

RAN\$TOP

2018

User manual

Contents

Table of Figures	3
1. Introduction	4
1.1. About TEMASOFT Ranstop	4
1.2. How TEMASOFT Ranstop works	5
1.3. TEMASOFT Ranstop components	5
2. Installing TEMASOFT Ranstop	7
2.1. Getting started	7
2.2. System requirements	7
2.3. Interactions with other software	7
2.4. Running the installation kit	7
2.5. Upgrading from previous versions	11
2.6. Uninstalling TEMASOFT Ranstop	11
3. Deploying TEMASOFT Ranstop in large environments	12
3.1. Initial deployment	12
3.2. Upgrading from previous versions	13
4. Monitoring TEMASOFT Ranstop activity	14
5. Detecting ransomware	15
6. File recovery	17
6.1 How file recovery works	17
6.2 Viewing files available for recovery	17
6.3 Performing manual file recovery	18
6.4 Managing exclusions	19
7. Configuration options	19
7.1 Application whitelist	19
7.2 Backup configuration	20
7.3 Support	23
7.4 Alerting	23
7.5 Reactions	24
7.6 Ranstop updates	25
8. How does Ranstop file protection work?	26
9. Licensing	27
10. Troubleshooting Ranstop	29
10.1 Troubleshooting the uninstall process	29

10.2	Running process checklist	29
10.3.	Contacting TEMASOFT Support	30

Table of Figures

Figure 1: How TEMASOFT Ranstop works.....	5
Figure 2: TEMASOFT Ranstop Console.....	6
Figure 3: TEMASOFT Ranstop Alerts	6
Figure 4: EULA Dialog.....	8
Figure 5: Detection of prerequisites.	8
Figure 6: TEMASOFT Ranstop installation wizard, the “Welcome” dialog	9
Figure 7: The license setup dialog.....	9
Figure 8: Backup drive setup dialog.....	10
Figure 9: TEMASOFT Ranstop installation - the progress dialog.....	10
Figure 10: TEMASOFT Ranstop installation complete dialog.....	11
Figure 11: Main dashboard	14
Figure 12: The "Alerts" tab.....	16
Figure 13: File recovery tab.....	18
Figure 14: Application whitelisting	19
Figure 15: Backup configuration	20
Figure 16: File Extensions dialog.....	21
Figure 17: Backup exclusions	22
Figure 18: Add/edit exclusion	22
Figure 19: Select storage drive dialog.....	23
Figure 20: Alerting configuration	24
Figure 21: Configuring additional reactions.....	25
Figure 22: TEMASOFT Ranstop Updates	26
Figure 23: The licensing dialog.....	28
Figure 24: Uninstall error message	29
Figure 25: Contact TEMASOFT Support dialog.....	30

1. Introduction

1.1. *About TEMASOFT Ranstop*

TEMASOFT Ranstop is an anti-ransomware tool that can identify the vast majority of the current and future ransomware in seconds based on behavior analysis. Once identified, TEMASOFT Ranstop will attempt to block the ransomware and notify the user.

TEMASOFT Ranstop detects and blocks ransomware as it starts compromising files, by identifying specific activity and can cover for zero-day ransomware and targeted ransomware variants. The files that the ransomware affects until it is blocked are recovered automatically. In addition, TEMASOFT Ranstop protects against many variants of screen lockers, and allows users to regain control of their machines in case of such incidents.

As any other security product, TEMASOFT Ranstop cannot guarantee it can catch all ransomware, but it allows files to be recovered (manually) even in the case when ransomware attacks cannot be blocked.

For best results, TEMASOFT recommends using Ranstop together with an anti-virus solution, in a multilayered security approach. Anti-virus solutions can block the main paths that ransomware uses to infect a computer, while TEMASOFT Ranstop takes care of those cases where ransomware manages to penetrate and starts encrypting files.

TEMASOFT Ranstop has two versions: the commercial, fully supported version (TEMASOFT Ranstop) and the freeware version (TEMASOFT Ranstop Home), which does not benefit from any technical support, and which is developed for personal, non-commercial use. There are a few differences between these two versions related to functional and deployment aspects, which are described further in this document.

1.2. How TEMASOFT Ranstop works

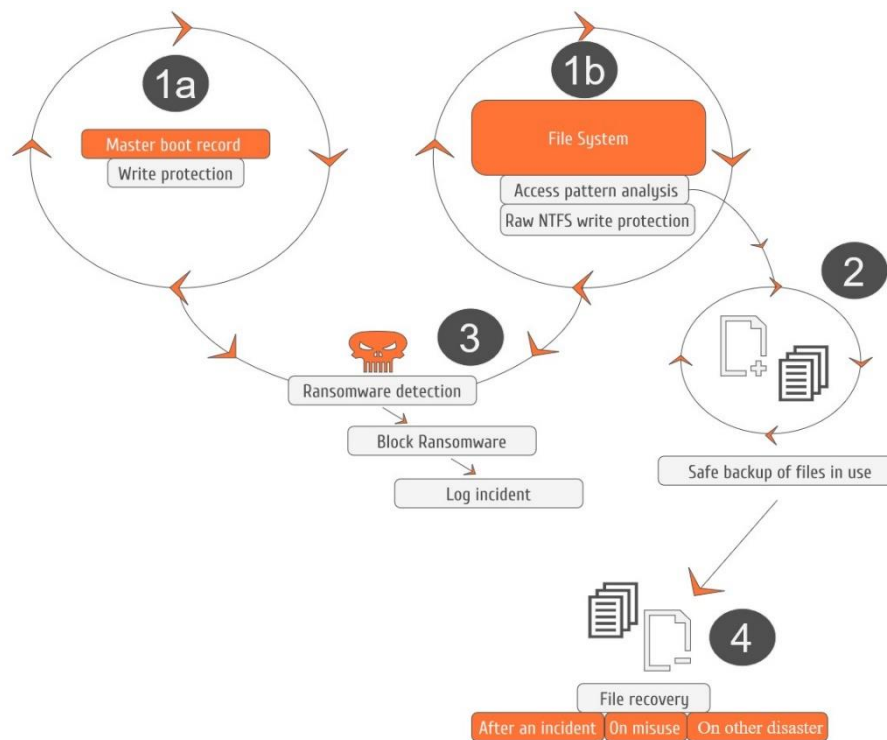


Figure 1: How TEMASOFT Ranstop works

1.3. TEMASOFT Ranstop components

- The TEMASOFT Ranstop Driver – this is responsible for detecting ransomware as well as protecting the storage area used for protecting the files and backup operations;
- The TEMASOFT Ranstop Agent Service – this service is responsible for managing the TEMASOFT Ranstop driver;
- The TEMASOFT Ranstop Tray Application – this is a tray application which allows starting the TEMASOFT Ranstop Console and displays notification balloons;
- The TEMASOFT Ranstop Console – this is the main UI application that allows configuration of the product and monitoring of its activity. This console may only be used by users with administrative privileges;

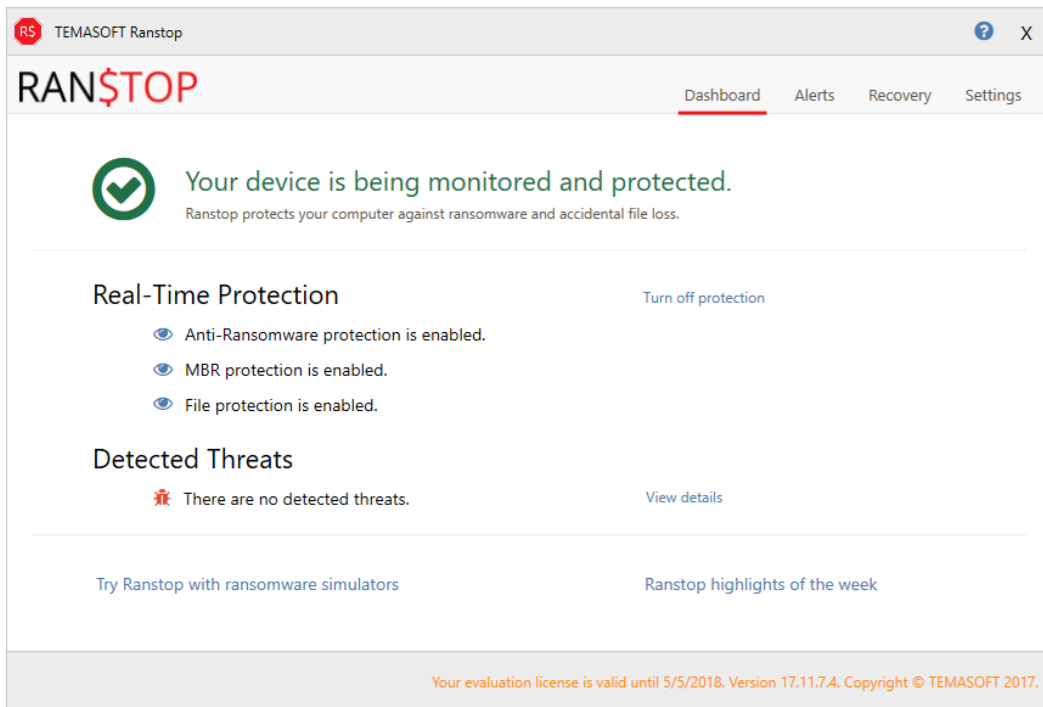


Figure 2: TEMASOFT Ranstop Console

- e) The TEMASOFT Ranstop Alerting View – this is a separate console which can be started from the TEMASOFT Ranstop Tray Application. It displays the list of current alerts. This can be started by users without administrative privileges.

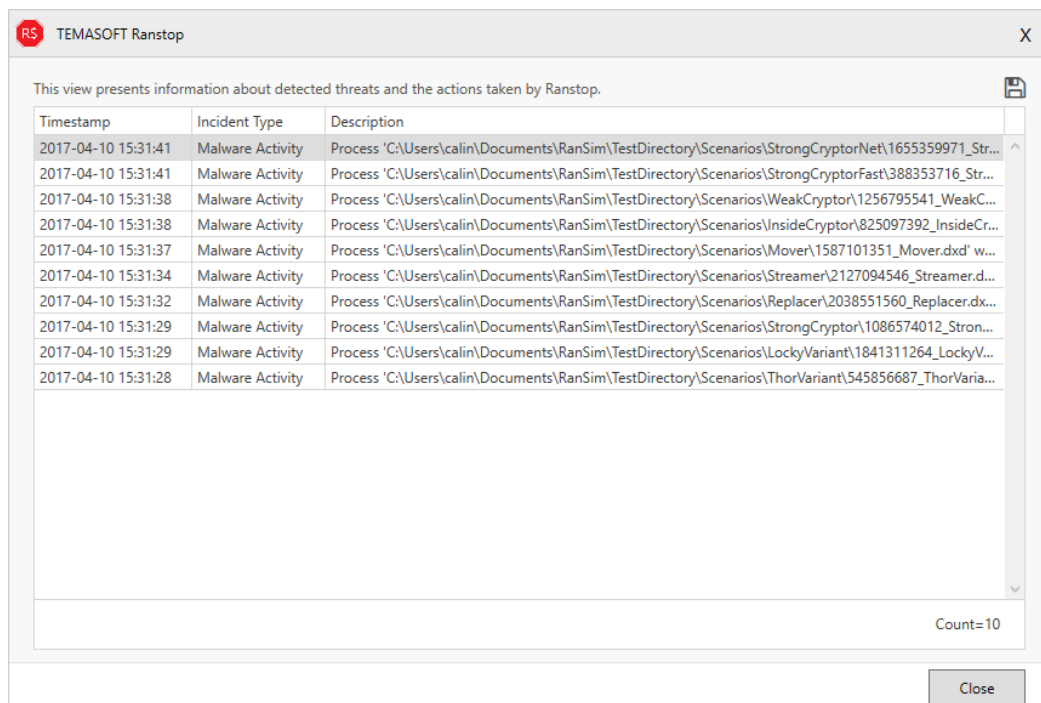


Figure 3: TEMASOFT Ranstop Alerts

2. Installing TEMASOFT Ranstop

This chapter presents the necessary information for installing TEMASOFT Ranstop 2018 on your computer.

