# How To Remove Ransomware From Windows OS?

## Detailed Instructions To Remove Ransomware From Windows OS.

## Method 1: Remove Ransomware and its associated files from computer through safe mode with command prompt.

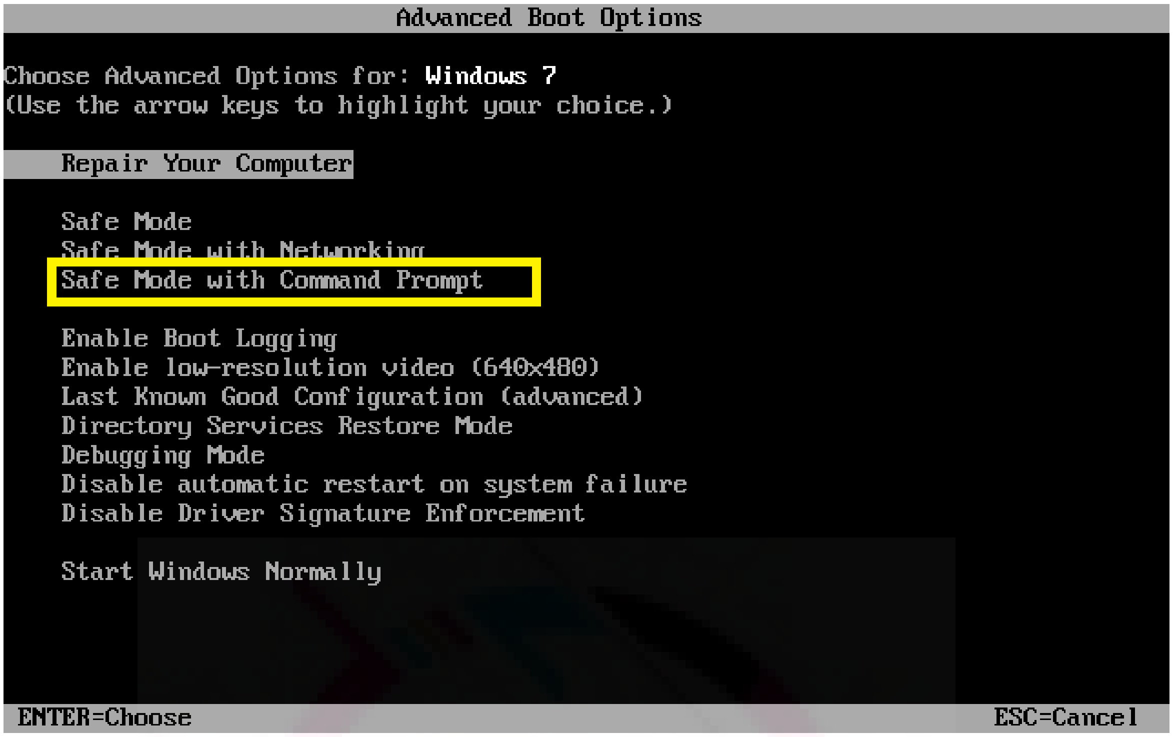
1. Reboot your computer to “Safe Mode with Command Prompt”
2. End malicious process from “Task Manager”
3. Deleting “Registry Entries” created by the Ransomware threat
4. Deep Scan the infected computer to ensure complete removal (Recommended)

## Method 2: Remove Ransomware virus using System Restore Procedure

After that the ransomware threat should may gone, but if it is still there, then you need to try the another method which is the “system Restore”.

## 1.1 Reboot your Windows 7/Vista/XP to “Safe Mode with Command Prompt”

1. Click on the Start menu, then on click the arrow next to “Shut Down.” Select Restart. (Just as you normally Restart your PC).
2. Once the computer screen is powered on, immediately start tapping “F8” key till you see “Advanced Boot Options” screen. if you don’t enter to the boot screen, then restart the process again and press F8 while the PC is restarting.
3. Here, you need to choose Safe Mode with Command Prompt option and press “enter” key to troubleshooting windows. As later on, you need to access the internet.
4. Once you choose the Safe Mode with Command Prompt option wait for the system to load necessary system files.



```
                    Advanced Boot Options

Choose Advanced Options for: Windows 7
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

ENTER=Choose                                      ESC=Cancel
```

