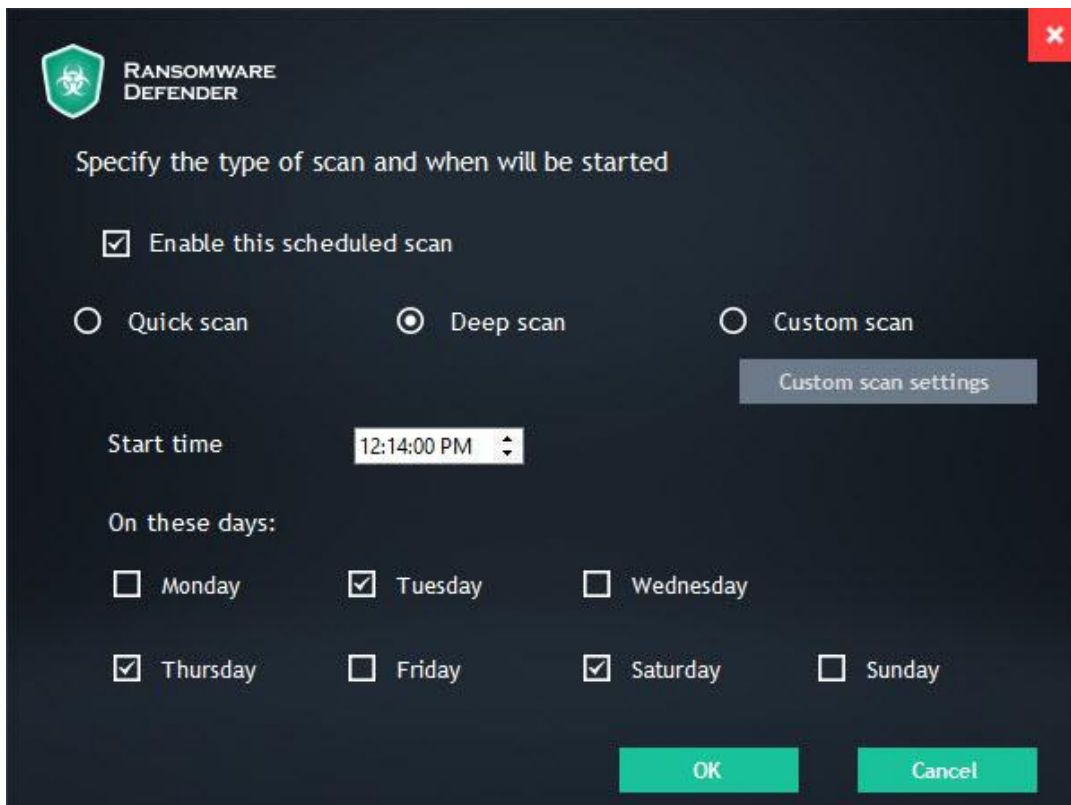
Select all Enable/Disable **Delete** Edit... Add new Back

Ransomware Defender 3.5.4 - PRO

Multiple schedules are available. While the **"Delete"** button removes every scheduled scan which has a checked box.

To create a scheduled scan/clean:

- ✓ Click **"Add New"**
- ✓ Set the time of the scan
- ✓ Pick a type of scan



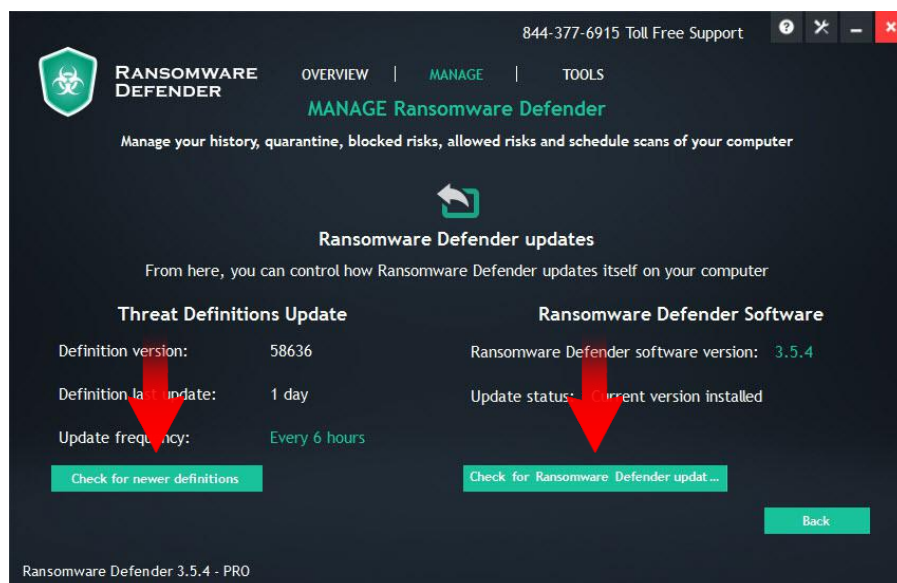
The screenshot shows a dark-themed dialog box titled "RANSOMWARE DEFENDER" with a biohazard icon. The main heading is "Specify the type of scan and when will be started". It includes a checkbox for "Enable this scheduled scan" which is checked. Below this are three radio button options: "Quick scan", "Deep scan" (which is selected), and "Custom scan". A "Custom scan settings" button is visible next to the "Custom scan" option. The "Start time" is set to "12:14:00 PM" in a time picker. Under "On these days:", there are checkboxes for each day of the week: Monday (unchecked), Tuesday (checked), Wednesday (unchecked), Thursday (checked), Friday (unchecked), Saturday (checked), and Sunday (unchecked). At the bottom right are "OK" and "Cancel" buttons.