2.1. *Getting started*

The TEMASOFT Ranstop 2018 installer is delivered as an executable which runs on Microsoft Windows x64 and x86 architectures, on workstations and servers (starting with Windows Server 2008 R2); TEMASOFT Ranstop Home edition does not work on servers.

In order to get started, you need to run this installation kit as an administrator. Please review the “System requirements” chapter below, before running the installation kit.

2.2. *System requirements*

TEMASOFT Ranstop 2018 requires the following hardware and software prerequisites

a. Hardware:

TEMASOFT Ranstop does not have significant hardware requirements. Any ordinary PC will be able to run Ranstop – 2GB of RAM and 2 CPU cores. However, in order to be able to protect as many files as possible, when suspicious activity occurs, TEMASOFT recommends at least 10 GB of free disk space.

b. Software environment:

Operating systems:

Microsoft Windows 7 and newer; Please note that we do not support the “Microsoft Windows Home” editions for any of the above desktop operating systems.

Microsoft Windows Server 2008 R2 or newer (not applicable to TEMASOFT Ranstop Home edition).

Prerequisites:

Microsoft Visual C++ 2015 Redistributable (x86) and (x64), Microsoft .Net Framework 4.6.1.

2.3. *Interactions with other software*

TEMASOFT Ranstop uses a kernel-mode driver to operate and works with the file system at a low level. Although during our tests we have not observed any kind of undesired interactions between TEMASOFT Ranstop and anti-virus and backup software, conflicts accessing files may occur in the future. In case they do, please contact TEMASOFT Support (not applicable to TEMASOFT Ranstop Home). We recommend the use of TEMASOFT Ranstop in conjunction with anti-virus solutions to maximize the protection against ransomware.

2.4. *Running the installation kit*

- a) Please run the installation kit as an administrator by following these steps:
 - i. Right-click the downloaded executable;

- ii. Select “Run as”;
 - iii. Enter administrative credentials.
- b) On the license agreement dialog, please scroll down and read the EULA. In order to proceed, you must accept and acknowledge the terms of the EULA by clicking the associated tick box.

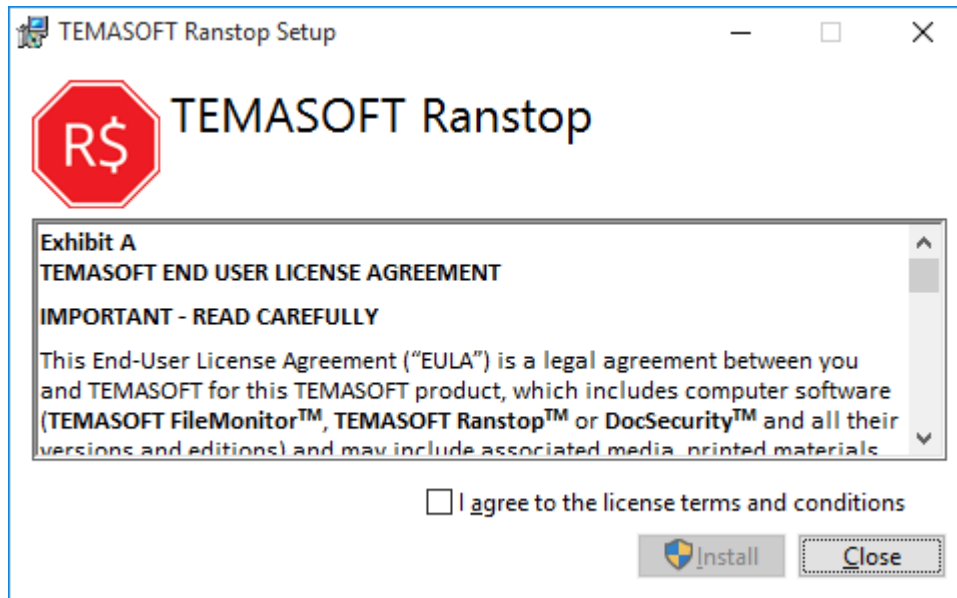


Figure 4: EULA Dialog

- c) Upon starting, the install kit will detect the existence of the prerequisites and install accordingly:
 - i. The TEMASOFT FileMonitor Agent;
 - ii. The TEMASOFT Ranstop Application.

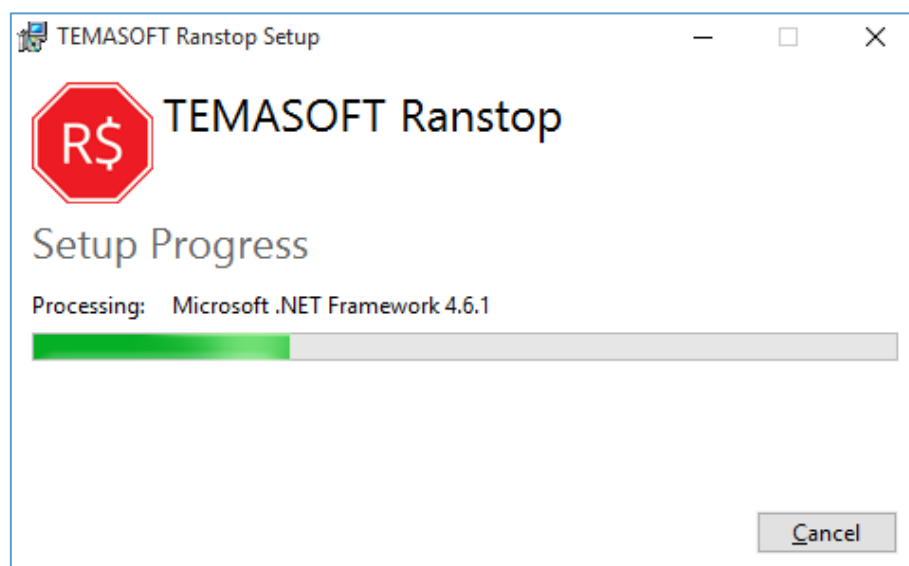


Figure 5: Detection of prerequisites.

- d) Once the prerequisites have been installed, the main installation wizard will start.

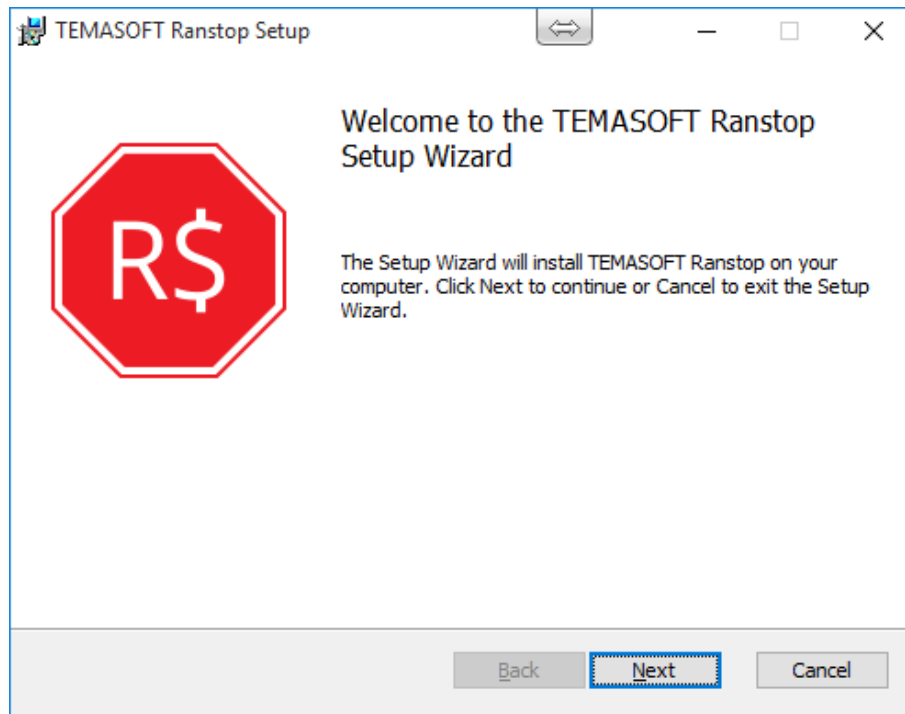


Figure 6: TEMASOFT Ranstop installation wizard, the “Welcome” dialog

- e) On the license setup dialog (not applicable to TEMASOFT Ranstop Home), please load the license file supplied to you by TEMASOFT or one of its partners. If you do not have one, you can proceed in Evaluation Mode for 15 days.

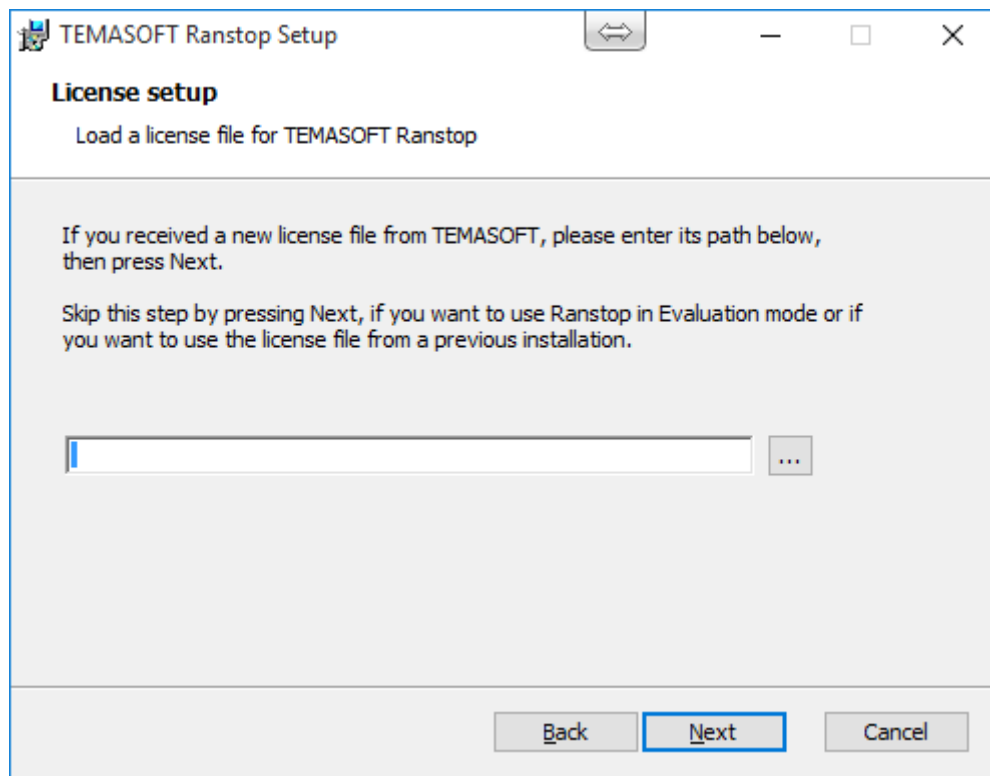


Figure 7: The license setup dialog

- f) On the “Backup drive setup” dialog, please select a drive where TEMASOFT Ranstop will create the backups of the user files in real time.