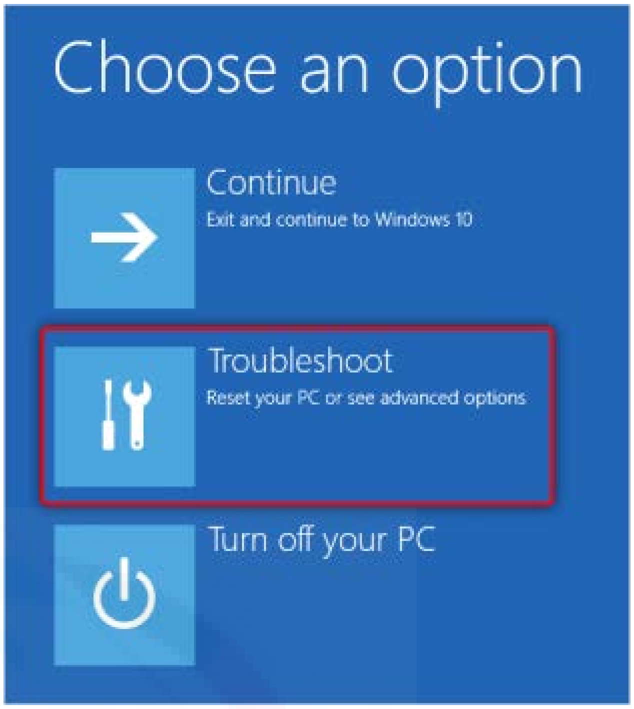
Window 7 Safe Mode Command Prompt

5. And you will now see the login screen. Now log in with your Administrator Account.

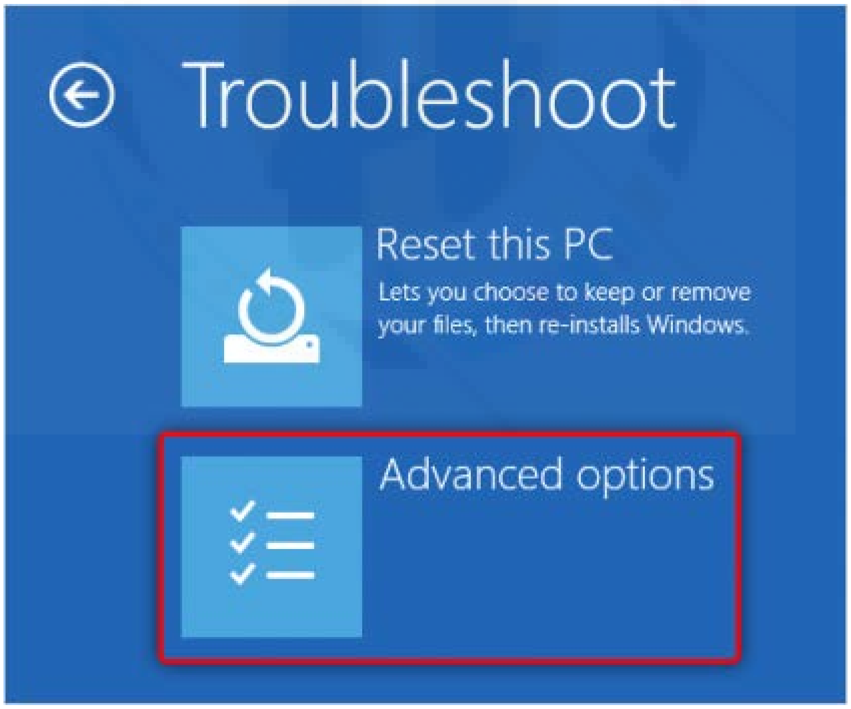
NOTE: To get back to your normal windows configuration, you need to repeat steps 1-3 and select Start Windows Normally.

## 1.1 Reboot your Windows 10, 8/8.1 - "Safe Mode with Command Pro mpt"

1. For Windows 10: Click Start → Power and then hold the Shift key on your keyboard and click Restart.
2. For Windows 8/8.1: Press the “Windows key + C“, and then click “Settings“. Click “Power“, hold down the Shift key on your keyboard and then click “Restart“.
3. From here steps are same for Windows 10 and 8.
4. Click Troubleshoot.
5. Click Advanced options.