Ransomware Defender Updates

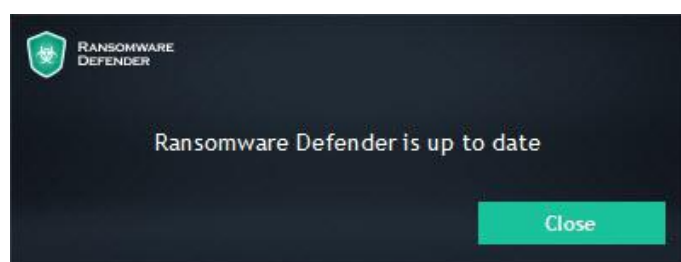
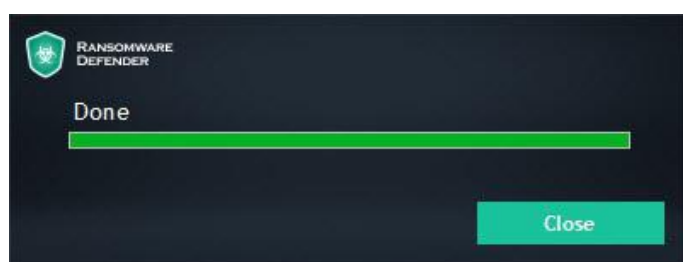
By default, Ransomware Defender is set to update everything automatically.

To check for updates manually:

- ✓ Click “Check For Ransomware Defender Updates”
- ✓ Click “Check For Newer Definitions”