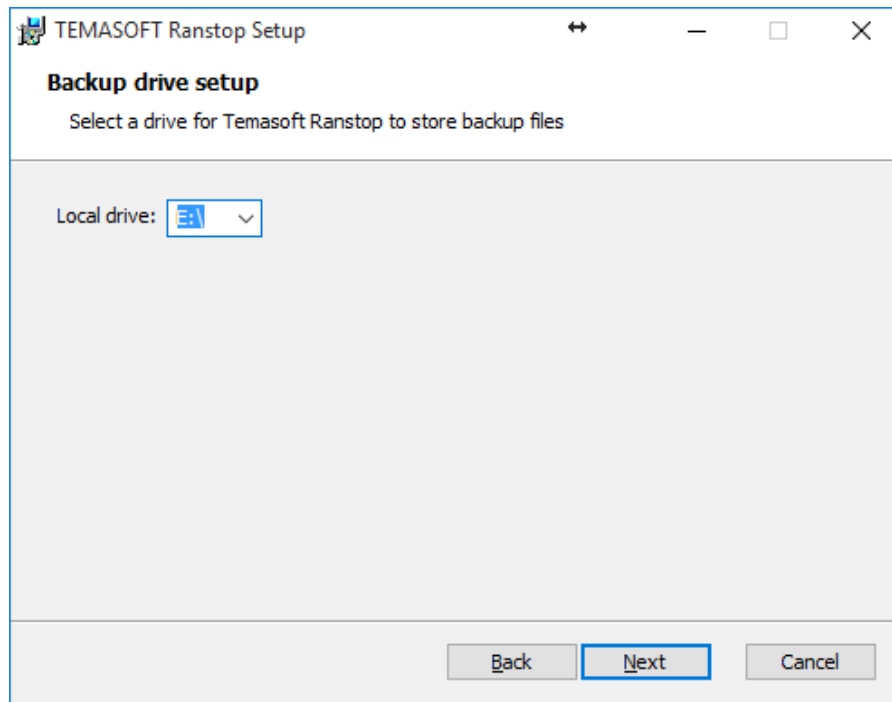


Figure 8: Backup drive setup dialog

- g) Click “Install” to start the installation process. TEMASOFT Ranstop runs as a tray application, but upon starting it, the UI will be fully visible.

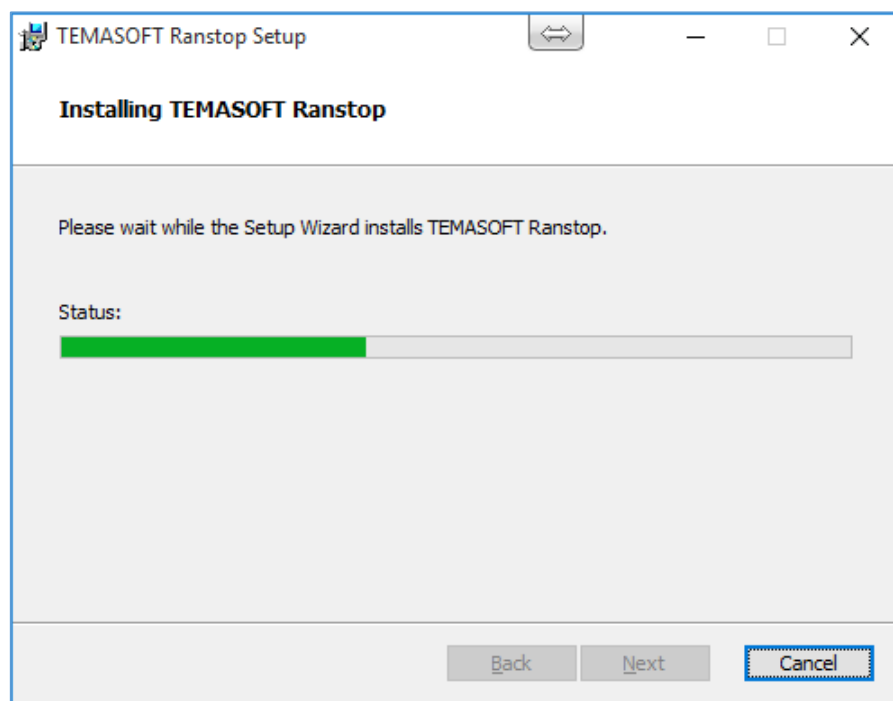


Figure 9: TEMASOFT Ranstop installation - the progress dialog

- h) Once the installation is complete, the wizard will display a confirmation dialog. You have the option to restart the computer upon closing the wizard. Note that a restart is required for the protection to function properly.

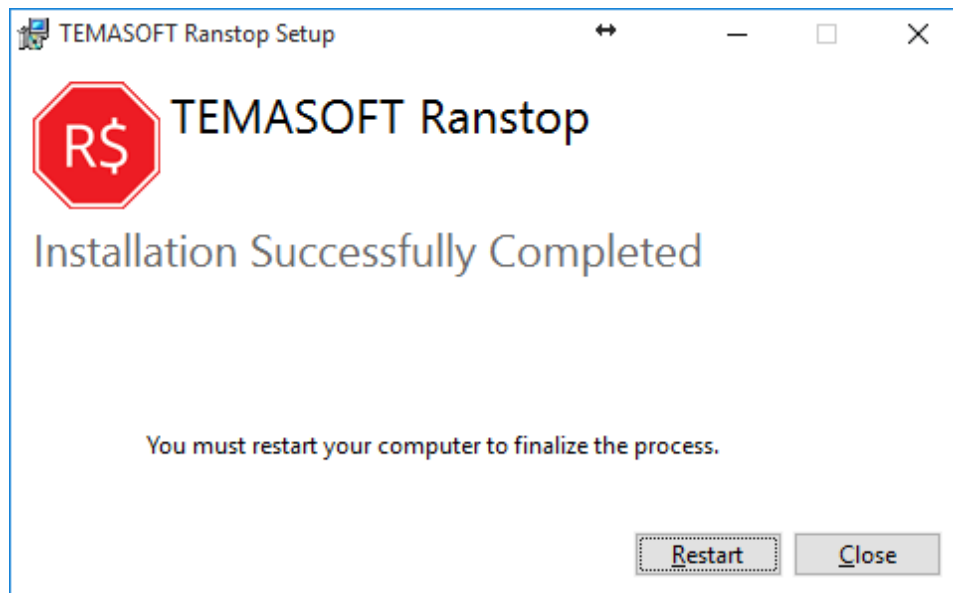


Figure 10: TEMASOFT Ranstop installation complete dialog

2.5. Upgrading from previous versions

The TEMASOFT Ranstop notifies you about the up-to-date status and the availability of new versions by displaying information in the product dashboard (provided that the computer running TEMASOFT Ranstop is connected to the internet). Whenever a new version is available, you can upgrade the existing version by following the below procedure:

- Download the installer of the new version from <http://download.ranstop.com> or <http://downloadfree.ranstop.com> (for TEMASOFT Ranstop Home);
- Uninstall the existing version and keep the backup and the configuration files;
- Install the new version.

Note: if you are upgrading TEMASOFT Ranstop in a large environment, please consult chapter 3, paragraph 2.

IMPORTANT: Temasoft Ranstop 2018 backup settings are not compatible with the backup settings of the previous versions, therefore one needs to completely remove any Ranstop 2017 version (any Ranstop build up to 17.6.28.4, from June 2107), including backup and other operational files, before installing Ranstop 2018 versions (builds released from October 2017 onwards) on the same machine.

2.6. Uninstalling TEMASOFT Ranstop

To uninstall TEMASOFT Ranstop please use the following procedure:

- Open "Programs and Features" dialog in Control Panel;
- Locate TEMASOFT Ranstop;

- Right click on it and select “Uninstall”;

The un-installation process will start and will prompt you to decide if to keep the backup and configuration files or not. If you plan to reinstall Ranstop, keeping the configuration and the backup files will make the new installation easier. If you want to remove the backup files, please choose “Yes” on the dialog mentioned above.

IMPORTANT: Do not attempt to uninstall TEMASOFT Ranstop using uninstall tools or any other third-party software. Ranstop uses tampering protection features that prevent external applications from interfering with its files. Therefore, it is highly recommended to avoid using custom uninstall applications to remove Ranstop from computers.

3. Deploying TEMASOFT Ranstop in large environments

TEMASOFT Ranstop can be deployed in large environments by following the below procedures (not applicable to TEMASOFT Ranstop Home):

3.1. Initial deployment

If you are running a domain environment

1. Create an Active Directory group containing the computers on which you want to deploy the product; the name of the group needs to be “**RanstopComputers**” – you cannot assign another name for this group; The designated computers must be members of this group explicitly, not by inheritance.
2. For the automatic deployment, create a group policy that will roll out the *AgentInstaller.msi* and the *RanstopInstaller.msi* packages; for more information on how to deploy an application via GPO, please consult this article: <https://support.microsoft.com/en-us/kb/816102>
3. The packages are available for download here:
<http://download.ranstop.com/AgentInstaller.msi>
<http://download.ranstop.com/RanstopInstaller.msi>
 - a. It is important to make sure that the prerequisites are already installed on the target machines, per chapter 2.2 “System Requirements”, the “Prerequisites” section. These prerequisites can also be rolled out via GPO;
 - b. It is also important to install the two “.msi” packages in the correct order: *AgentInstaller.msi* first, followed by *RanstopInstaller.msi*.
 - c. Once the packages have been installed, the target machines need to be restarted.
4. For configuring the agents please follow these steps:
 - a. Install TEMASOFT Ranstop on a single computer, configure it as needed and make a copy of all the XML files present under (C):\ProgramData\Temasoft\FileMonitor Agent\Config. For example: *AlertingConfig.xml*, *AppWhiteListConfig.xml*, *BackupConfig.xml*, *ReactionsConfig.xml*, *ExclusionsConfig.xml*, *Datacollector.xml*, *Agentconfig.xml*. These configuration files will be shared with other computers;
 - b. Choose a machine in Active Directory which will host a share, containing the agent configuration file;
 - c. Create the share on the machine chosen above, and assign write privileges for the “Domain Admins” group, and read privileges for the “RanstopComputers” group defined at point 1;

- d. In Active Directory Users and Computers -> Computers create a share named **"ranstopconfig"** (name cannot be changed) and assign it the UNC path to the share created at point 4.c above;
- e. In the **"ranstopconfig"** share, copy the configuration files listed under 4.a; they contain the settings to be used by all agents; also copy here the licensing file received by email. This file will be used by all the agents in the group;
5. For more granular configurations please follow these steps:
 - a. You can create additional groups that will have different settings for TEMASOFT Ranstop; (e.g. **"AccountingComputers"**). Make sure the computer(s) are explicit members of both **"RanstopComputers"** and the custom (e.g. **"AccountingComputers"**) groups;
 - b. In the **"ranstopconfig"** share created at point 4.d, create subfolders with the name of the groups defined at point 5.a;
 - c. In the subfolders created at point 5.b copy the files listed under point 4.a, with the corresponding settings, and the licensing file;
Note: if a machine is member in multiple groups as per point 1 and 5.a, the settings that exist in the first group identified by TEMASOFT Ranstop will be used.
 - d. You can also configure individual settings for computers in **"RanstopComputers"** by creating a subfolder in the **"ranstopconfig"** share with the same name as the name of the computer.
Note: If, for a computer, there are settings found as defined at 5.d, these will take priority over other settings (when the computer is a member in a group that also has a configuration created based on this procedure)

So, for a computer in the AD **"RanstopComputers"** group, the settings will be applied as follows (ordered by priority)

- From the subfolder with the same name (as the computer name) in the **"ranstopconfig"** share (if any);
- From the subfolder with a group name that the computer belongs to in the **"ranstopconfig"** share (if any);
- From the **"ranstopconfig"** share (root directory – if found);
- From the TEMASOFT Ranstop installation folder of the local machine (if none of the above paths contain any configuration information)

If you are running in a workgroup environment

In this case, you will need to deploy the install on each machine manually, or use a remote deployment tool. The configuration and licensing information needs to be manually performed on each agent;

3.2. Upgrading from previous versions

If you are running a domain environment

To upgrade an existing version of TEMASOFT Ranstop in a domain environment, please follow the below procedure:

- Remove existing TEMASOFT Ranstop instances using group policy;
 - o Use the same policy you have created when deploying TEMASOFT Ranstop;
 - o Select **"All tasks"** -> Remove;
 - o Choose the **"Immediately uninstall the software from users and computers"** option;

- Once the product has been removed, install the new TEMASOFT Ranstop version per [chapter 3.1](#)

If you are running a workgroup environment

To upgrade TEMASOFT Ranstop in a workgroup environment, you need to first uninstall the existing version and then install the new version manually.

