Returnil System Safe
2011 User Manual

English version

Returnil System Safe 2011 User Manual: English version

Table of Contents

Overview

What Makes Returnil's Technology Unique?

Intro

Returnil System Safe is totally integrated, intelligent layered security for your computer or network. Combining Instant System Recovery with antimalware, anti-execute, and system restore functionality, the product provides a level of protection in a single, high performance solution that is designed to reduce your security costs while providing a higher level of security protection than can be achieved using multiple programs.

Utilizing its powerful virtualization technology, Returnil's products allow you to work on a copy of the operating system of your computer, thus facilitating the possibility of keeping your real operating system in an unchanged, preserved, hence safe condition. With Returnil's virtualization feature turned ON, you can renew the working-copy of your operating system from the original as many times as you want, or need to, by just simply restarting your system. Additionally, you can create a virtual storage disk within your computer where you can save documents, data, and files while using the Virtual Mode feature. Using the File Manager utility, you can choose to pick and save any changes you want to your real system (this feature is only available in the Paid versions).

So what does this all do?

- The **Virtual Mode** feature is the Instant System Recovery component that clones your real system partition (usually the C:\ drive) and prevents changes from being made to the real system. In other words, Virtual Mode presents Windows with a fantasy world where anything can happen, and like a dream, is gone at computer restart; leaving your computer clean. This feature can be used in two ways:
  - **On demand**: Some users will leave the feature off and activate it when they are engaged in risky behavior (surfing the dark side of the internet, malware research, opening a website you are not certain of, etc). In this mode, it is called Session Lock where the virtualization is on only until the computer is restarted. To enable it, you do not have to restart so it functions as a "panic button" in a way.
  - **Always on**: This is the most secure, but the user needs to make some adjustments in how they use their computer and save files and data. With all changes to the system partition being lost at restart of the computer, it is true that work, files, pictures, etc saved in areas like Documents, Pictures, Downloads, etc would not persist following said restart. For this reason, it is recommended to change your other program settings to save their output and data on a non-system drive or partition. **So what is a non-system drive or partition?**

    Examples:

    - Data Drive D:\
    - USB drive E:\
    - Optical CD/DVD+_R drive F:\
    - External drive or IEEE drive G:\
    - Virtual Drive Z:\: Our software provides a convenience feature called the Virtual Drive for those who do not have access to a non-system drive (in other words, you only have a single a C:\ drive) without the need to partition your hard disk. It creates a large, empty file with special properties that makes Windows believe it is an actual drive. When opened (mounted), you can use it like any other drive, and files saved within it will remain following a restart of your computer with the Virtual Mode activated.

- **Antimalware**: The product ontains a fully functional antivirus and antimalware component that is designed to incorporate both local signatures and policies, but also takes advantage of our powerful cloud based AI/machine learning technology to improve zero-day detection and remdiation of malware on your system. Further, the cloud based analysis helps to reduce false positive and negative detections.

- **Anti-execute**: HIPS solutions are powerful, but often fail due to complex and/or cryptic wrning messages that the user cannot understand or react to properly. This is why we have worked to reduce the decision to only a few choices that either allow or not allow programs and services that do not already exist on your system to run. In other words, if the product does not know the program that is trying to start, it will be blocked and provide you with protection from installation and activation of malicious or potentially unwanted programs.

- **System Restore**: While the Virtual Mode component enables you to simply restart your computer, we realize that it might not be used 100% of the time, depending on the requirements of the user. This is why we have included the System Restore component that will allow you to restore your computer to an earlier time and/or repair damaged system files with a few quick clicks of your mouse.

  In future versions of Returnil's software, this feature will be upgraded to include the all new **Returnil Multi-snapshot** engine which provides support for creating, storing, and recovering to multiple snapshots of your system automatically.

  ### Note

  The virtualization software and the all new Returnil Multi-snapshot Utility are designed to be integrated and as a result, work well together on the same computer. For those interested in our technology and approach to security are encouraged to give the RMS Utility a try and let us know what your think.

  Potential uses include:

  - Recovering your system to an earlier time in the day
  - Testing a new program across restarts of your computer
  - Peace of mind knowing that you are covered!

Returnil's protection concept is very easy to understand. It provides an impenetrable, yet extremely simple to use mechanism to prevent unwanted or malicious changes from being made to your supported Windows® Operating System and the drive where Windows® is installed. You operate a copy of your system in a virtual environment, so anything you do will happen in the virtual environment (to the copy) and not to the real operating system. If your computer is attacked or gets infected with malware, you can block it from starting, detect it before it has a chance to infect your real or virtual systems, and/or restart your PC to erase all changes induced by it. Once restarted or restored to an earlier time, the working-copy of your system is renewed, enabling you to go on working as if nothing ever happened.

When the virtualization protection is OFF, you can install or remove programs, save documents within the Windows® disk drive, install security upgrades and software patches, alter configurations, and update user accounts. All changes made will remain following a restart of the computer.

Returnil's products are designed to take the risk and worry out of exposing your computer to all types of malicious software, downloads, websites, or any accidental unwanted changes that might have adverse effects on it, or infect it with harmful viruses, spyware and other malicious programs.

How does Virtualization fit into my overall Security?

Layered approach - A true layered approach to security is based on the following principles:

Prevention: The most obvious examples of this are your Firewall, Separation of programs and data storage, Microsoft® Security Updates, Email Filters, Internet content scanners, parental controls, User Account Control, EXE and program control, Policy, Best practices, and even Obscurity to some extent.