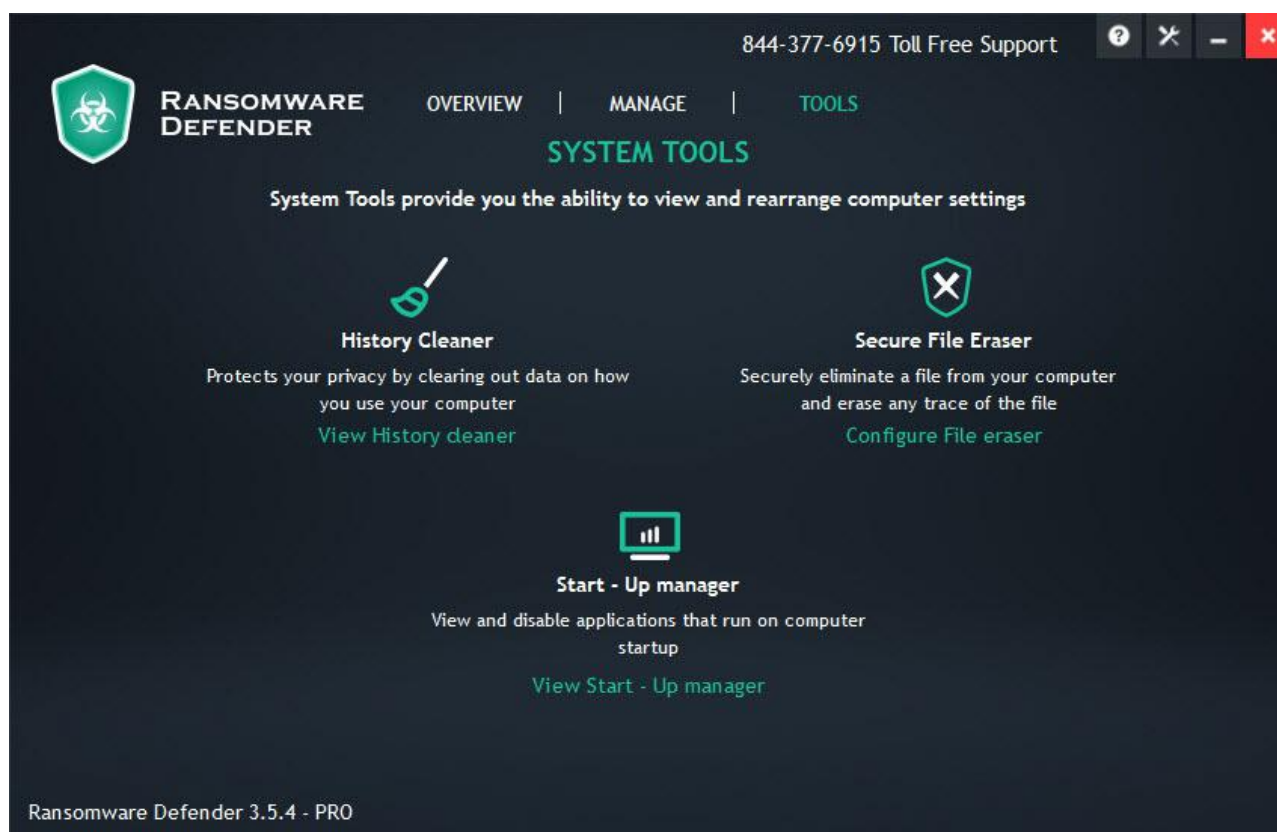


The page also displays detailed information about the current version of both the software and threats database installed on the computer.



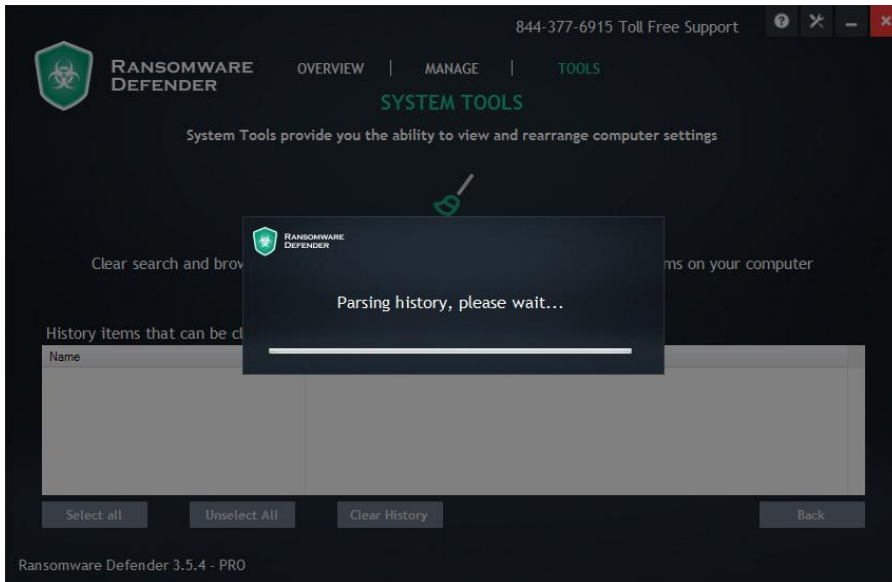
If there are software or threat database updates, their download and installation will begin instantly. If not, the software will display an up-to-date confirmation.

Ransomware Defender can be used for more than just virus protection. The additional tools can improve privacy, PC's performance and support proper hard drive maintenance.

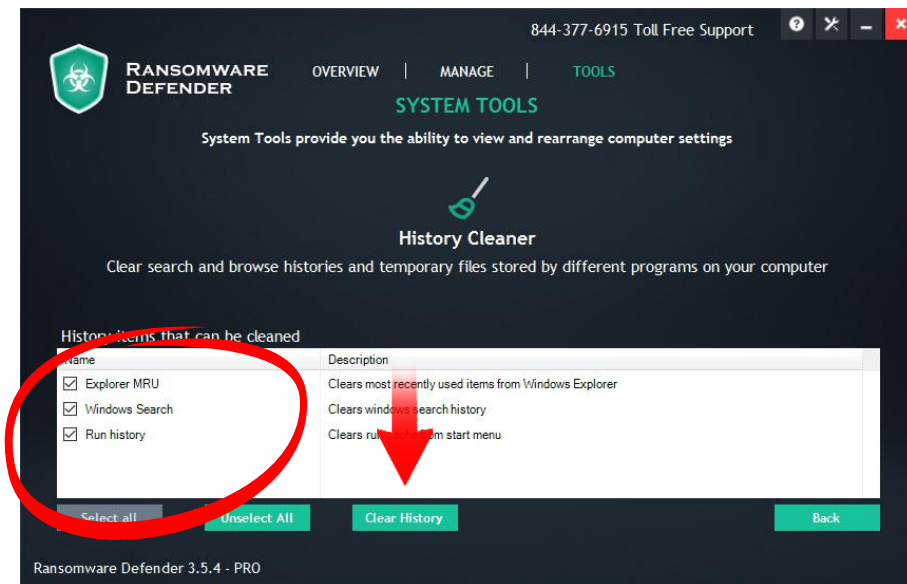


History Cleaner

This tool searches through the usage records of your browser, allowing its complete removal.