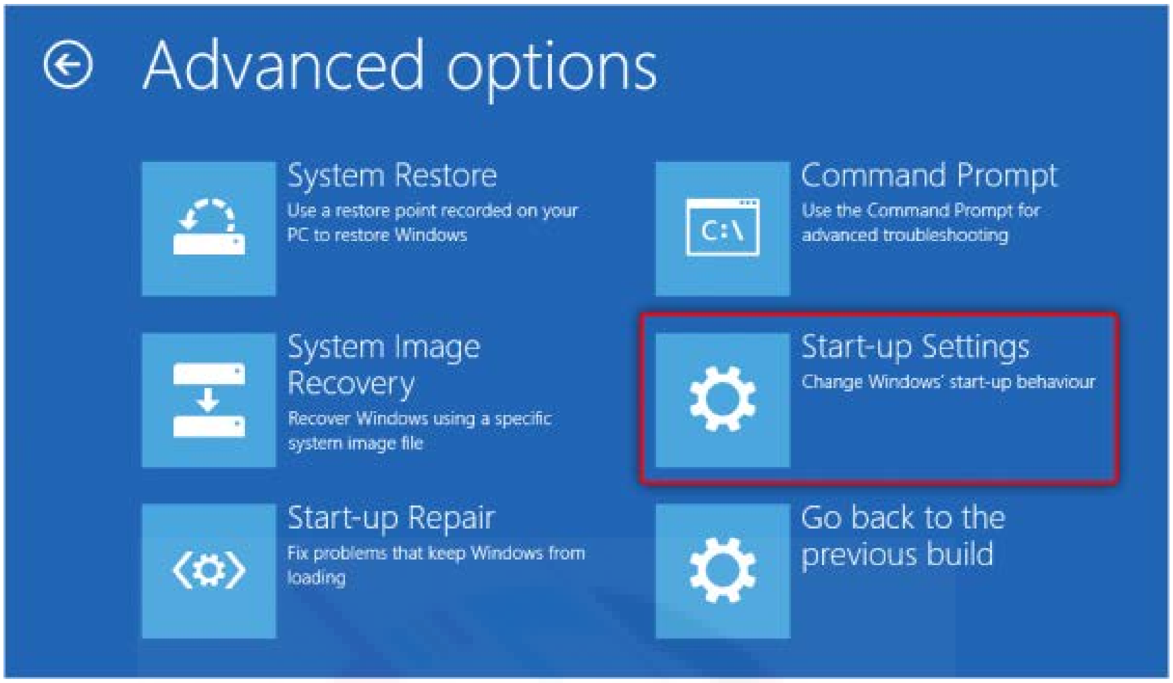

Choose an option
Continue
Exit and continue to Windows 10
Troubleshoot
Reset your PC or see advanced options
Turn off your PC

Choose Troubleshoot


Troubleshoot
Reset this PC
Lets you choose to keep or remove your files, then re-installs Windows.
Advanced options

Choose Advanced Options

6. Click Startup Settings.



Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Image Recovery
Recover Windows using a specific system image file

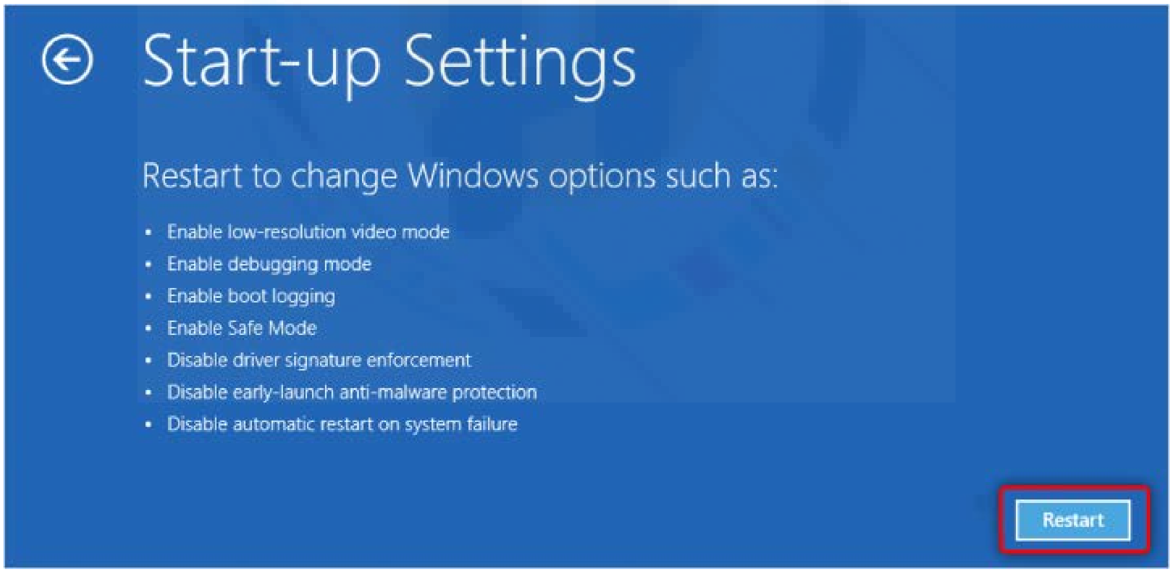
Start-up Settings
Change Windows' start-up behaviour