4. Monitoring TEMASOFT Ranstop activity

TEMASOFT Ranstop provides a dashboard for monitoring current activity. On the dashboard you can see the product status and the up-to-date status. Only users with administrative privileges are able to run the Ranstop Main Console. Users without administrative privileges can only run a limited user interface consisting of the “Alerts” tab.

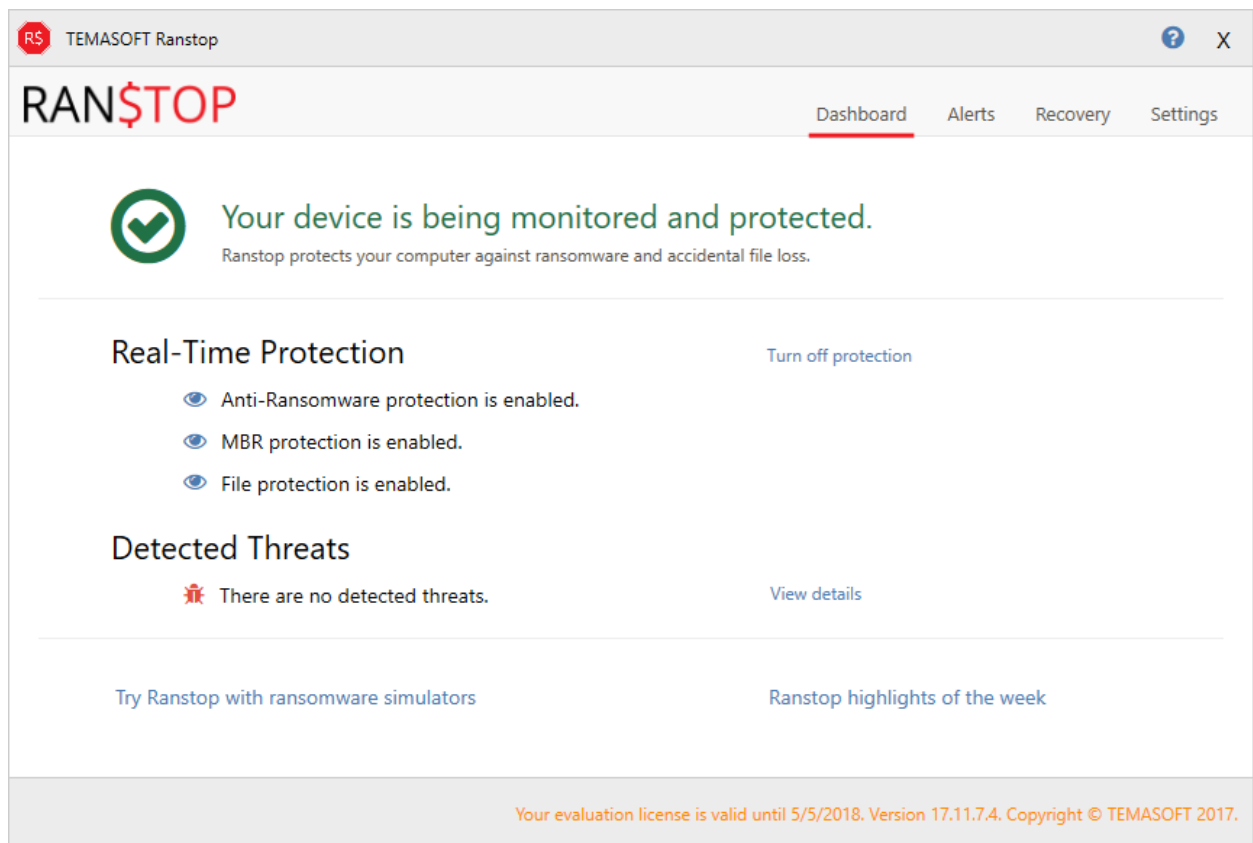


Figure 11: Main dashboard

Manage the real-time protection

The dashboard allows turning on and off the real-time protection by using the “Turn off protection” or “Turn on protection” links. When the real-time protection is turned on, TEMASOFT Ranstop protects the master boot record, and detects and blocks ransomware, screen lockers or other types of malware that damage files. When the real-time protection is turned off, you are not protected from these threats.

Monitoring the real-time protection status

The dashboard displays the following message across the top panel, highlighted in green: “Your device is being monitored and protected.” The text is preceded by a green “check” icon. In addition, the Real-Time Protection status message will state “Anti-ransomware protection is enabled”, “MBR protection is enabled”, and “File protection is enabled”. If there are any errors, the messages on the dashboard will change accordingly.

Monitoring the up to date status

The bottom left of the dashboard displays up-to-date status information, if there is a new version available. The product checks for updates automatically and displays the message accordingly. The bottom right of the dashboard contains version and licensing information.

Testing Ranstop

The bottom left link “Try Ranstop with ransomware simulators” will take you to a page on our website, which explains how to test TEMASOFT Ranstop against ransomware simulators.

Keeping abreast with the latest threats

The link at the bottom right takes you to our blog section where we post information and videos about latest ransomware threats.

5. Detecting ransomware

Whenever TEMASOFT Ranstop detects ransomware activity, it will perform the following actions:

- Alert the user on the incident by a tray balloon or email; this incident will also be added to the counter of the “Detection Details” panel on the dashboard, as well as to the list of incidents on the “Alerts” tab.
- Attempt to stop the process performing ransomware activity;
- Attempt to quarantine the process so that it can no longer execute without user intervention; When quarantined the offending executable(s) files will get the “.qrnt” extension.

Important: if you want to remove a process from quarantine, please follow the below procedure:

- Add the process to the whitelist (as per [Chapter 7.1](#));
- Make sure that you put in the entire path to the executable, as shown in the “Alerts” tab of the Ranstop main console, the “Description” field.
- If already quarantined, the executable file will be renamed to its original name.
- Follow back on the list of files accessed by the process;
- Automatically recover those files that the process had managed to compromise;

Managing TEMASOFT Ranstop incidents

The “Alerts” tab presents the list of TEMASOFT Ranstop incidents, providing information on:

- Timestamp when the incident occurred;
- The reason for recording the incident (e.g. Malware activity);
- The path to the responsible process and the name of the affected file;
- The list of alerts can be cleared by using the “Clear” link at the top right of the screen.

TEMASOFT Ranstop reports on ransomware activity, screen locker activity and important operational alerts.

Right-clicking an item in the list brings up the context menu which gives quick access to the following options:


- Open the application folder – this will open the path where the image file of the malicious process responsible for the incident resides;
- Open file folder – this will open the path to the affected files;
- Add to whitelist – automatically adds responsible executable to the whitelist. This removes the quarantine and ensures TEMASOFT Ranstop no longer interferes with that process. This option should be used to handle false positives (if any).
- Open the list of restored files – opens a dialog showing the list of files that were restored
- Copy to clipboard.

The screenshot shows the TEMASOFT Ranstop application window. The title bar reads "TEMASOFT Ranstop". The main header features the "RAN\$TOP" logo and navigation tabs: "Dashboard", "Alerts" (which is selected and highlighted with a red dashed box), "Recovery", and "Settings". Below the header, a message states: "This view presents information about detected threats and the actions taken by Ranstop." To the right of this message are icons for a close button (X) and a download button (floppy disk). The main content area contains a table with the following data:

Timestamp	Incident type	Description
2017-11-08 11:03:59	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\StrongCrytorFast\212678654...
2017-11-08 11:03:58	Malware Activity	Process 'C:\Windows\System32\cmd.exe' performed ransomware activity. Several files were affected, i...
2017-11-08 11:03:57	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\InsideCrytor\1178730217_Ins...
2017-11-08 11:03:52	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\Streamer\466681951_Streame...
2017-11-08 11:03:52	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\VirlockVariant\1639920244_Vir...
2017-11-08 11:03:52	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\StrongCrytorNet\114567951_...
2017-11-08 11:03:51	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\WeakCrytor\497888543_Wea...
2017-11-08 11:03:51	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\CritroniVariant\979560036_Cri...
2017-11-08 11:03:51	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\Mover\343195146_Mover.br'...
2017-11-08 11:03:51	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\LockyVariant\1719934162_Loc...
2017-11-08 11:03:51	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\Replacer\929008785_Replacer...
2017-11-08 11:03:50	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\StrongCrytor\862857084_Str...
2017-11-08 11:03:50	Malware Activity	Process 'C:\Users\calintms\Documents\RanSim\TestDirectory\Scenarios\ThorVariant\997242663_ThorV...

At the bottom right of the table area, it says "Count=13". Below the table, a footer message reads: "Your evaluation license is valid until 5/5/2018. Version 17.11.7.4. Copyright © TEMASOFT 2017."

Figure 12: The "Alerts" tab

You can use the buttons at the top right to export the list to CSV  or clear it .

TEMASOFT Ranstop post-attack cleanup

When detecting ransomware incidents, after stopping and quarantining the malicious processes and recovering the affected files, TEMASOFT Ranstop also attempts to clean up ransom notes and

encrypted files left over from the ransomware attack. It does so by deleting them. However, before it deletes them, it archives them into a zip file and leaves a journal (a file with .jrn extension) containing a listing of the files that had been deleted. Please consult this journal in case you believe files were deleted in error, and then recover them from the archive as needed.

These files are located in [c]:\ProgramData\Temasoft\FileMonitor Agent\Storage. To open the zip file, it is recommended to use a tool like 7zip.

6. File recovery

TEMASOFT Ranstop delivers file recovery technology to recover files lost to:

- Ransomware, from the time it starts its activity, until it is detected and blocked;
- Ransomware, on successful attacks that cannot be detected and blocked;
- Misuse or by accident.

The files that are compromised by ransomware which is later detected and blocked, are automatically recovered and require no user intervention. However, the files that are compromised as part of successful, undetected, ransomware attacks, or files lost by accident need to be manually recovered by the user using the TEMASOFT Ranstop user interface.

6.1 *How file recovery works*

TEMASOFT Ranstop uses a protected zone on the selected local drive to perform real-time backup of the important files when they change. The protected zone is dynamically allocated and can consume space depending on the configured values. Thresholds may be configured based on free space % or amount. Due to security reasons, only use NTFS drives can be used for backup purposes. The backup drive can be customized from the “Settings ->Backup configuration” tab as described further in this manual.

The real-time backup keeps up to four versions of the same file, and backs up the file types configured in the “Settings ->Backup configuration” tab. By default, there are more than 70 file types being backed up (documents, images, personal files usually the target of ransomware attacks), but the list can be customized.

TEMASOFT Ranstop Home can only backup common image and video files (.png, .jpg, .jpeg, .bmp, .gif, .mp4, .avi, .mkv, .mov, .3gp, .webm, .wmv), and the list of file types cannot be edited. Keep in mind though to avoid backing up system or application binary or temporary files.

The file versions are managed automatically to make sure there is always a recent, valid copy of the file available.

6.2 *Viewing files available for recovery*

To view the files available for recovery, please navigate to the TEMASOFT Ranstop “Recovery” tab. Here, you can find a file and directory listing of the current hard drive, containing only the files that can be recovered and the corresponding folders.