At the same time, the software looks for temporary files created by an application on the system and supports its deletion as well.



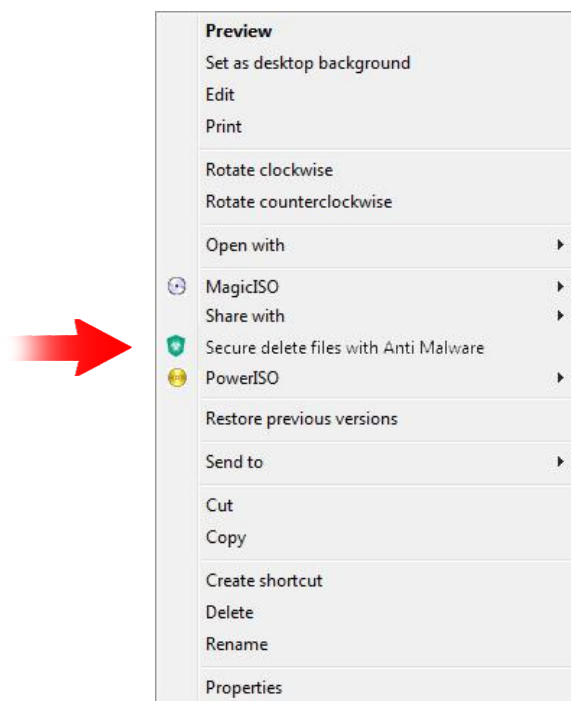
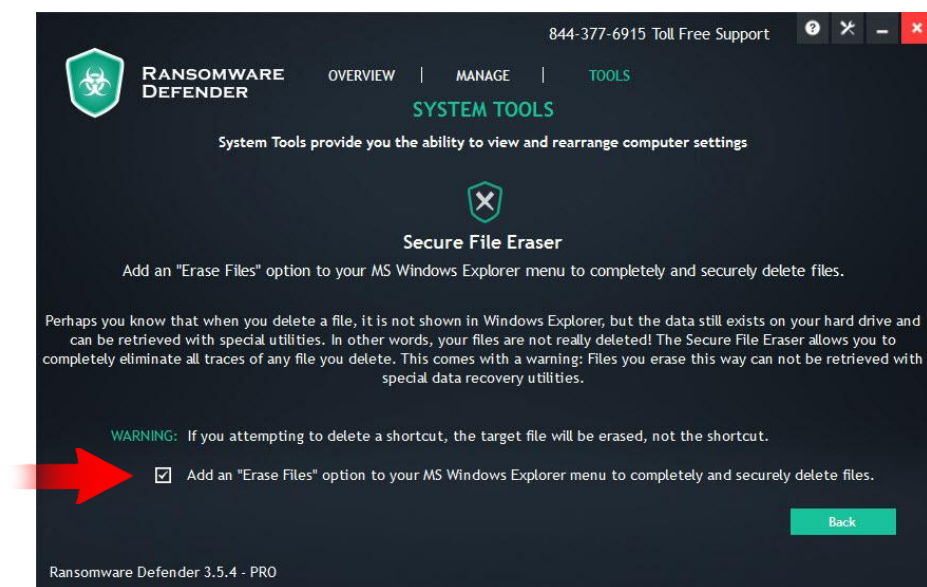
To remove potential privacy concerns and junk files from the hard drive, click **"Clear History"**. Check the box next to the name of the history/program if you wish to selectively delete specific items.

Secure File Eraser

This tool adds a right-click item to your standard right-click menu that allows safe deletion of files on your computer.