Start-up Repair
Fix problems that keep Windows from loading

Go back to the previous build

Choose Start-up Setting

7. Click Restart.



Start-up Settings

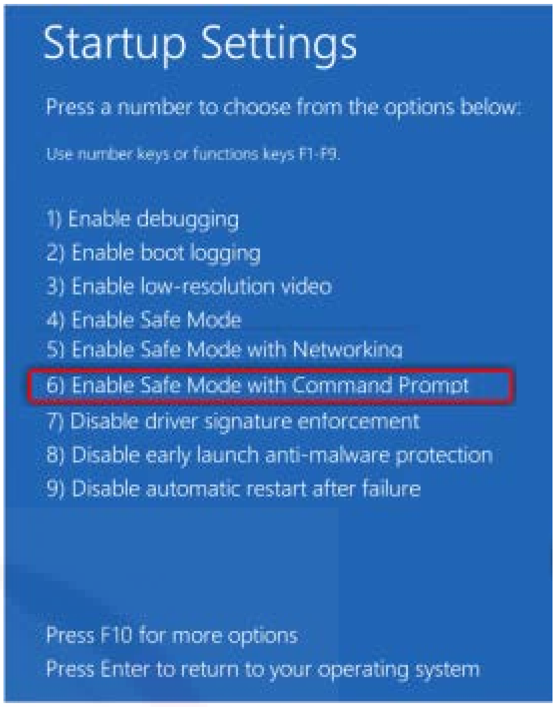
Restart to change Windows options such as:

- Enable low-resolution video mode
- Enable debugging mode
- Enable boot logging
- Enable Safe Mode
- Disable driver signature enforcement
- Disable early-launch anti-malware protection
- Disable automatic restart on system failure

Press Restart

8. After your computer restarts, select Safe Mode with Command Prompt
9. Enter your Administrative username and password to start Windows in Safe Mode with Networking.

NOTE: To get back to normal Windows configuration you need to Click Start → Power and then click Restart.



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

Press F10 for more options
Press Enter to return to your operating system

Choose SSafe Mode with Command Prompt

## 1.2 Open task manager using command prompt:

- Type “taskmgr.exe” within the cmd(Command Prompt) window and press enter.
- Once the Task manager window opens-switch to the “Processes” tab to locate the malicious process and end them all.
- To end the ransomware associated process: click on the process name and hit the “End Process” button at the bottom-right corner.
- Once done close the task manager window.

Note: If you are not sure of any process if it is exactly a malware or not then leave it.

## 1.3 Deleting Registry Entries created by the Ransomware threat

- Within the command prompt window: type “regedit” and press “enter”.
- This will open the Registry Editor window. You need to find the “Winlogon” folder within the left menu pane. Or simply copy and paste the URL “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon” (without quotes).
- In the middle pane, will appear the list of registries and its values set. Find the entry for “Shell” and default value for this should be “explorer.exe”. If appears to be some different like “C:\Documents and Settings\username\desktop\ransomwarename.exe”.Then you need to reset it to its default value. (But before that copy the name “ransomwarename.exe” of the virus to find more such entries and delete them.)
- Right click on the “Shell” and choose “modify” now replace its malicious value to “explorer.exe” and click “ok”.
- Now press “ctrl+F” to open the “Find” window, now paste the malicious entry which you found within the Shell and once you find the name, Right click on it and choose the “Delete”

option. Continue to find and delete till you delete all malicious entries.

- Once finished, close the registry editor window.
- Now you are back to command prompt window type “shutdown /r /t 0”(without quotes) and press Enter. This command will restart the computer in normal mode.

Once your computer is started normally, and start the deep scan to the computer system to remove any traces of the threat remain inside.

## 2.1 Remove Ransomware virus using System Restore Procedure

### 2.1 Reboot your computer to Safe Mode with Command Prompt

Steps mentioned above section.

2.2 Restore your system to default settings as it was prior to the Ransomware attack

- Once the Command Prompt window appears, type “cd restore” and press Enter.
- Now again type “rstrui.exe” and hit “Enter” button;
- It will show up a new window, now click on “Next” and select your restore point that should be prior to the attack of ransomware threat. Click on “Next”.
- Now click on “Yes” to confirm the system restore.
- Once the system restore to your selected date is done, then you need to restart your computer normally.
- Download effective antivirus program and scan your computer to ensure successful removal of the Ransomware threat.