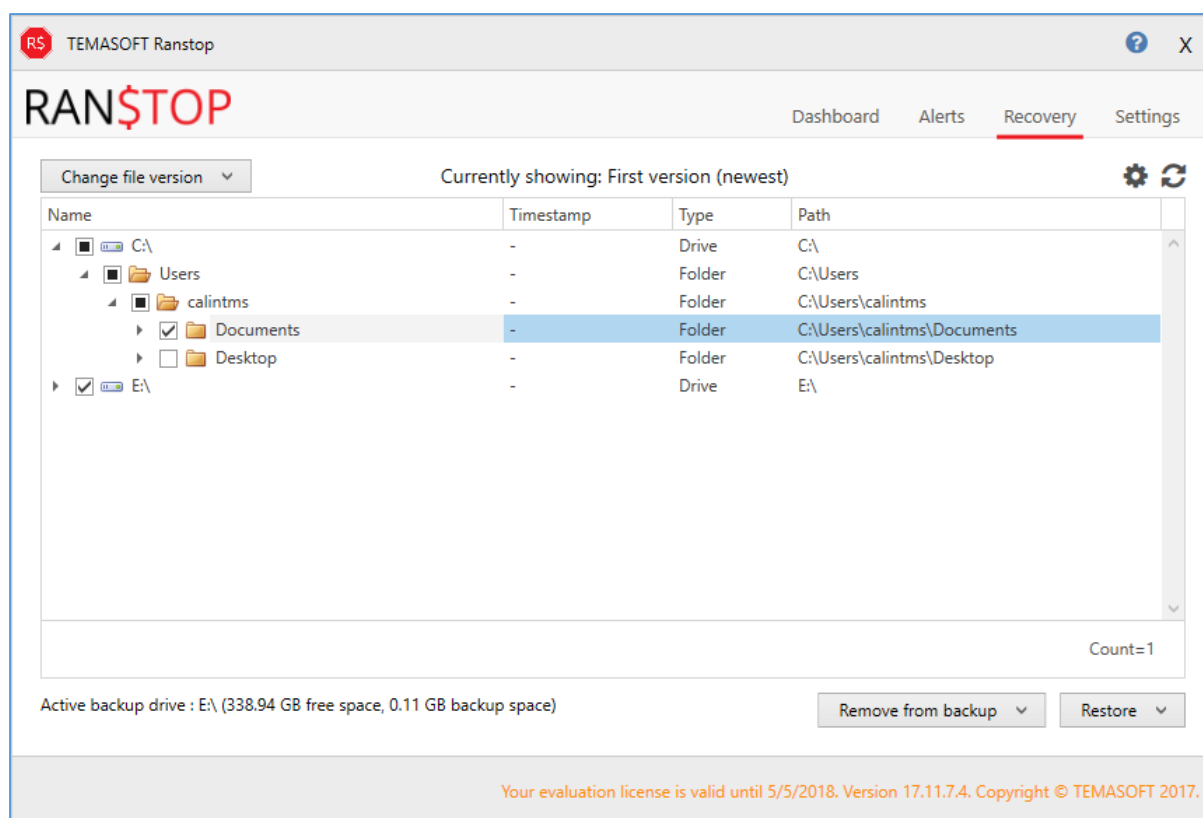


Figure 13: File recovery tab

You can use the triangle shaped buttons (or double click) to expand or collapse the folder structure. To refresh the view, use the “Refresh” button at the top right.

Select the desired file version view from the combo box at the top left. Depending on the selection, the list of available files will be updated.

6.3 Performing manual file recovery

To perform manual recovery of files, first use the above paragraph to navigate to the files in issue. Once the files have been located, select them using the associated tick box, corresponding to files or folder. Next, use the “Restore” button at the bottom right of the screen. Note that you will be restoring the file version designated in the combo box at the top right as per the previous paragraph.

The “Restore” button presents two options: one to restore the files to their original location and another option which allows selecting a destination folder to accommodate specific restore needs.


Cleaning up the backup repository

To clean up the backup repository, you can remove files from backup entirely, or partially (by removing only certain versions). To achieve this, navigate to the files / folders that you want to remove from backup and tick the associated tick box. Next, use the “Remove from backup” button to bring up the associated options:

- Remove “Selected version”; the selected version is the version chosen in the comb box at the top left as per [paragraph 6.2](#).
- Remove “All versions”.

Select one of the options to perform the desired action. You will next be prompted to confirm the operation, and decide whether to “Keep the oldest backup version for each file”. By default, the option is ticked, so if you want to remove the files entirely, you need to untick it before clicking on the “Yes” button. If you click “No”, the operation will be canceled entirely.

6.4 Managing exclusions

To exclude folders from the real-time backup process, please use the  button at the top right of the screen: This will take you to the “Backup configuration” dialog described in [sub-chapter 7.2](#).

7. Configuration options

This chapter presents the TEMASOFT Ranstop configuration options available on the “Settings” tab in the main user interface.

7.1 Application whitelist

The application whitelist tab allows configuration of applications that are ignored by TEMASOFT Ranstop when performing ransomware detection based on file access patterns. Any application listed here will not be analyzed and its actions will not register as malware activity. Consequently, any application listed here will not be blocked by TEMASOFT Ranstop. This functionality is intended to allow users to define encryption applications, or other applications that may register as having suspicious behavior so that their functionality is not blocked by TEMASOFT Ranstop.

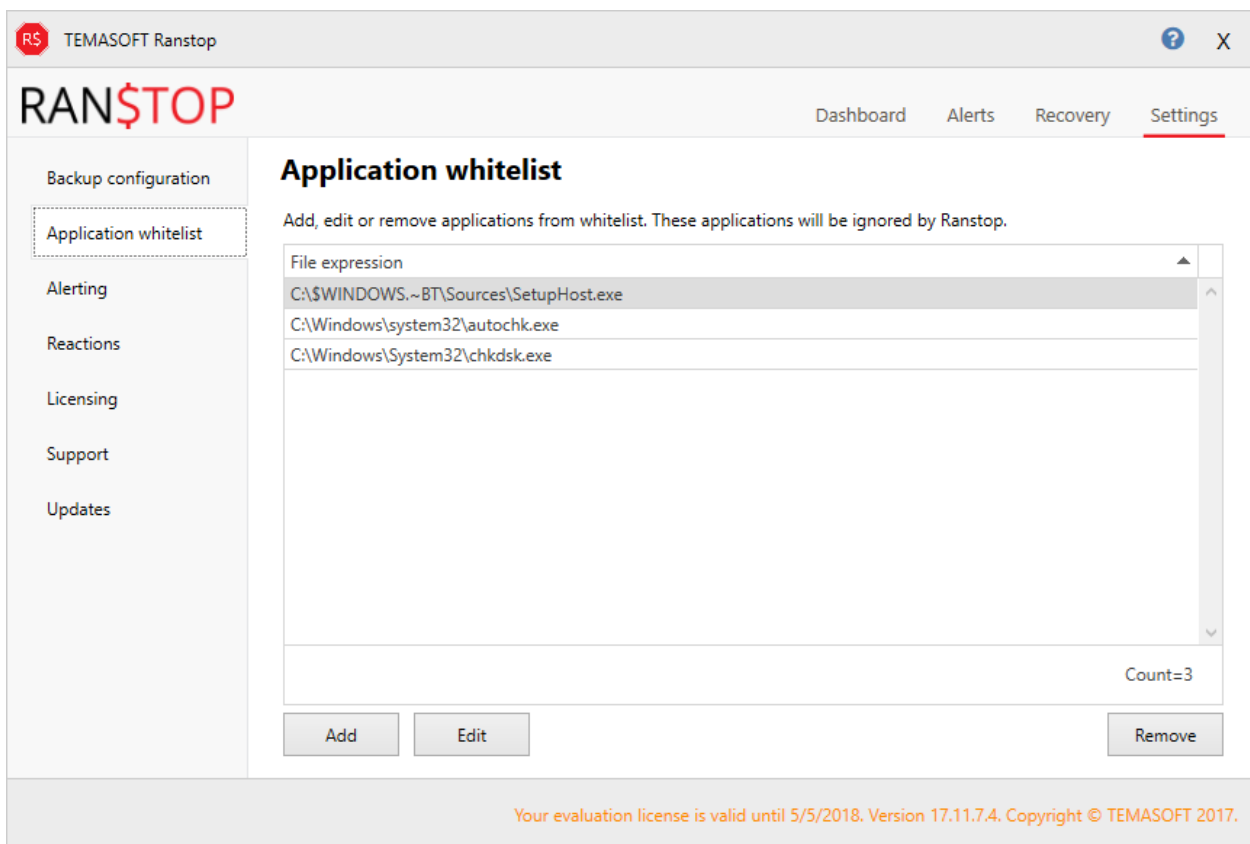


Figure 14: Application whitelisting

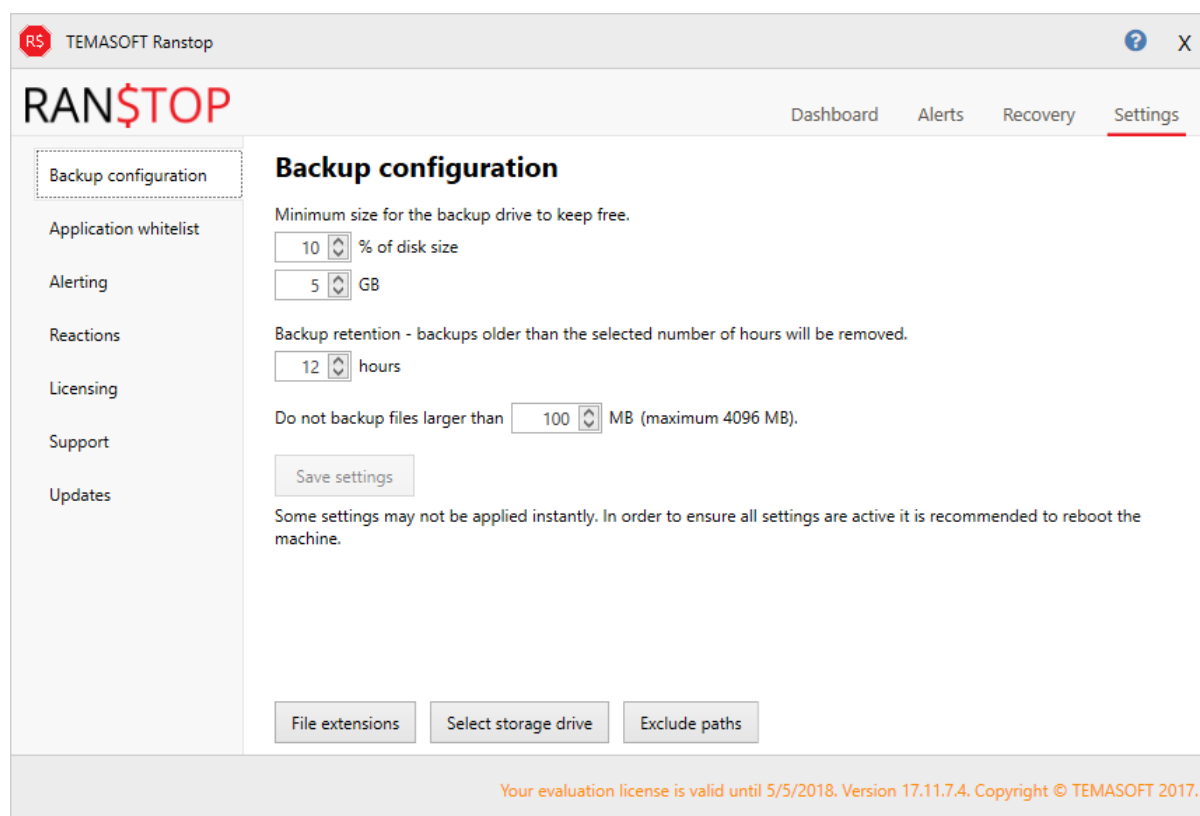
To add an application please click the “Add” button. This will bring up the “Add new application” dialog.