Detection: This is provided by your Antivirus, Antispyware, RootKit scanners, Antimalware, and integrity checkers.

Cure: Enforcement of clean machine state with Virtualization.

You try to keep the content from infecting your system, yet you are still getting infected; why? This is because prevention and detection/removal methods are incapable of enforcing a desired state. Be this because the rules were not strict enough, your antivirus is not updated to detect or properly remove the content, or even if your Operating System is vulnerable to a previously unknown exploit is irrelevant; the fact remains that you can never be entirely certain your security will protect you!

Returnil's virtualization products close this gap in your security, period. By cloning your System Partition, the software ensures that unwanted or malicious content is not able to make the changes it needs to make to the portion of the hard drive where Windows is installed in order to infect your system. This in essence provides a LONG TERM CURE by maintaining a clean computer rather than trying to block or chase malware around your system.

Features

- Keeps your system safe when connected to the Internet
- Viruses, Trojans, Worms, Adware, Spyware, Keyloggers, Rootkits and unwanted content disappear with a simple reboot
- Enforces settings and protects your Internet privacy
- Helps reduce overall disk wear by copying and operating your system from memory rather than the hard disk
- Saves time and money by considerably speeding up the system
- Reduces or eliminates the need for routine disk de-fragmentation
- Leaves absolutely no traces of computer activities
- Eliminates the dangers of evaluating new software
- Seamless integration with supported Windows Operating Systems
- Easy to use, simple to configure, and the one tool in your arsenal that will be there to save the day when all else fails
- Returnil's virtualization products are your last "line of defense" against malicious software

Why Use Returnil's products?

The Early Days

From the earliest days of Malware research it was known that signature based solutions would be at best, a stop-gap approach to true system security and system integrity protection.

The technology was widely accepted and, in the early days at least, was adequate to address current threats. As the Malware developers became more sophisticated, the gap began to dwindle quickly and

in time has turned 180 degrees in favor of these same developers. Where the security industry once held the advantage over their malicious adversaries, they became complacent with too much faith in the efficacy of brute-force detection and removal methods that have done nothing to stop, or even slow malicious content development.

Returnil's Solution

This is why we at Returnil continue to develop better mousetraps. To this end we quickly decided that the best way to address the growing threats was to take a risk and explore ways in which the security could become proactive. The good news is that we have acheived it with the all new Returnil System Safe, Returnil Virtual System, Returnil Multi-Snapshot, and integrateable SDK line of products. Not only do you have the peace of mind knowing that malicious changes can be removed with a simple restart of your computer, our technology spans:

- Antimalware protection on the client with cloud based analysis
- Artificial Intelligence and advanced machine learing
- Anti-execute: either you allow programs to run as they will or you block what is not already known
- System Recovery: restore damaged files or your entire system to an earlier period of time with a few simple clicks
- Fully integrated components with superior performance

Returnil System Safe is a culmination of years of research and experience that provides you with real, long term protection while lowering your overall security costs. Don't be fooled by pretenders, Returnil is the real security!

Chapter 1. Installation

System Requirements

Supported Windows® Operating Systems

(all 32-bit / 64-bit systems)

- Windows XP (service pack 2 and higher)
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Supported Hard Disk Drive configurations

- ATA
- IDE
- SATA
- SCSI
- SSD
- Raid 0
- Raid 1

Supported Windows® File Systems

- FAT32
- NTFS

Recommended hard drive requirement

- Minimum 2*RAM (or 16GB) of free disk space on the system disk is required to start using the Virtual Mode feature
- Minimum 100 MB of free disk space on system disk is required for installing the product

Minimum System Requirements by OS

- **Windows XP (service pack 2 and higher)**
  - CPU: 300 MHz or higher
  - RAM: 128 MB

- **Windows Vista**
  - CPU: 800 MHz or higher
  - RAM: 512 MB (without Aero® desktop)
  - 1 GB (With Aero® desktop)
- **Windows Server 2003**
  - CPU: 750 MHz or higher
  - RAM: 128 MB
- **Windows Server 2008**
  - CPU: 1 GHz or higher
  - RAM: 512 MB
- **Windows 7**
  - CPU: 1 GHz or higher
  - RAM: 1 GB

Pre-requisites

Disk defragmentation

- **Windows Vista and 7**
  - **Deactivate automated defragmentation**. Both Win Vista and Win 7 have a redesigned disk defragmentation feature that is configured for automatic by default during the original installation of the Operating System. While this is a useful feature for many users, it can cause file damage when using a virtualization solutions such are Returnil's products. We have addressed this issue by blocking any attempt to perform a disk defragmentation while our products virtualization feature is activated regardless of whether it is Windows itself, or a third party defragmentation solution. As this type of feature is redundant while using Returnil's products, we highly recommend that the user deactivate automatic defragmentation settings in Windows and/or any third party defragmentation solution they may be using. To do this in Windows Vista and Windows 7:
    - Click START > Control Panel > System and Maintenance > Performance and Information Tools > Advanced Tools > Open Disk Defragmenter > "Continue" when challenged by the Windows User Account Control feature (UAC) > UNCHECK the "Run on a schedule (recommended)" option > And then Click "OK" to save your new setting
  - For third party defragmentation programs we refer you to your program's user manual for the proper deactivation instructions
- **Windows XP**
  - No additional instructions are required for this Operating System as automated defragmentation is not configured as a default setting. If you are using a third party defragmentation solution however, automated defragmentation should be deactivated as indicated for Windows Vista and 7
- **Windows Server 2003 and 2008**
  - Network Administrators are encouraged to review their configurations and ensure that automated defragmentation is deactivated

Clean System

While some of Returnil's products now include an antimalware detection and removal feature, we highly recommend ensuring your computer is free from malicious and potentially unwanted software before you begin the installation process.