# Use Anti-Ransomware To Remove Ransomware Virus.

# Ransomware Defender Overview

ShieldApps’ Ransomware Defender is a specially designed security program for Ransomware threats. This anti-ransomware program detects and permanently blocks any ransomware prior to its attack on the protected system.

Ransomware Defender maintains its threat database and its related information which makes the program proactively detect any sort of threat and notifies users upon detection. This anti-ransomware program works well along with your primary anti-malware applications and does not interfere with its work.

Ransomware Defender is compatible with Windows 7, 8, 8.1 and 10. And is suitable for both home and business network. It has various prominent features like real-time ransomware detection, scan protection, history cleaner, file transfer tools and automated scans that helps in better detection of ransomware threat and blacklist them from your system permanently. Additionally, this anti-ransomware solution also provides firewall security, internet protection, mobile security, and virtual private network configuration. The solution also offers 24/7 customer support via email.

If you generally do not keep backups of your important files and documents or use your computer or device for storing financial and business details, then it is very important to keep them secure. Here Ransomware Defender is proved as a comprehensive anti-ransomware solution.
Do not compromise with your computer's security.

Ransomware Defender solution comes with a subscription of $49.95.

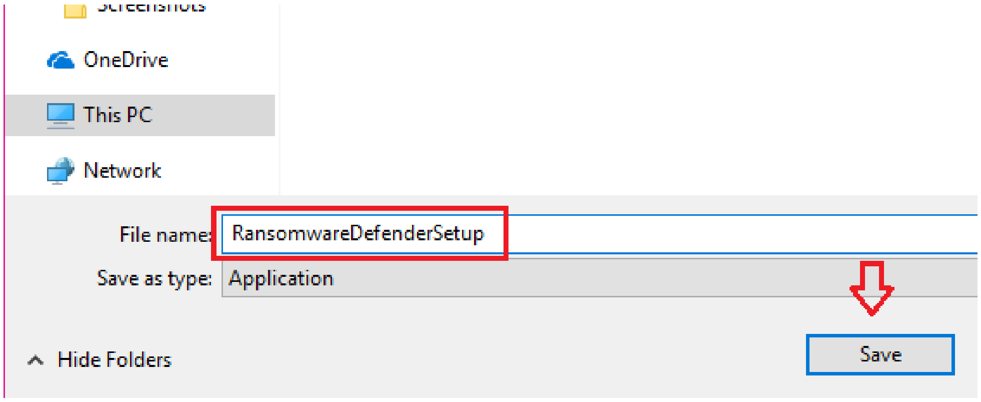
## Ransomware Defender Features

- Ransomware Protection: This ransomware solution effectively detects, removes and blacklists any ransomware that attempts to attack your system. And always keep monitoring the system within background for any possible attacks.
- Smart Ransomware Detection: Due to its advanced technology of threat detection, you can rest assured of system protection. It will give real-time updates and report of any suspicious activity.
- Internet Security: Protects from any unethical web activity, malicious attempts to breach your internet security, blocks any malicious websites and infected online scripts through ransomware generally enter.
- Scheduled Scan/Clean Action: It provides a user-friendly and fully automated solution for schedule scans at your preferred timings, thus even if you forgot to manually scan your computer you are still protected.
- Secure File Eraser: It's a very important feature provided by Ransomware defender that empowers you to fix any of your files/applications that you suspect as infected.
- 24/7 PROTECTION: Ransomware Defender provides 24/7 real-time protection due to its auto and schedules scan mechanism that guards your system all the time.

## Installing Ransomware Defender

Follow these steps to download and install Ransomware Defender on your computer.

- Click on the link to Download Ransomware Defender.
- Choose the location to save the installation file and click on "save".