Input the path and file name of your application in the edit box and click “Save” to add it to the application whitelist. Similarly, you can edit existing applications by clicking the “Edit” button and following the same flow.

7.2 Backup configuration

The “Backup configuration” tab allows configuring the backup process. You can choose the drive to use for backing up files, the maximum amount of space to be used by the backup and the retention policy. In addition, the dialog allows configuring a size limitation for the files to be protected, as well as the extensions to protect and file paths excluded from the backup process.

By default, there are more than 70 file types (documents, images and personal files) being backed up by TEMASOFT Ranstop, but users can customize this list.



The screenshot shows the TEMASOFT Ranstop application window. The title bar reads "RS TEMASOFT Ranstop". The main interface has a sidebar on the left with the "RAN\$TOP" logo and navigation links: "Backup configuration" (selected), "Application whitelist", "Alerting", "Reactions", "Licensing", "Support", and "Updates". The main content area is titled "Backup configuration" and contains the following settings:

- Minimum size for the backup drive to keep free:
 - 10 % of disk size
 - 5 GB
- Backup retention - backups older than the selected number of hours will be removed:
 - 12 hours
- Do not backup files larger than: 100 MB (maximum 4096 MB).
- A "Save settings" button.
- A note: "Some settings may not be applied instantly. In order to ensure all settings are active it is recommended to reboot the machine."
- Three buttons at the bottom: "File extensions", "Select storage drive", and "Exclude paths".

At the bottom of the window, a status bar reads: "Your evaluation license is valid until 5/5/2018. Version 17.11.7.4. Copyright © TEMASOFT 2017."

Figure 15: Backup configuration

Configuring the main backup parameters

By default, each protected file is kept in a backup repository on the designated backup drive. If there is not enough space on the backup drive, an alert will be triggered, and files will not be backed up until more space becomes available again. The main parameters to configure are:

1. The amount of space to leave empty on the backup drive when performing the backup (in percentage). This defaults to 10% and can be configured to use a custom value;
2. The amount of space to leave empty on the backup drive when performing the backup (in GB). This defaults to 5 GB and can be configured to use a custom value;

3. Size limitation for the files to be protected. This defaults to 100 MB – files smaller than 100 MB will be protected. The value can be customized to accommodate larger files, up to 4GB.
4. Backup retention. This defaults to 12 hours. Backups older than the configured value will be deleted. If a ransomware attack is detected and the retention period is less than 3 days, then the retention period is automatically increased to 3 days.

Adding extensions

You can add new extensions to the list by clicking *“File extensions”*. This will bring up the *“File extensions”* dialog. Click *“Add”* and input the desired extension in the corresponding edit box of the new dialog. Click *“Save”* to confirm the changes. This feature is not available in TEMASOFT Ranstop Home, which uses a fixed list of file types (.png, .jpg, .jpeg, .bmp, .gif, .mp4, .avi, .mkv, .mov, .3gp, .webm, .wmv).

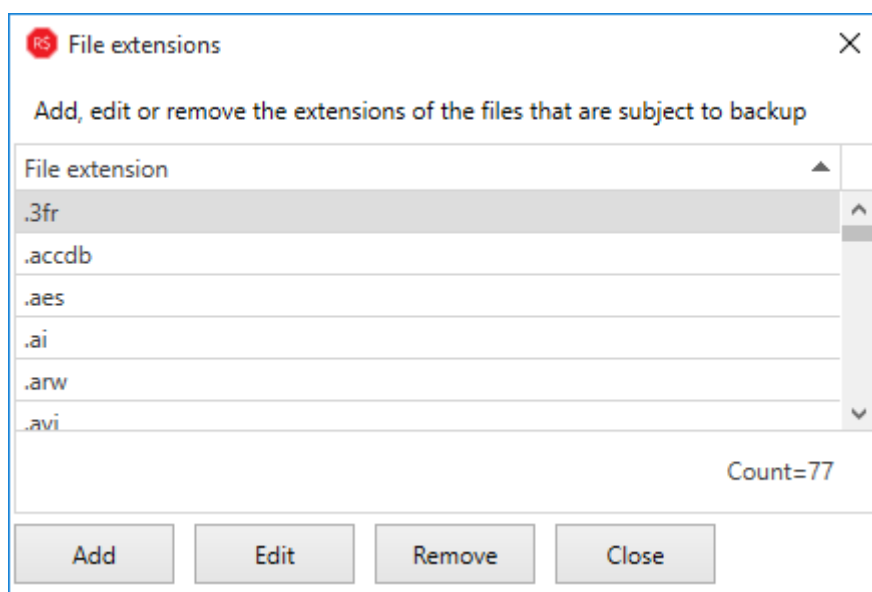


Figure 16: File Extensions dialog

Editing extensions

In the *“File Extensions”* dialog, select the extension you want to edit and click the *“Edit”* button. Make the desired changes and click *“Save”*.

Removing extensions

You can remove extensions from the list by selecting the desired extension and clicking the *“Remove”* button.

Manage exclusions

This option allows management of the folders to be excluded from the backup process.

Click the *“Exclude paths”* button to bring up the corresponding dialog, below.

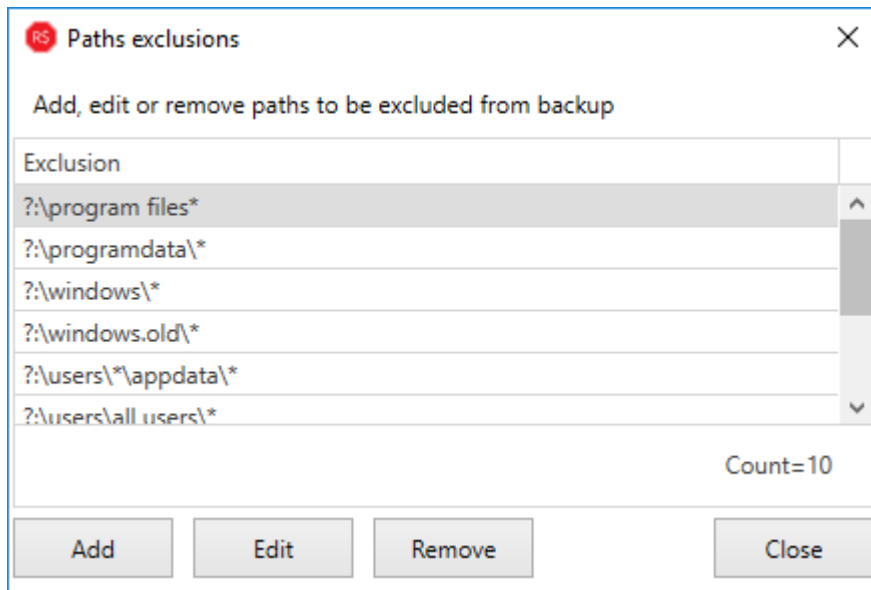


Figure 17: Backup exclusions

By default, there are several paths excluded from the backup process as can be seen in the screenshots above.

To add folders to the list of exclusions, click on the “Add” button (“Edit” if you want to edit the selected path). This will bring up the “Add /Edit” file path dialog.

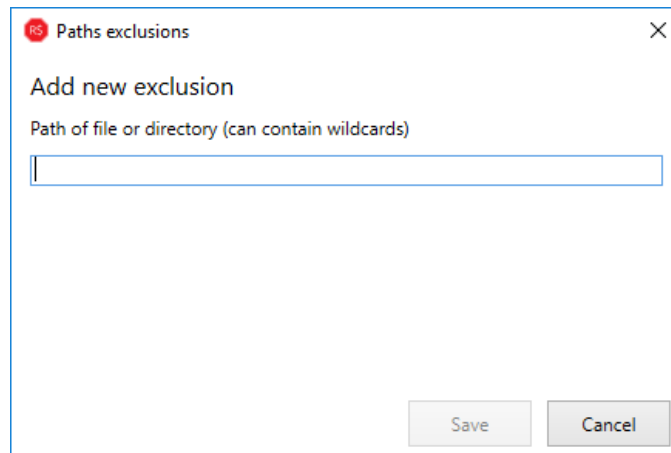


Figure 18: Add/edit exclusion

Enter the desired path in the corresponding edit box, and click “Save”. Note, the file path can be input using wildcards. The file path will be added to the list of exclusions.

Configuring the backup drive

The “Select storage drive” button allows configuring the drive to be used by Ranstop to create the backups of the user files in real time. Please note that changing this setting requires reboot.

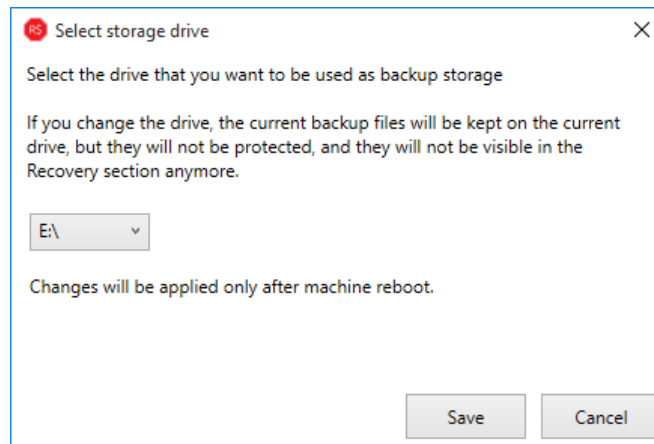


Figure 19: Select storage drive dialog

7.3 Support

The “Support” tab offers the ability to submit a support ticket from the application. Its functionality will be explained in [“Chapter 9. Troubleshooting”](#). This feature is not available in TEMASOFT Ranstop Home.

7.4 Alerting

TEMASOFT Ranstop can send email alerts when ransomware is detected, as well as when the licensing expires or there is not enough disk to backup new files. The “Alerting” tab allows configuration of the details required to send the notifications:

- The “Server name” field: enter the name of the email server;
- The “Port” field: enter the email server port;
- The “SSL” tick box: tick if the email server uses SSL;
- The “Server requires authentication” tick box: enable if you email server requires authentication (two additional fields will spawn):
 - o “Account name”: The name of the account to use for authentication;
 - o “Password”: Password to use for authentication;
- The “Email from” field: choose a text or address that will be added to the email “From” field.
- The “Email recipient(s)” field: choose the recipient(s) for the email notification.