A defragmented hard disk drive

Although we recommend deactivating automated defragmentation, we do recommend that you defragment your hard disk drive manually before enabling Returnil's virtualization feature to ensure that your computer operates at peak efficiency at all times. Our virtualization feature will enforce this by not allowing changes that could cause defragmentation over time, so doing this now is a good idea.

Temporarily deactivate your current security solutions during install or uninstall of Returnil's products

Some Antivirus, HIPS, and Anti-Executable programs can interfere with the proper install and/or uninstall of Returnil's products. To avoid any unexpected issues, we strongly recommend that you temporarily deactivate these programs when installing or uninstalling Returnil's products. Once the software is installed or uninstalled properly, simply reactivate your other security programs and there should not be any issues.

Note

Some imaging programs may also interfere with the proper functioning of Returnil's products so you may need to deactivate these types of programs before installing the program. Further, you may need to uninstall third party imaging programs prior to installing Returnil's products and then re-install your imaging program once Returnil's software install/restart cycle is complete to avoid potential conflicts.

Step by Step Installation

1. **Download the installation file and save it to a convenient location. (Desktop is recommended)**

   ### Note

   You should backup your data if you have not already done so. A critical component of securing your computer involves protecting your data against emergencies and unexpected circumstances (natural disaster, hardware failure, stolen equipment, etc). While Returnil's products are designed to protect your system from unwanted or malicious software and data changes, it cannot protect you from physical dangers so this would be an excellent time to learn about **data replication** (backing up your data and files) and **disk imaging** (Think of this as taking a "picture" of your disk drives as they are right now that can be used to recover from a catastrophe.)

   ### Note

   New versions of Returnil's products can be installed over older versions. Users of RVS 2008, older RVS 2010 betas or RVS Lite 2011 must uninstall their current version before installing the newest upgrade. If you are installing an upgrade over an existing, compatible version Returnil's products, the installation Quick Scan will be delayed until after you have restarted your computer if the Quick Scan option is activated.

2. **Open the file to begin the installation (by Operating System)**

   - Windows XP / Windows Server 2003:

     1. Log into a computer Administrator account

2. Double click the installation file downloaded in Step 1
3. Select the appropriate language and then click OK
4. Go to Step 3

- Windows Vista / Windows Server 2008 / Windows 7:

1. Right click the file downloaded in Step 1 and select "Run As Administrator" from the right click menu
2. Right Click "Allow" when challenged by the UAC (User Account Control) feature
3. Select the appropriate language and then click OK
4. Go to step 3

3. **Select the proper language for the installation**

4. **Product's setup welcome screen**

1. Click **Next** to continue with the installation
   - Proceed to Step 5
2. Click **Cancel** to exit the setup wizard if you do not wish to proceed. Stopping the process at this point will not harm your computer and nothing will be installed.

5. **End User License Agreement (EULA)**

1. Please read the entire text of the EULA. An important part of securing your computer is to understand the licensing terms for all programs you may want to install on your computer; and if you have not done this in the past, now is a good time to begin doing so…
2. Place a check in the box to the immediate left of the text **"I accept the terms in the License Agreement"** if you agree to the terms.

Note

You must agree to these terms in order to install the software.

3. Click **Next** to continue with the installation
   - Proceed to Step 6
4. Click **Back** to return to Welcome screen
5. Click **Cancel** to exit the setup wizard if you do not wish to proceed. Stopping the process at this point will not harm your computer and nothing will be installed.

6. **Destination Folder (Where do you want to install the program?)**

1. Keep the default installation path or click the **Browse…** button to select a different location. We suggest that you keep the default installation path, but are free to install as required, even if the installation location is not on the system partition.
2. Click **Next** to proceed
3. Click **Back** to return to the EULA screen or,
   - Proceed to Step 7

4. Click **Cancel** to exit the setup wizard if you do not wish to proceed. Stopping the process at this point will not harm your computer and nothing will be installed.

7. **Ready to begin the installation**

    1. Click **Install** to proceed

    2. Click **Back** to return to the Destination Folder screen or,

    3. Click **Cancel** to exit the setup wizard if you do not wish to proceed. Stopping the process at this point will not harm your computer and nothing will be installed.

8. **Installing the software**

    Please be patient while the installation process completes. A progress bar is provided for your convenience and no further action on your part is required at this time. **DO NOT INTERRUPT** the installation process at this point. Doing so may damage your computer or the program you are attempting to install.

9. **Click Finish to complete the initial installation process**

10. **Registration of software**

    Please register your copy of the software on this screen. By registering,, depending on what type of registration you choose (Free/Trial/Commercial), you gain access to product updates, technical support, full version of Virus Guard and Password Protection.

    The unregistered free version has certain limitations: Virus Guard and Password Protection expire in 30 days. For more details on the product differences and special offers, visit our website at: http://www.returnilvirtualsystem.com/products .

11. **Quick System scan**

    Our software includes all new antimalware detection and removal capabilities that will not interfere or conflict with your currently installed antivirus and/or antispyware solutions. The Quick Scan is implemented before you restart the computer as it is essential to ensure that your system is clean before using the product.