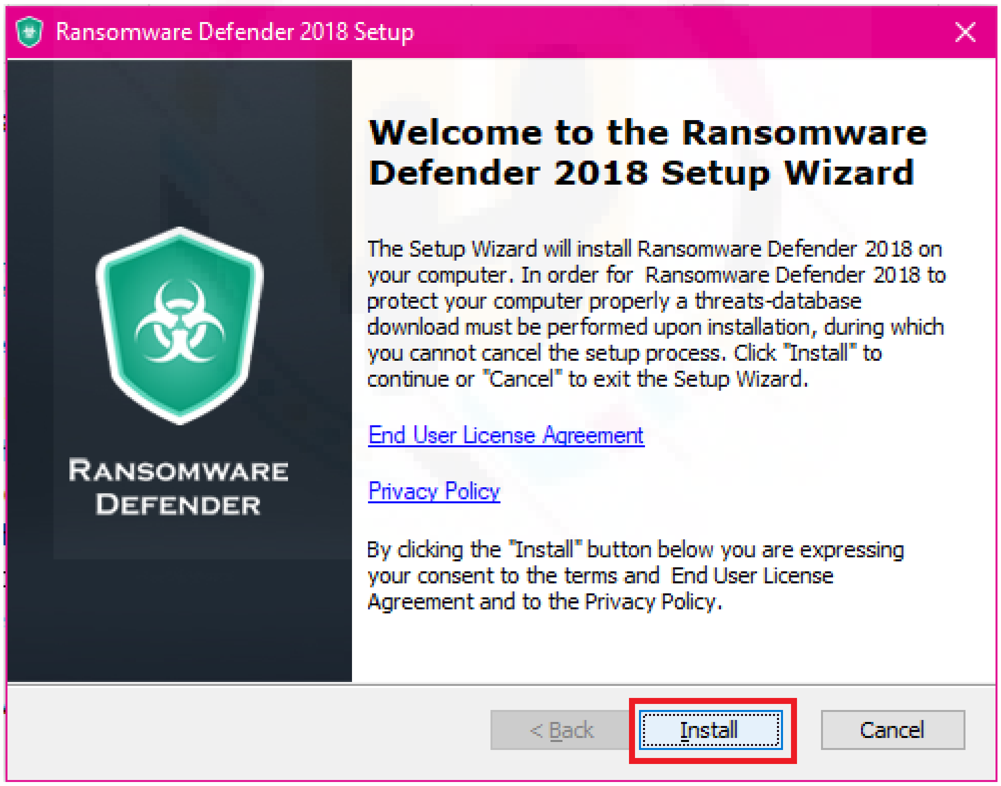


File name: RansomwareDefenderSetup

Save as type: Application

Ransomware Defender install step 1

- After the download is completed, double-click on the downloaded file to open.
- If prompted by User Account Control: click on “Yes” button.
- This will open an installation wizard. Click on “Install”. Now simply follow the on-screen instructions to complete the installation procedure.



**Welcome to the Ransomware Defender 2018 Setup Wizard**

The Setup Wizard will install Ransomware Defender 2018 on your computer. In order for Ransomware Defender 2018 to protect your computer properly a threats-database download must be performed upon installation, during which you cannot cancel the setup process. Click "Install" to continue or "Cancel" to exit the Setup Wizard.

End User License Agreement

Privacy Policy

By clicking the "Install" button below you are expressing your consent to the terms and End User License Agreement and to the Privacy Policy.