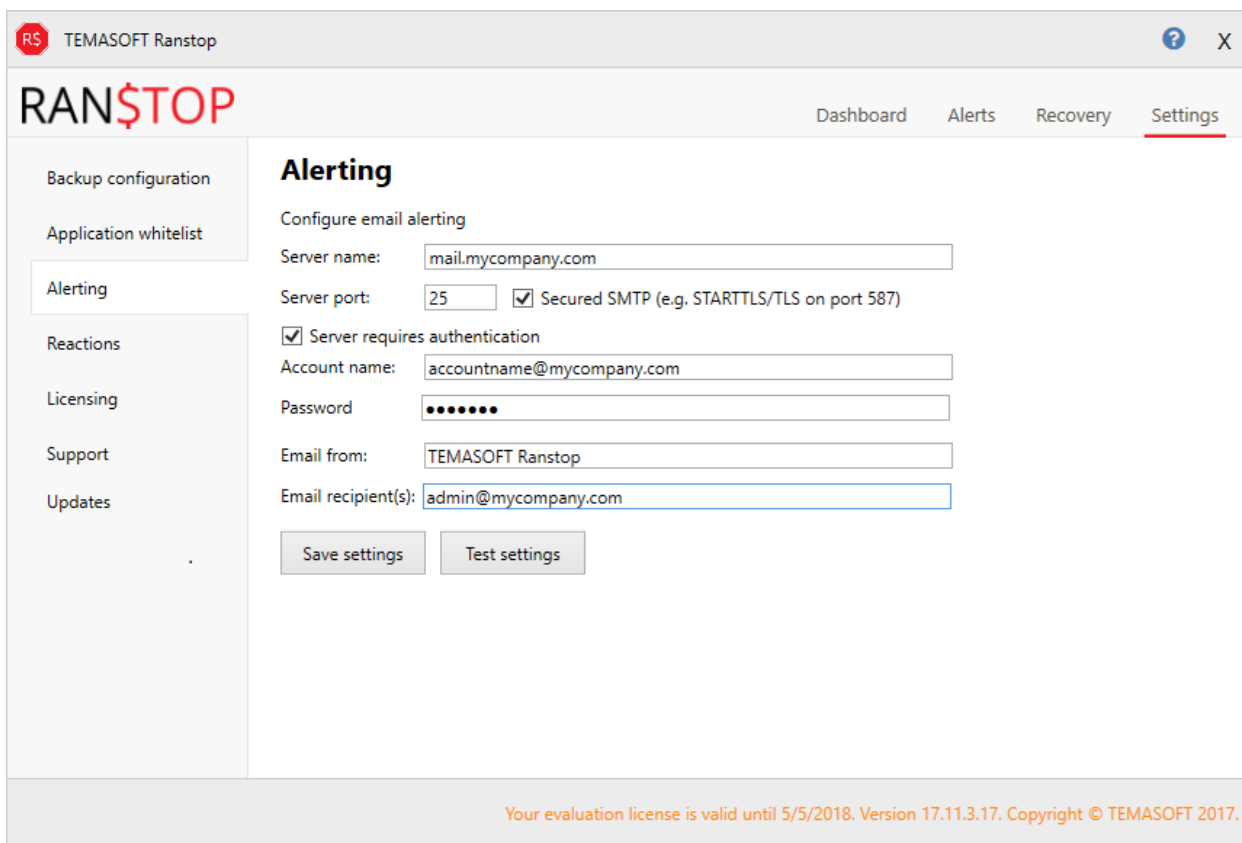


Figure 20: Alerting configuration

Once alerting configuration is complete, you can test it using the “*Test settings*” button. This function will attempt to send a test email and report on the outcome.

If the test is successful, click the “*Save*” button to save your configuration.

7.5 Reactions

The “*Reactions*” tab allows configuration of additional actions to be taken when ransomware is detected. The following options are available:

- Disable the network interfaces: TEMASOFT Ranstop can disable the network interface in order to prevent any risk of spreading;
- Shutdown the computer: TEMASOFT Ranstop can shut down the computer to prevent further risk to the files;

To configure the reactions, enable the “*Perform additional actions when ransomware is detected*” tick box, then select your desired action and click on “*Save settings*”.

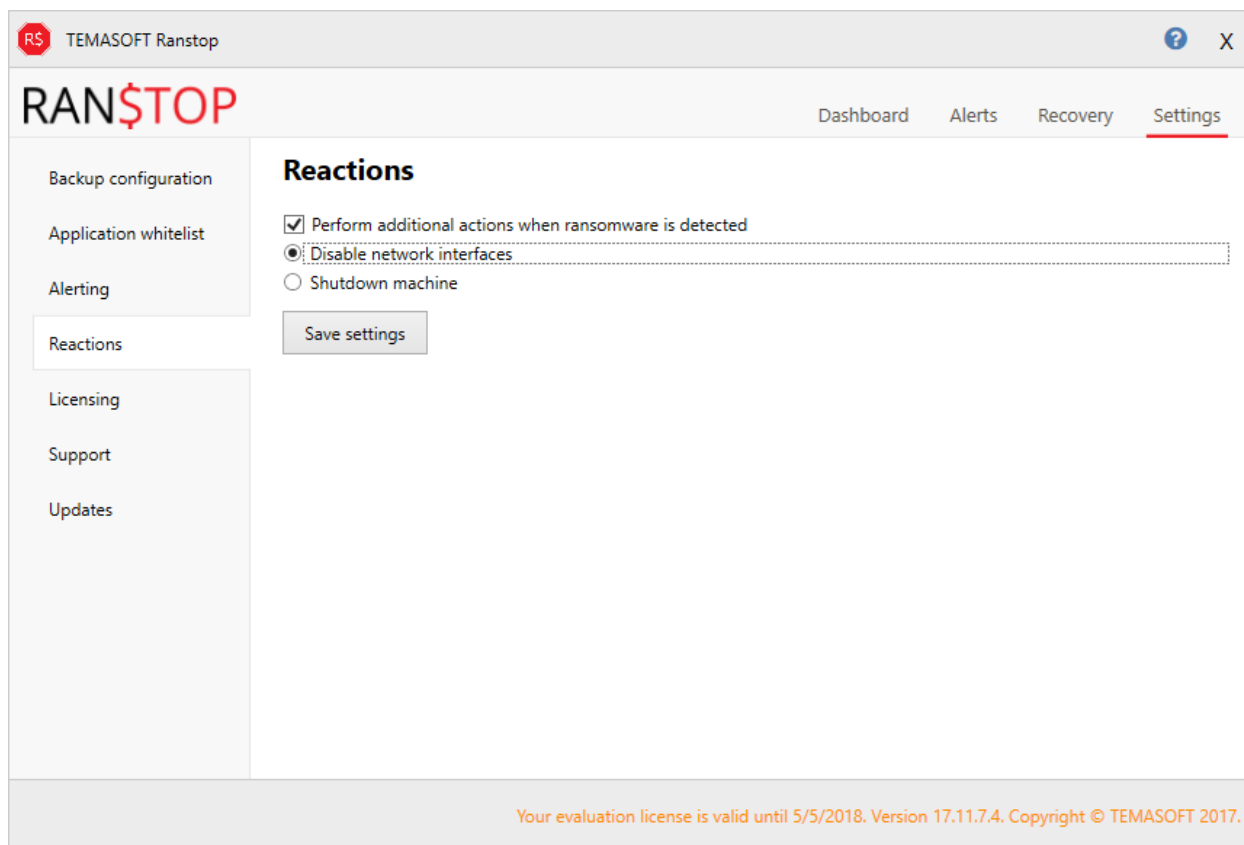


Figure 21: Configuring additional reactions

The sequence happening on ransomware detection, is the following:

- Stop the ransomware process;
- Quarantine the ransomware process file;
- Start the cleanup process;
- Send notifications;
- Trigger the reactions (shutdown the machine or disable the network interface).

7.6 Ranstop updates

TEMASOFT Ranstop features the ability to automatically detect and install new updates. This feature is configurable via the “Updates” tab in the “Settings” section of the TEMASOFT Ranstop Console.

The “Updates” tab allows users to enable or disable automatic updates using the “Auto update” check box. At the same time, it makes available the configuration of a custom URL which will be used for checking for, and downloading updates. By default, if this field is left empty, in the “Custom update URL” edit box, the product will search for updates at the following URL:

<http://ranstop.com/updates>.

In TEMASOFT Ranstop Home, there is no option to edit the updates URL. Ranstop Home will always check for updates at this URL: http://ranstop.com/updates_free.

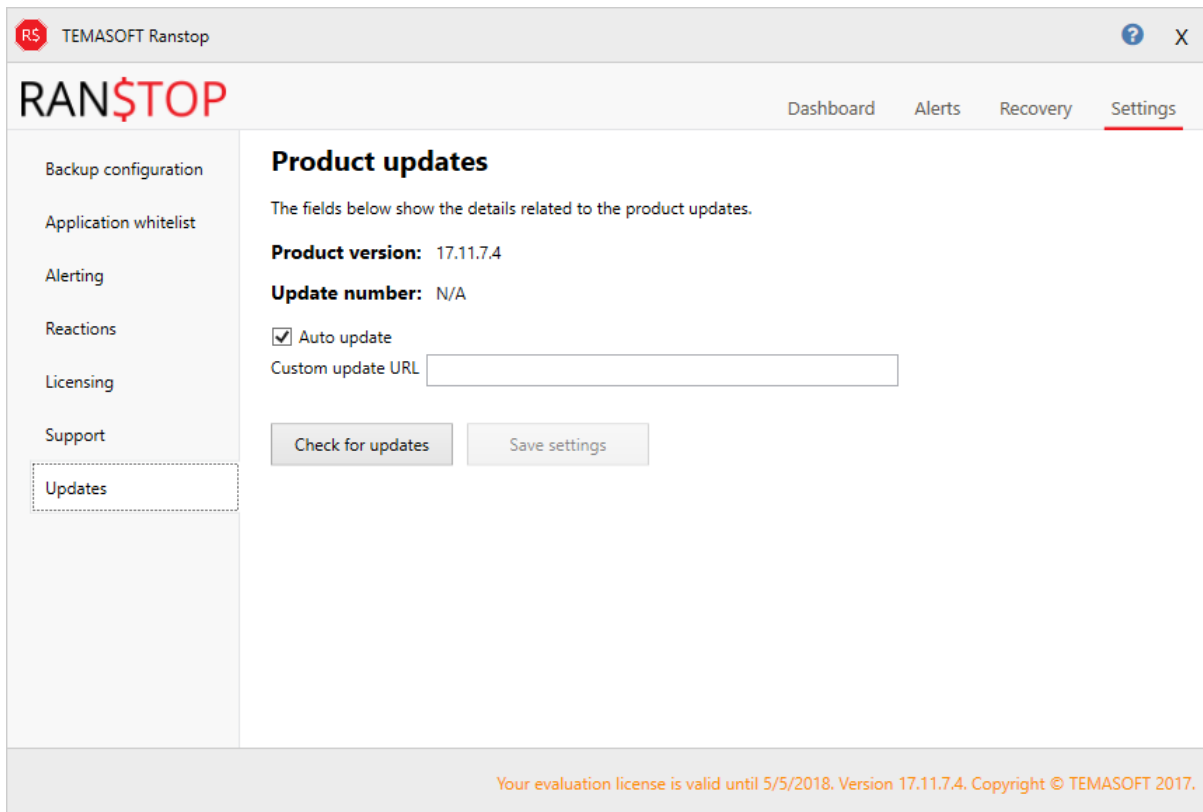


Figure 22: TEMASOFT Ranstop Updates

How does the automatic updating process work?

The check for updates runs every 10 minutes and is performed by the “FileMonitor Agent Service”. When the verification occurs, the service checks for updates at the configured URL as described above, or at the default URL. If updates are found, they are downloaded to “[System drive]:\Updates”. Next, the updates are installed as needed.

Note: if there are updates to the TEMASOFT Ranstop driver, the updating process will require a reboot. You will be notified accordingly.

8. How does Ranstop file protection work?

TEMASOFT Ranstop features an innovative real-time file protection engine that ensures that files are not lost, even in case of a successful ransomware attack. For the protection to work, you must have a licensed product.

In order to do that TEMASOFT Ranstop performs the following:

- Immediately after install, it creates a kernel-protected hard drive zone, dynamically allocated, to the size required by the files in need of protection; The backup repository is created in conformance with the settings configured in [chapter 7, paragraph 7.2 “Backup Configuration”](#). (initially with the default values)

- On every file change of the user files (configured via the main console, as per [chapter 7, paragraph 7.2 “Backup Configuration”](#)) it creates a backup copy of the file being changed in real time. Up to four file versions are kept.

TEMASOFT Ranstop also protects files residing on network drives mapped to the protected computer. The backup mechanism for these files is similar to the mechanism used for the local files. Hence, in case of a ransomware incident, TEMASOFT Ranstop is able to restore files on the network to a local repository. By default, protected network files are restored to the “%repository drive%\restore” where “%repository drive%” is the drive configured as described in [chapter 7, subchapter 7.2 “Backup configuration”, the “Configuring the backup drive” paragraph](#).