    Perform Quick System Scan:

    1. If you are sure that your system is clean, simply uncheck the **"Perform quick system scan"** option and click **Next** to restart your computer and complete the install of the software **OR**

    2. Leave this option checked

    3. Data Collection Policy

        - Report anonymous information and parts of malicious programs for analysis to Returnil Research team **(Recommended)** – To ensure that your product remains effective, we need to understand not only how the program is being used, but to also provide behavioral analysis and sample collection that will help us harden Returnil products against attacks faster. This is not required to use the program.

        - Ask me for approval when parts of a malicious program are required for analysis – Selecting this option will force the product to seek your approval before any information is sent to our servers. Saying "no" will cancel the communication.

        - Do not collect and report any malicious activity – Selecting this option will terminate data collection.

    4. Click **Next** to activate the scan before your computer restarts to complete the installation.

12. **Scan complete (If scan option activated)**

    1. Click **Next** to proceed

    2. Click **Cancel** to exit the setup wizard if you do not wish to proceed.

13. **Finish**

    1. Click **Finish** to complete the installation process and then select one of the two choices when asked to restart your computer

       - Click **Yes** if you want to restart your computer now or

       - Click **No** if you want to restart the computer later

       ## Note

       Returnil products will not be completely installed until you restart your computer!

Chapter 2. User Interface Overview

(Availability: All versions)

General Overview

- **Product logo**

  Clicking the Returnil logo in the upper left corner of the interface will open the the Returnil home page on our website in your default browser.

- **Product Edition**

  Displays the Edition name or product type of your copy of the software.

- **Preferences**

  Opens the configuration options screen described in more detail in the **preferences** section of this manual.

- **Help**

  Opens the included Help manual.

- **About**

  Displays program copyright and version information.

- **Registration status (lower left corner of the main interface)**

  Displays product registration and provides a link to open the product registration screen.

- **Lock/Unlock the interface link**

  Locks/unlocks access to important product configurations.

  ### Note

  Password required to lock and unlock the interface. If you do not know the password, please consult with the authorized product user/owner for assistance.

Main Features

- **Home**

  Here you will find access to messages and status of major product features.

- **Virus Guard**

  Start a scan of your computer, change antimalware settings, check the log for information about detected malware, activate/deactivate real-time and product self protection options, adjust protection and malware sample data collection policy, and manage your antimalware exclusion list.

- **Virtual Mode**

  Activate/deactivate the virtual protection, change various settings related to the virtualization such as Anti-execute and virtualization cache wipe options, use tools to define your File Manager list for trusted files, create, mount, dismount your Virtual Disk, and access sensitive areas of your real system while the virtualization feature is active using the **Access Real Disk** browser.

- **System Restore**

  Turn the restore monitor on or off, select your choice of restoration provider restore your system to an earlier time, or restore a copy of a specific system or user file.

  ## Note

  The custom Returnil provider may not be available in some versions of the software during the beta phase.

- **Status**

  Displays information about your current protection status, product version details, and licensing status for your copy of the software.

Chapter 3. Home

Overview

(Availability: All versions)

- **Protection status warning panel**
  - **System Secure**: Text in green and indicates that the **Virus Guard Real-time protection monitor** is active.
  - **System Not Secure**: text in red and indicates that the **Virus Guard Real-time protection monitor** is **NOT ACTIVE**.
- **Start Scan button**

  Opens the Virus Guard Scan screen
- "**advanced**" link

  Opens the Full Scan configurations screen to allow a full check or your computer or to perform a custom scan of selective areas of your computer.
- **Real-time protection**

Displays current status of the **Virus Guard Real-time protection monitor** with a "**disable/enable**" link on the far right side allowing you to turn the monitor on or off as required.

- **Virtual Mode**

  Displays the status of the virtual protection feature with a link to the far right side of the interface allowing you to open the **Virtual Mode Overview** screen to activate/deactivate the virtualization.

- **System Restore**

  Displays the status of the Real-time Restore Analysis monitor with a link to the far right side of the interface that allows you to enable/disable this feature.

  ### Note

  Turning this feature off will stop the program's monitoring of changes in your files and may result in you not being able to restore a damaged or missing file at a later time. We highly recommend that you do not deactivate the monitor.