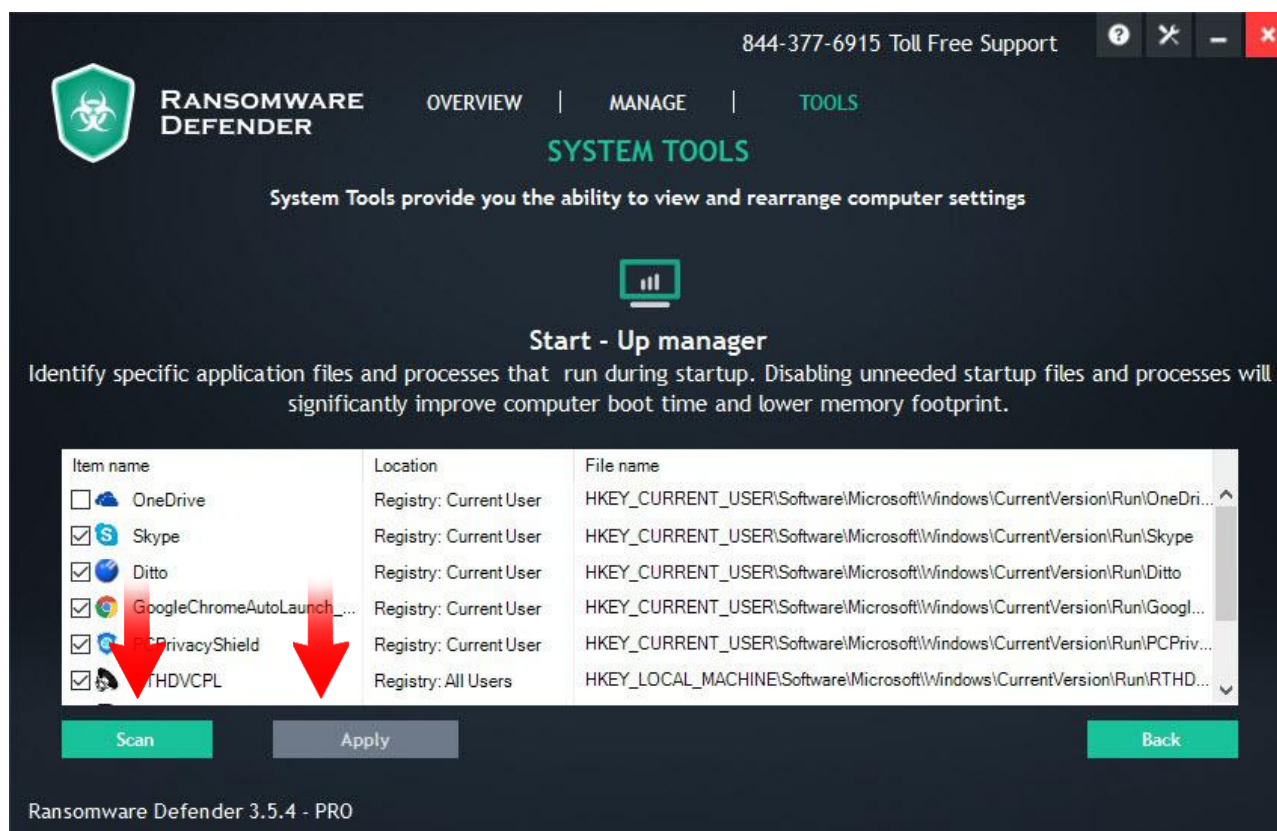
To turn on this tool:

- ✓ Check **“Add an Erase File”** box
- ✓ A new option will be added to the right-click menu



Start-Up Manger

This tool allows you to control which programs are launched by default upon reboot/startup of your computer. Some software automatically add themselves to the startup sequence and make it slower and more time consuming, so removing those from the startup process will speed up boot time.



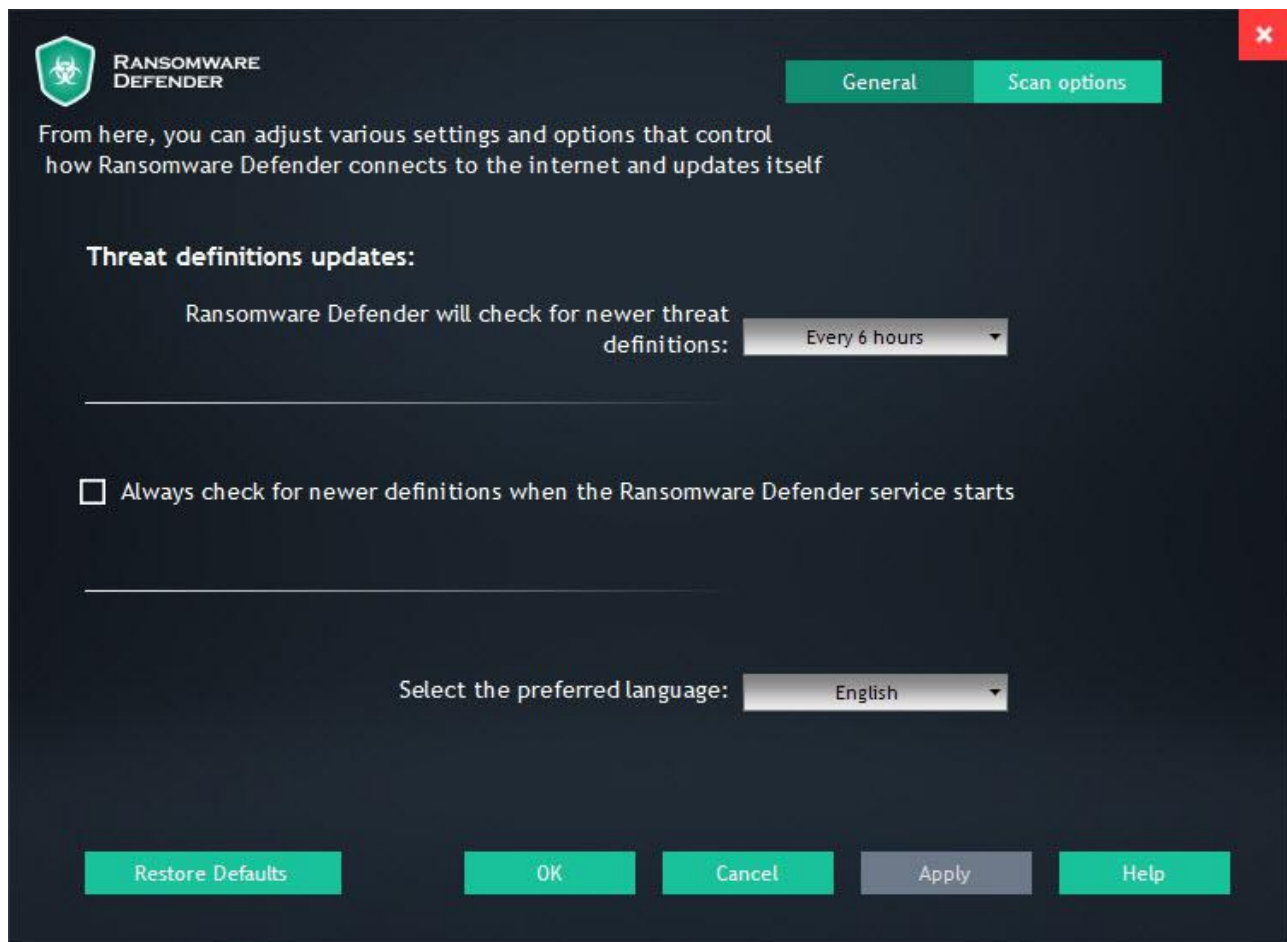
To pick which software will start alongside with the system:

- ✓ Click **"Scan"**
- ✓ Check the boxes of the applications you do want launched upon reboot, and uncheck the ones you want excluded
- ✓ Click **"Apply"**

Each of the software's option can be tweaked, changed or adjusted from within the settings menu. Some additional tools are also available in this menu.

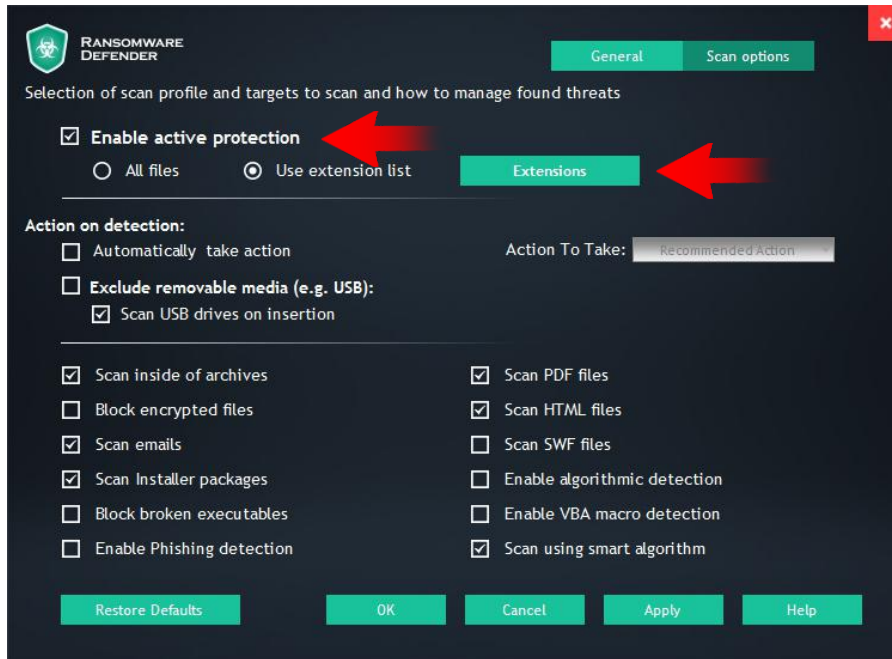
General

Standard settings, definitions update and language (11 different) are adjusted here.

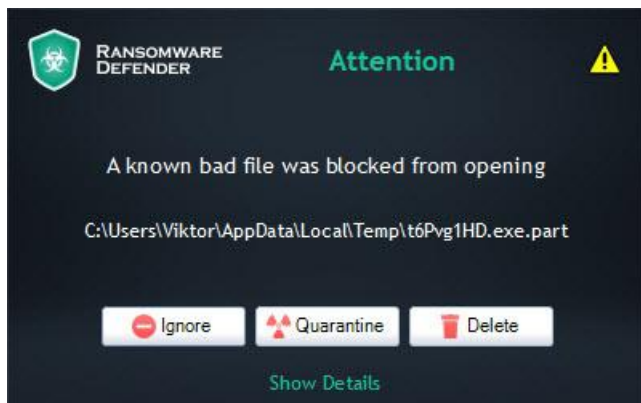


Scan Options

This tab contains the ransomware scan settings and preferences. Scan areas, type of files and extensions that are scanned are all defined in this tab.