Recovery:

- On ransomware attack detected and stopped:* TEMASOFT Ranstop automatically identifies and recovers those files which have been compromised by the ransomware from the moment it executed, to the moment it was blocked by TEMASOFT Ranstop.
- On hypothetically successful ransomware attack:* In this case the user manually recovers the lost files via the TEMASOFT Ranstop Console;
- On accidental file loss:* In this case, the user manually recovers the lost files via the TEMASOFT Ranstop Console.

Recovery location

The local files will be restored to their initial location if its corresponding drive is still available (e.g. removable disks are still mounted) and enough space exists. Otherwise, users must manually restore the files in a different location.

The network files will be restored to the “%repository drive%\restore” where “%repository drive%” is the drive configured as described in [chapter 7, subchapter 7.2 “Backup configuration”, the “Configuring the backup drive” paragraph](#).

Important: if the product is not licensed, the backup process will not take place.

9. Licensing

This section is not applicable to TEMASOFT Ransotp Home, which is freeware and does not need a license.

There are two types of license with TEMASOFT Ranstop: evaluation license and commercial license. The evaluation license is integrated by default in the installer. The commercial license is based on the OS type (Windows Server or Windows Workstation) and consists of a licensing file which must be loaded as follows:

- (Recommended) during the installation process, in the appropriate dialog, as presented in [Chapter 2.4](#);
- At any time, in “TEMASOFT Ranstop -> Settings -> Licensing”.

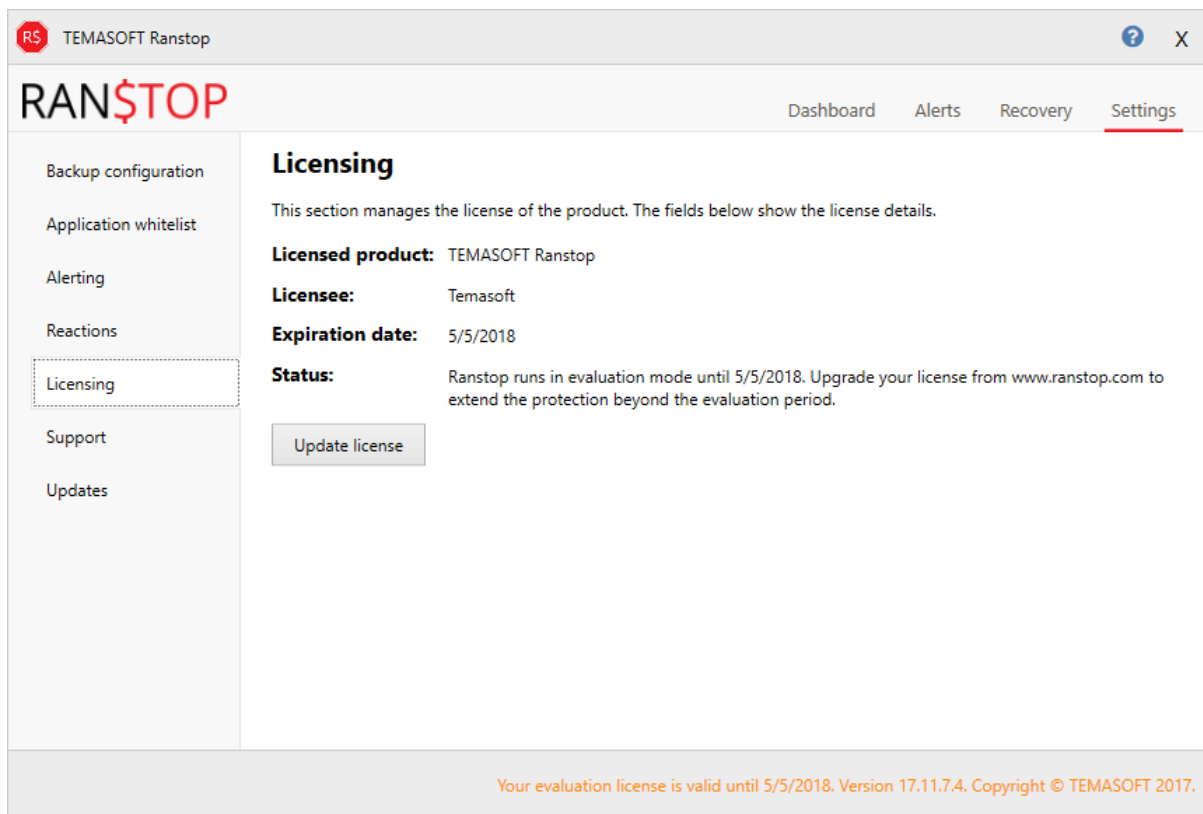


Figure 23: The licensing dialog

The licensing file is loaded by clicking on the “Load license” (or “Update license”) button. This action will open a computer browser that allows selecting the appropriate file.

When deploying in Active Directory environments, the licensing file needs to be copied to the appropriate location, as per the instructions in [Chapter 3 “Deploying TEMASOFT Ranstop in large environments”](#).

The evaluation license

The evaluation license is valid for 15 days and delivers all the functionality of the product. When the evaluation license expires, the protection is deactivated. To avoid this situation, a commercial license needs to be loaded during the evaluation period. At the same time, an extension of the evaluation period may be requested by registering on the TEMASOFT website.

The commercial license

This license is valid for one year, for the number of computers specified in the licensing file. Upon expiry of the license period, the user is notified via email. The license for a server computer is different than the license for a workstation computer. Hence, each licensing file encodes the number of licensed servers and the number of licensed workstations.

If Ranstop is deployed on a Windows Server computer, a Server license file is needed, otherwise a Workstation license file is needed.

Activation

The commercial license requires activation, which takes place automatically, provided that the machine is connected to the internet. In case the machine is not connected to the internet, the product needs to be activated manually by sending an email to support@temasoft.com.

The activation needs to take place within 30 days from when the product has been licensed.

Once activated, a license is tied to the machine where it is activated. The process is not reversible. In general, to use Ranstop on more machines, you need more licenses. Please note that there is a tolerance level (e.g. for certain licenses we allow a bit more activations than the purchased quantity) to cover for situations where hardware is changed for a licensed machine. In this case, you need to contact TEMASOFT to arrange for new license activation.

10. Troubleshooting Ranstop

This chapter describes how to troubleshoot TEMASOFT Ranstop. This feature is not applicable to TEMASOFT Ranstop Home, which does not benefit from any technical support.

10.1 Troubleshooting the uninstall process

If during uninstall you receive an error like the below, then a TEMASOFT Ranstop component has not closed in time. If that happens, please follow this procedure:

- Reboot the machine;
- Attempt to uninstall again using the “Programs and Features” or “Add/Remove Programs” panels.

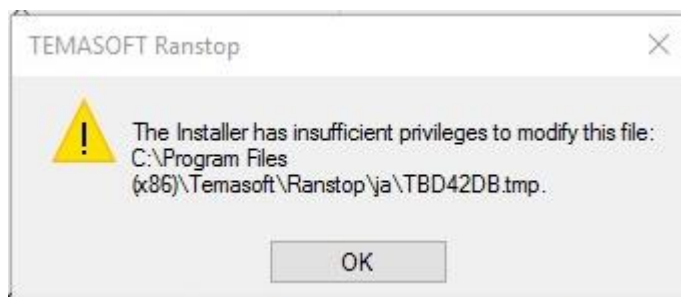


Figure 24: Uninstall error message

10.2 Running process checklist

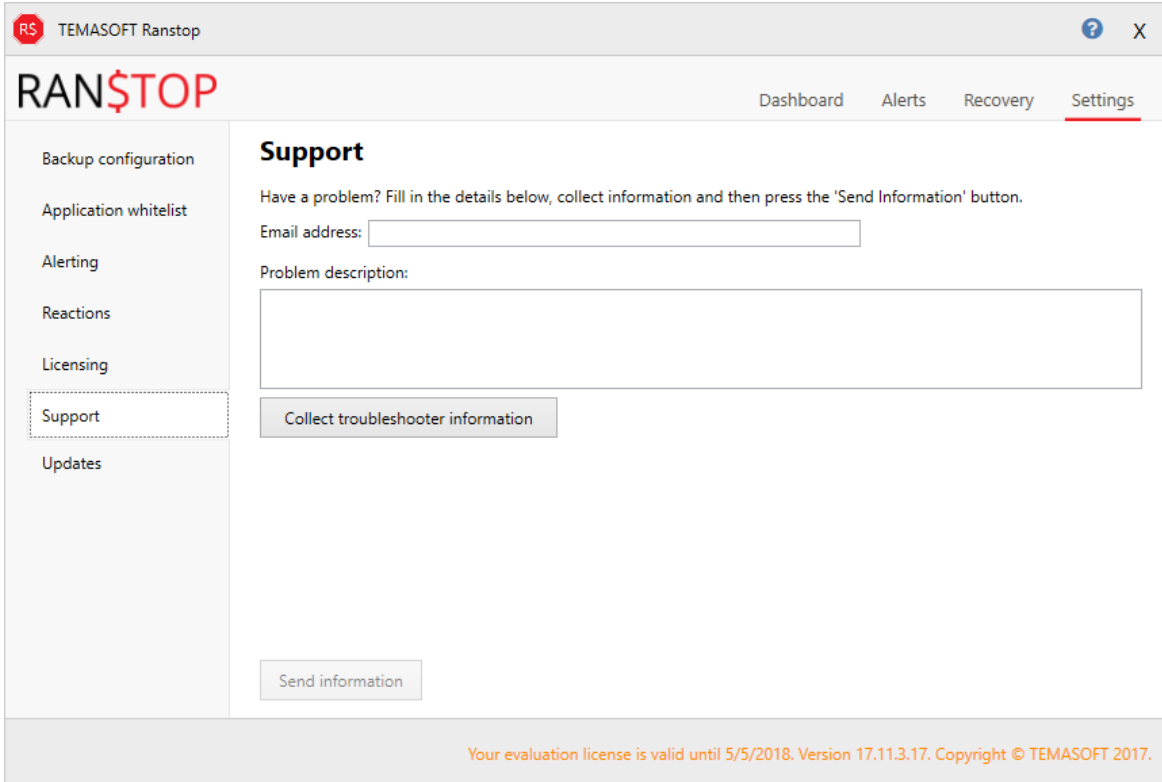
When you experience issues with TEMASOFT Ranstop, please verify that the following services and processes are started:

- Processes: right click the task bar and select “Task Manager”, then click on “Details” and go to the “Details” tab. Verify if the following processes are running:
 - o *Ranstop.exe*;
 - o *AgentService.exe*.
- Services: in the “search” box, type “services.msc”. Verify if the “FileMonitor Agent” service is running and make sure that startup is set to “Automatic”.

10.3. Contacting TEMASOFT Support

To contact TEMASOFT Support, please use the “Support” tab in the “Settings” section of the main application. Please fill in the required fields:

- Email address: the email address you want to use for communications;
- Problem description: a description of your issue;
- Click the “Collect troubleshooter information” button in order to collect logs and system information;
- Once the collection process is ready, click the “Send information” button.



The screenshot shows the TEMASOFT Ranstop application window. The title bar reads "RS TEMASOFT Ranstop". The application has a sidebar on the left with the following menu items: Backup configuration, Application whitelist, Alerting, Reactions, Licensing, Support (highlighted with a dashed border), and Updates. The main content area is titled "Support" and contains the following text: "Have a problem? Fill in the details below, collect information and then press the 'Send Information' button." Below this text are two input fields: "Email address:" followed by a text box, and "Problem description:" followed by a larger text area. There are two buttons: "Collect troubleshooter information" located below the problem description field, and "Send information" located at the bottom of the main content area. At the bottom of the application window, a status bar reads: "Your evaluation license is valid until 5/5/2018. Version 17.11.3.17. Copyright © TEMASOFT 2017."

Figure 25: Contact TEMASOFT Support dialog

Alternately, you can contact TEMASOFT Support at support@temasoft.com.