- **Messages**

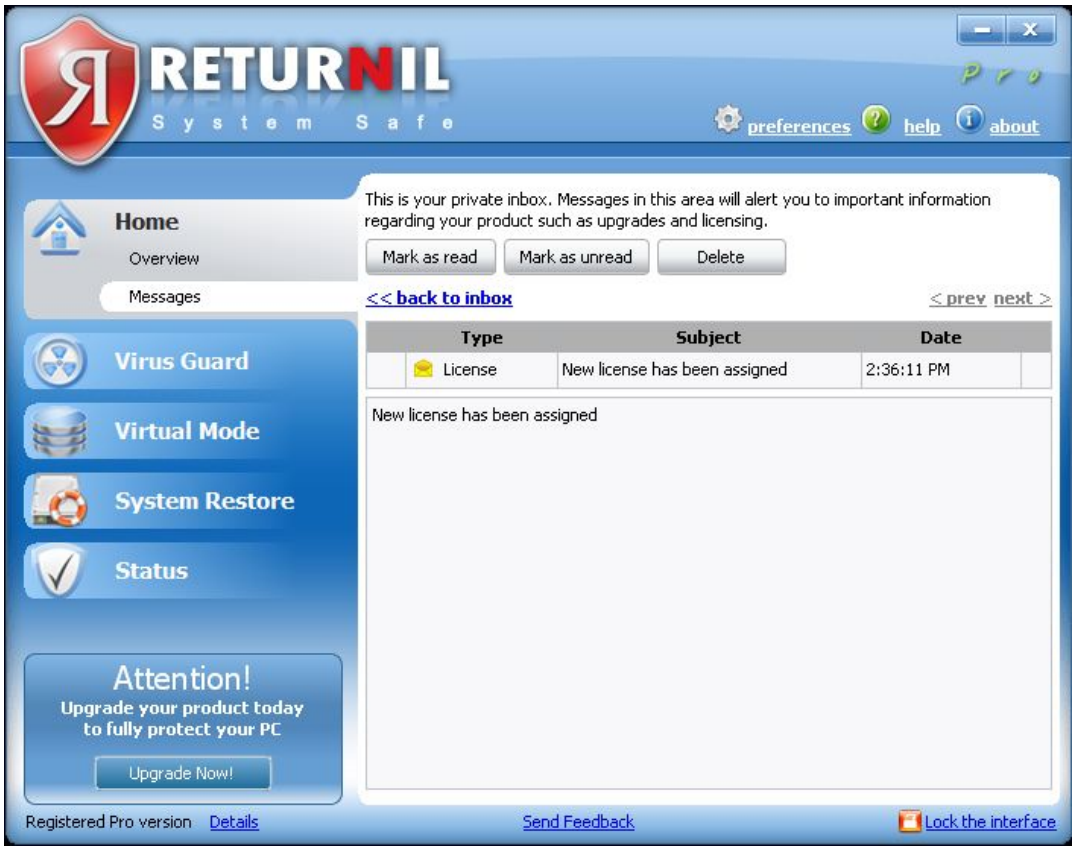
  Displays the number of unread messages out of the total number of messages you have in your queue (format: "x"/"y") with a "**read now**" link to open the Message center.

- **Expiration date**

  Displays the date your current product subscription ends.

Messages

(Availability: All versions)



- **Mark as read button**

  Select the messages you want to mark as **read** by placing a check in the box to the left of the message in the list window and then click this button.

- **Mark as unread button**

  Select the messages you want to mark as **unread** by placing a check in the box to the left of the message in the list window and then click this button.

- **Delete button**

  Select the messages you want to **delete** by placing a check in the box to the left of the message in the list window and then click this button.

- **<< back to inbox**

  Returns you to your inbox.

- **<prev next>**

  Cycles to the previous or next message in your messages list.

- **Message list**

  - **Check box**: click the box to select or deselect the list item
  - **Type**: Displays the message type

  - License: Message is related to your product licensing and registration.
  - Product: Message is related to product upgrades or offer information.
- **Title**: Displays the Title of the selected message.
- **Date**: Date and time the selected message was received.

Chapter 4. Virus Guard

Scan

(Availability: All versions)

- **Real-time Protection**

  Turn ON or Turn OFF the **Virus Guard** real-time malware monitor.

- **Quick Scan**

  Launch a quick malware scan of the most important areas associated with malware activity and content.

- **Full Scan**

  Launch a Full, in-depth or custom malware scan of your entire computer.

  ### Note

  Please be patient while the scan completes. Time to completion will vary with the size of your disks and the amount of content, data, and files they contain.

- **Protection Sensitivity slider**

This is an alternate option for changing the Real-time Protection Sensitivity of the Virus Guard scans: left (low) to right (high).

Note

The slider will override the existing sensitivity level for the Real-time Protection and Quick Scan only. For Full Scan, use the Full Scan screen to setup the scan's sensitivity.

- **Cloud Protection**

  (Availability: Paid products)

  This new premium feature is our way to reward our customers and to thank them for their continued support and loyalty. Using our all new Artificial Intelligence and Machine Learning Engine, we now offer additional malware screening and whitelist updating via our servers. Put simply, our best customers and partners receive priority service with high availability and an immediate trip to the head of the line for their computer protection.

- **View Quarantine**

  Opens the Quarantine file list.

- **AV Exclusion List**

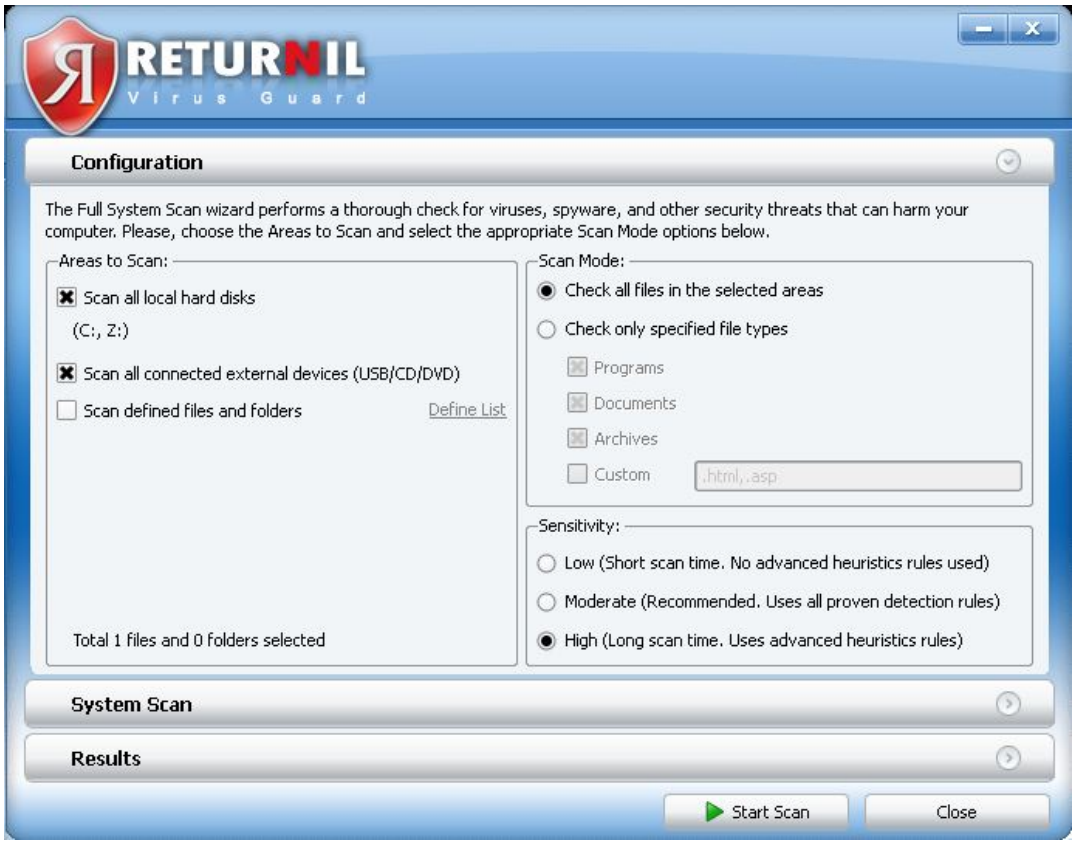
  Specify files and folders to exclude from Real-time Protection.