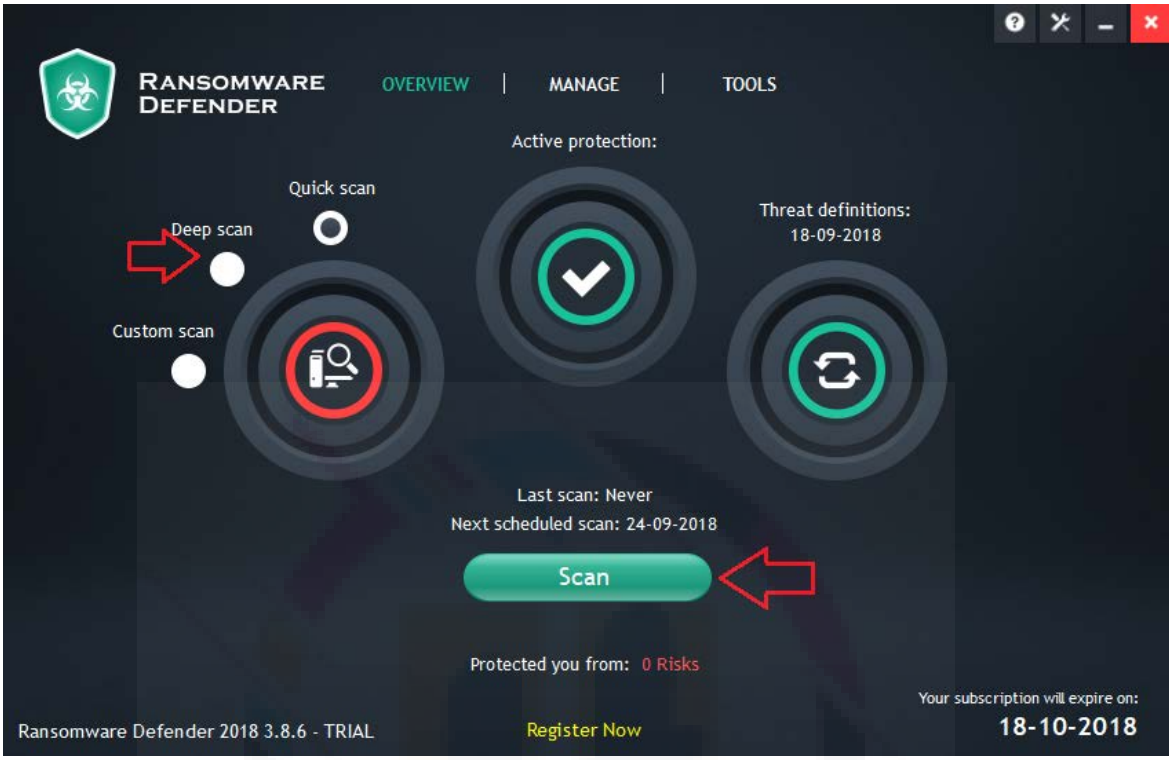
Ransomware Defender install Step 2

- After Ransomware Defender successfully installs, a new tab or window will open on your browser showing confirmation of the installation.

## Run Scan To Detect Ransomware threat on your computer

Follow the steps to properly scan and remove ransomware threat from your computer:

1. Start the scan: Once the installation is completed, the Ransomware defender application window will open. Here you have 3 options for scan: Quick, Deep, and Custom. We suggest doing Deep scanning for the first time for better detection of ransomware threats.



Active protection:

Threat definitions: 18-09-2018

Last scan: Never

Next scheduled scan: 24-09-2018

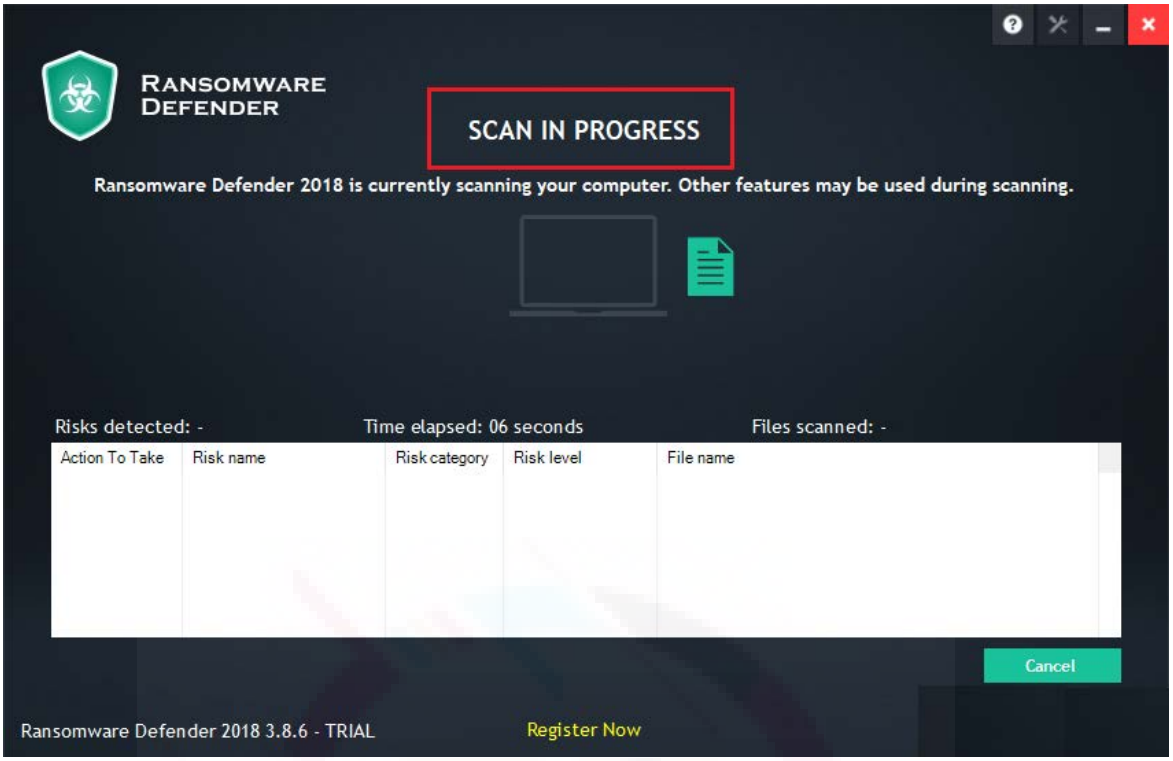
Protected you from: 0 Risks

Ransomware Defender 2018 3.8.6 - TRIAL

Your subscription will expire on: 18-10-2018

Ransomware Defender Scan

2. Let the scanning process be completed: Scan will take a few minutes so be patient and let the scan be fully completed.