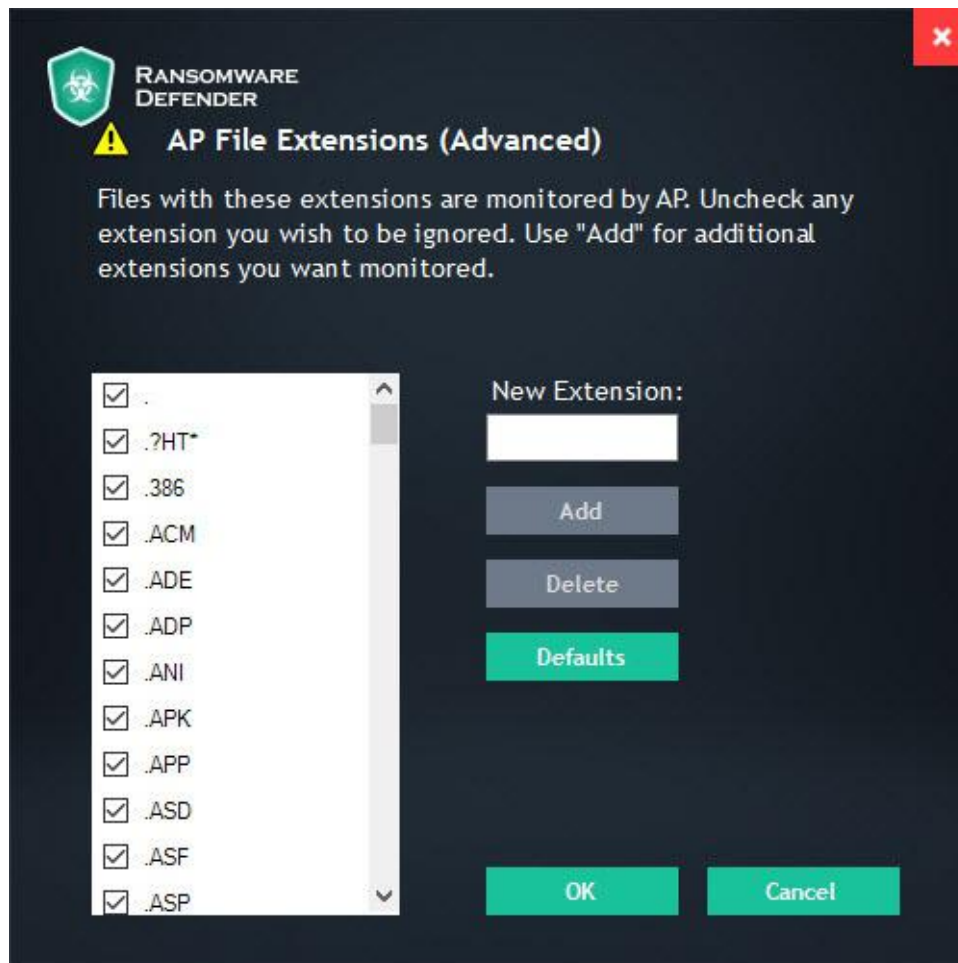
Active protection allows real-time notifications in a form of a prompt window every time a new threat is found.



Once the threat is found the software offers a few options:

- ✓ "Delete"
- ✓ "Quarantine"
- ✓ "Ignore"

Active protection can be standard for all the files on the computer, but it can also be specified for the type of files which will be closely monitored.