Full System Scan

(Availability: registered Home Free/Lux and Enterprise Premier)

Configuration Screen

Set the appropriate preferences for the full scan of your computer before you begin the scan.



- **Areas to Scan**
  - **Scan all local hard disks:** as implied. Available disks will be displayed below this option (Ex: (C:)).
  - **Scan all connected external devices (USB/CD/DVD):** as implied.
  - **Scan defined files and folders:** user-defined scanning targets.

    Define list (File and folder inclusion list): Displays a list of user-defined files and folders to be added to the scan.

    - Add File…: as implied.
    - Add Folder…: as implied.
    - Export List: Export a custom list of files and folders to be added to the scan when appropriate.
    - Import List: Import a custom list of files and folders to add to the current or future Full System Scan.
    - Update List: Saves changes you make to the custom list.
    - List info: Is the list populated?
    - List File: information about the current list file.

- OK: Click to save your current list and return to the Full System Scan Configuration screen.
- Cancel: Close the current screen without making changes. If a list is not defined, the option will be unchecked automatically on the Full Sysem Scan Configuration screen.

- **Scan Mode**
  - Check all files in the selected areas: default setting which forces the RVS Virus Guard to scan all file types.
  - Check only specified file types: as implied. RVS will scan only the types defined by the user from the included and/or custom list. List items should be added with a comma separating them. Ex: .HTML, .asp.
- **Sensitivity**

  Configure the appropriate sensitivity level for the scan

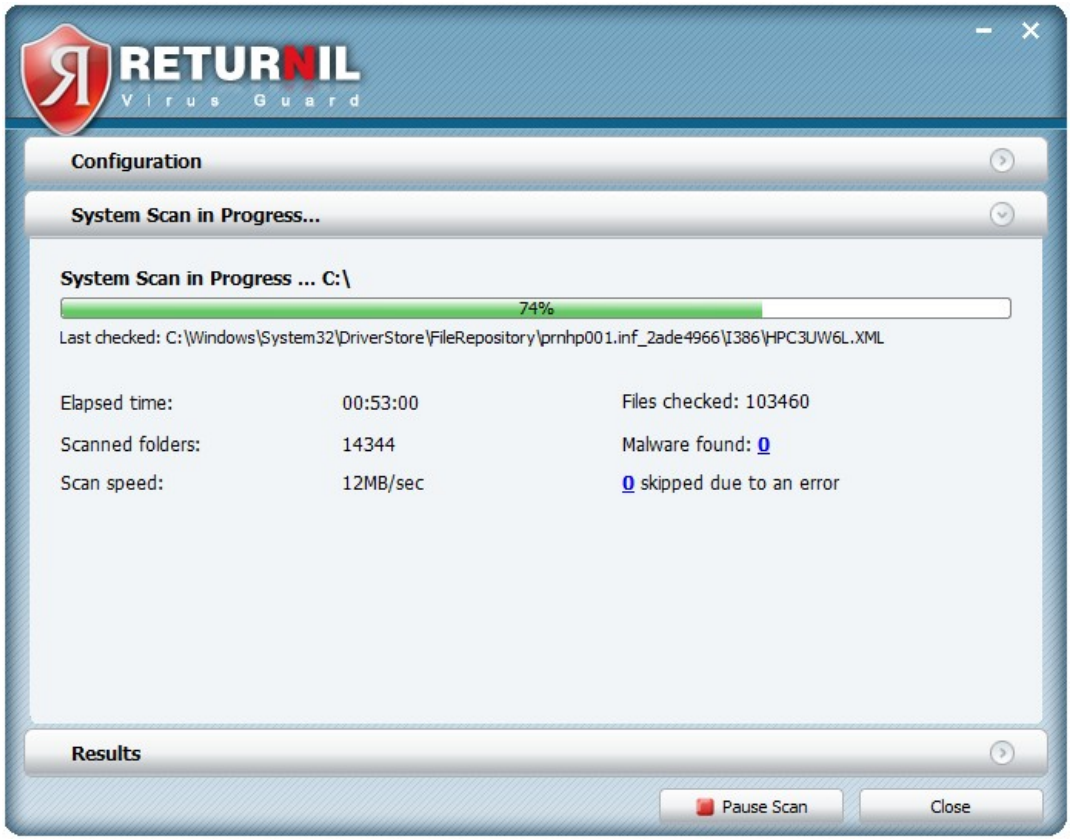
  ### Note

  The higher the sensitivity level, the more likely it will be to have a false positive detection. Please use caution and thoroughly review your scan results at the highest sensitivity level.