Ransomware Defender 2018 is currently scanning your computer. Other features may be used during scanning.

Risks detected: -

Time elapsed: 06 seconds

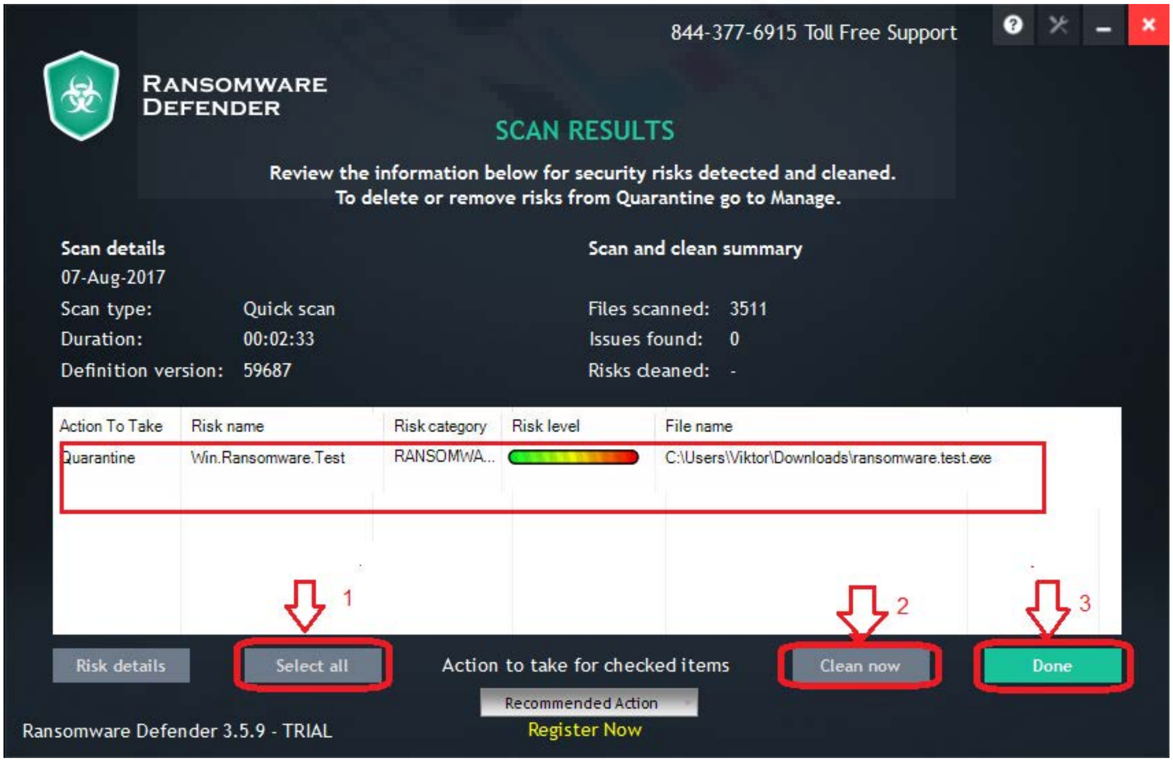
Files scanned: -

| Action To Take | Risk name | Risk category | Risk level | File name |
|---|---|---|---|---|

Ransomware Defender 2018 3.8.6 - TRIAL

Ransomware Defender Scan In Progress

3. Review the Scan Results and remove the threats: Review the scan results that will show all the threats and malware found during the scan process, you can manually choose to remove the threats one-by-one by clicking on the threat name and select “delete” or simply click on the “Clean All” button.



Review the information below for security risks detected and cleaned.
To delete or remove risks from Quarantine go to Manage.

**Scan details**

07-Aug-2017

Scan type: Quick scan

Duration: 00:02:33

Definition version: 59687

**Scan and clean summary**

Files scanned: 3511

Issues found: 0

Risks cleaned: -

| Action To Take | Risk name | Risk category | Risk level | File name |
|---|---|---|---|---|
| Quarantine | Win.Ransomware.Test | RANSOMWA... | | C:\Users\Viktor\Downloads\ransomware.test.exe |

Ransomware Defender 3.5.9 - TRIAL

Ransomware Defender Remove Threats