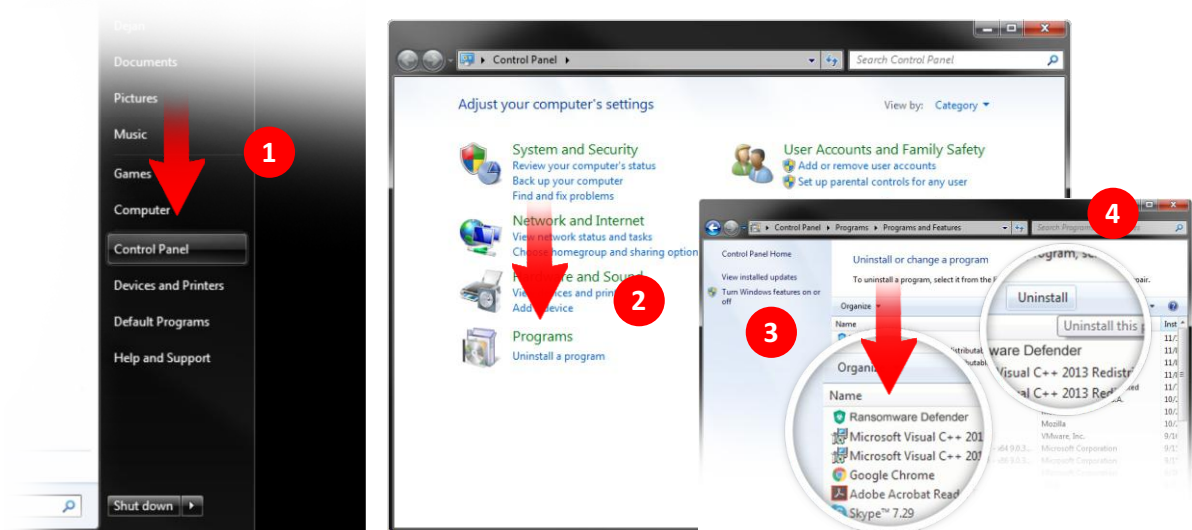


To extend or reduce the list of files that are scanned:

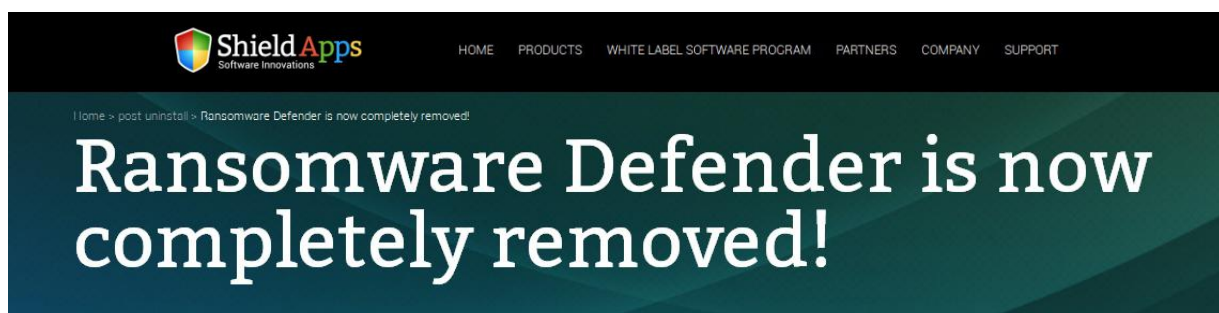
- ✓ Check **"Use Extension List"**
- ✓ Open **"Extensions"** menu
- ✓ Check on/uncheck extensions for scanning

To remove the software from the PC:

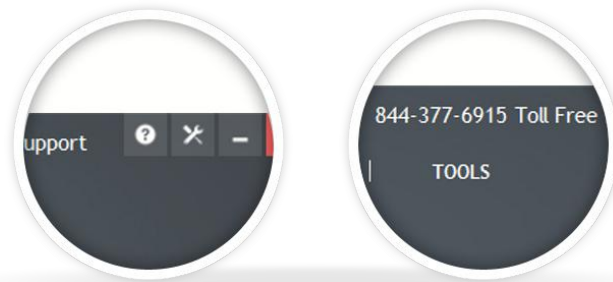
- 1 Go to Windows Control Panel
- 2 Locate **"Programs" – "Uninstall a Program"**
- 3 Locate Ransomware Defender
- 4 Click **"Uninstall"**



Once the uninstall is complete a confirmation page will open.



If there's anything our team can help you with or there is something you don't understand, you can always click the **"Help"** button. It will instantly take you to our FAQ page where you can look up anything that might be confusing you. If this doesn't help, you can contact us 24/7 through our email center on the support page, or by calling us directly using the number in the software.



[HOME](#) [PRODUCTS](#) [WHITE LABEL SOFTWARE PROGRAM](#) [PARTNERS](#) [COMPANY](#) [SUPPORT](#)

[Home](#) > [Support](#) > [Ransomware Defender Support](#)

Ransomware Defender Support

Please browse the frequently asked questions below. If you do not find the answer to your question - please contact us via the form below.

Installing Ransomware Defender

To properly install Ransomware Defender please follow the steps below.

1. Download Ransomware Defender. If prompted by the browser, click on the download confirmation.
2. After the download is complete, click on the downloaded file shortcut.
3. Confirm the installation process by clicking on the "Yes" button.
4. Click on the "Install" button and let the installation process run its course.
5. After Ransomware Defender installs on your computer, the program will open after it finishes loading.
6. You are all DONE! Ransomware Defender will stand guard against all ransomware attempts.

Uninstalling Ransomware Defender