  - **Low (Short scan time. No advanced heuristics rules used)**: While the majority of the known malware will be detected at this level, there is a higher probability that some content may go undetected.
  - **Moderate (Recommended. Uses all proven detection rules)**: The level has the best ballance between performance and total detection efficiency and is appropriate for most users for regular full computer checkup scans.
  - **High (Long scan time. Uses advanced heuristics rules)**: this setting is most likely to detect new variants and some zero-day malware, but is also most likely to have false positive detections. Please use caution and thoroughly review your scan results before removal/quarantine when scanning the real disk.

System Scan screen (System Scan in Progress/Suspended…)

Displays active scan data.



- **Progress bar**

  Displays the progress of the current scan as well as the last file checked (includes file path information).

- **Last checked**

  Displays the path and name of the files being scanned. As the scan engine is ahead of this display, the path and file you see listed will be the one preceeding the file and area actually being scanned.

- **Elapsed time**

  Time the scan has taken so far.

- **Scanned folders**

  Number of folder scanned so far.

- **Scan Speed**

  Current scanning speed. This fugure may vary depending on the load your computer is under at any given moment during the scan process.

- **Files checked**

  Number of files scanned so far.

- **Malware found**

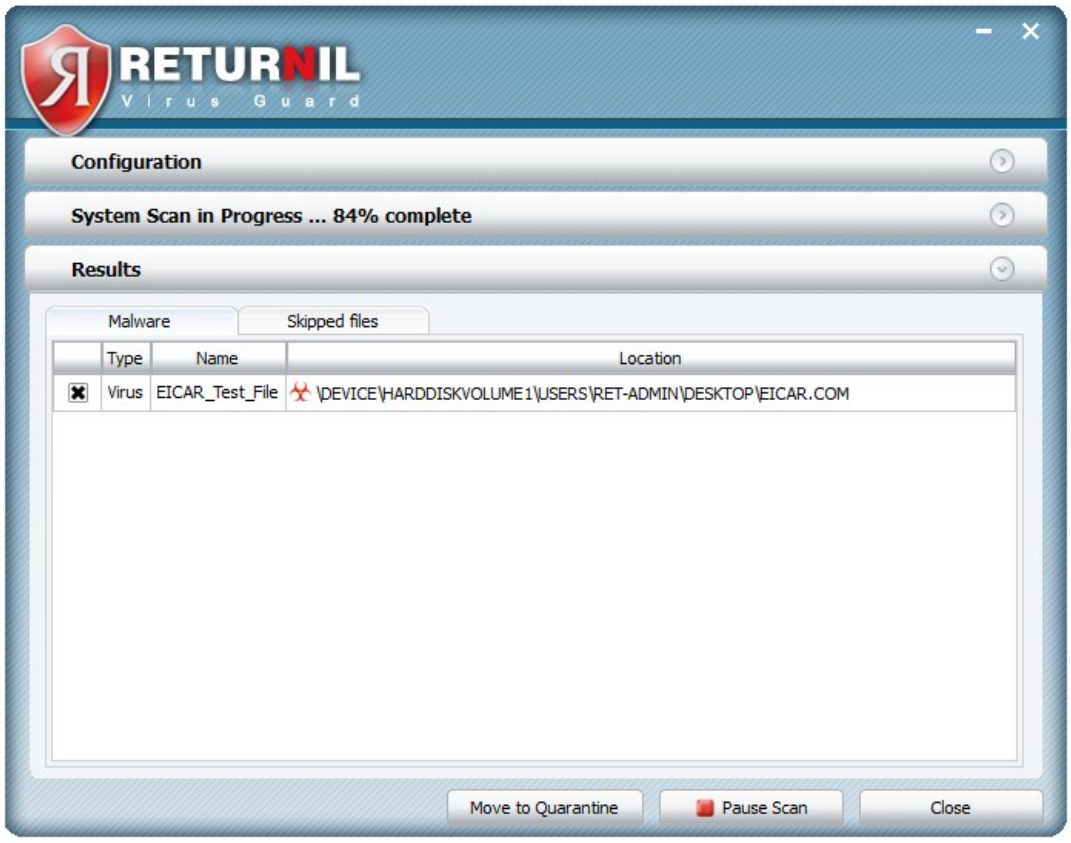
Number of infected items detected so far.

- **# Skipped due to an error**

  Number of files that could not be opened because they were in use by Windows or another program at the time of the scan. This is normal and these files are very unlikely to be infected (if the AV cannot access them, neither can malware).

Results screen

Displays the results for the current Full System Scan.



- **Malware tab**

  Displays each malicious component detected, what file type it is, what the name of the file is, and where it was found on your system.

  - **Status**: Displays the status of the specific malware found.

    - **Denied**: Means the file has been detected and blocked from executing but is still in the location where it was detected.

Note

To act on the detection, click the box to the left of the malware list item and then click the Repair button. After the file has been cleaned or sent to exile in the protected quarantine, a new box will open with a summary of the action taken.

- **Quarantined**: file has been removed and placed within a protected quarantine where it cannot harm your computer.
  - **Repair Summary screen**: will display the results of the remediation of the detected malware to be repaired.
    - **Total processed**: total number of malitious items where action has been taken (quarantined or cleaned).
    - **Errors**: number of errors (if any) encountered during the acation taken to remediate the selected malware content.
    - **Quarantined**: total number od remediated malware exiled to the protected quarantine.
    - **Restored**: total number of infected files that were able to be restored fromclean sources..
    - **Show details**: Shows the detailed statistics that relate to the summaries.
    - **Close** button: use this to close the Repair Summary screen and return to the Scan Results screen.
  - **Restored**: The file was restored to a clean state.

- **Skipped files tab**

  Similar to the Malware tab, but displays information about the files that could not be scanned and why the RVS Virus Scan was not able to access the file or device.

Actions

- **Start Scan/Pause Scan**

  As implied. A scan can be interrupted and resumed at any time during the process.

- **Close**

  Closes the Full System Scan screens and returns you to the previous screen you were on.

Quarantine

(Availability: All versions)

Displays the list of malicious files that have been removed to a secure area away from your real system and rendered harmless.

- **Date**

  Date and time the file was added to the Quarantine

Note

Files listed, but added on the same day you are reviewing the Quarantine list will only show the time the file was added. Once the date advances beyond the date it was added to the Quarantine, this section will also display the full date information.

- **Purpose**

  Displays the type of malware, its ID, and whether the detection was due to exact matching to a known signature or due to a heuristic or AI detection.

- **Name**

  Displays the original location and name of the file when it was added to the quarantine.

- **Size**

  Size of the file in Quarantine.

- **Restore**

  Restores the selected, quarantined file to its original location.

- **Restore to...**

  Restores the file to a user defined location.

- **Remove**

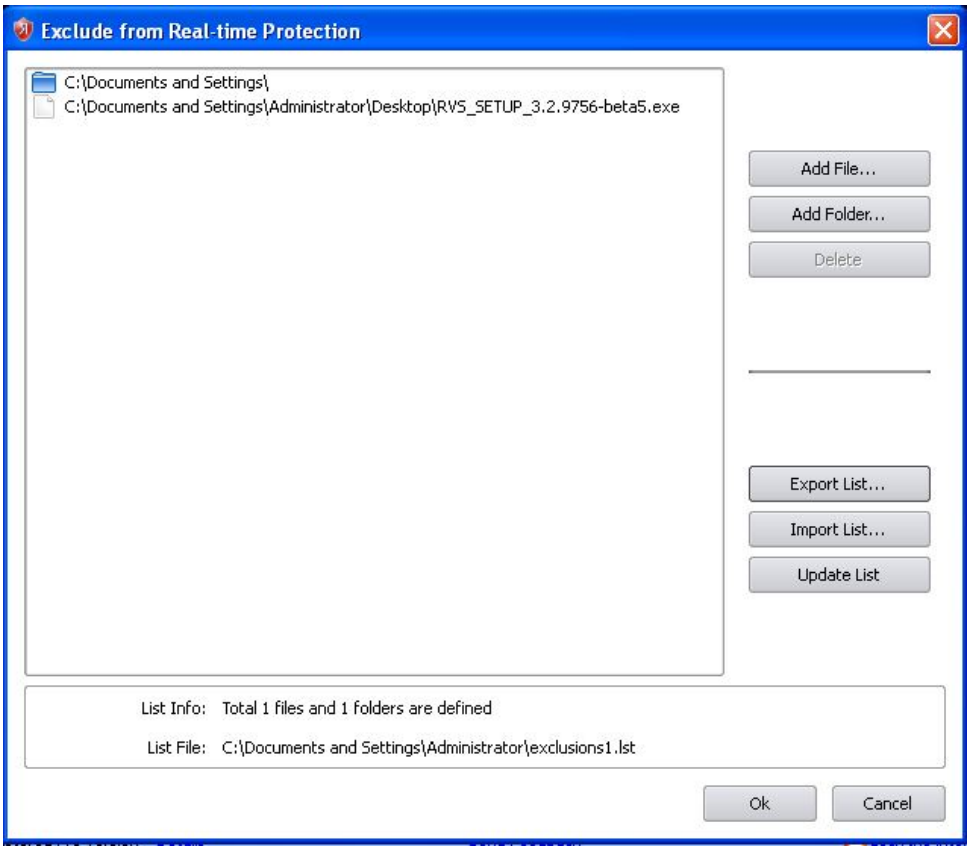
  Deletes the selected, quarantined item.

- **Close**

  Closes the Quarantine list window and returns you to the **Virus Guard Scan** screen.

AV Exclusion List

(Availability: All versions)



- **Exclude from Real-time Virus Protection**

  Displays a list of files and folders that have been excluded from **Virus Guard Real-time** monitoring.

- **Add File...**

  Select this to browse your computer to add a specific file to the AV Exclusion List.

- **Add Folder...**

  Select this to browse your computer for specific folders and even entire drives and partitions to add to the AV Exclusion List as required.

- **Delete**

  Deletes the selected list item from the AV Exclusion List.

- **Export List...**

  Exports the AV Exclusion List for backup or to create specialized scanning profiles.

- **Import List...**

  Imports a backed up or different profile list, overwriting the previous list.

- **Update List**

Updates your current copy of the AV Exclusion List when new entries are added in the **List** display window.

- **List info**

  Displays the number of files and folders in your custom Full Scan List file when defined.

- **List File**

  Displays the path and name of your saved AV Exclusion List

  ### Note

  To save a custom AV Exclusion List you must export the list.

Log

(Availability: All versions)

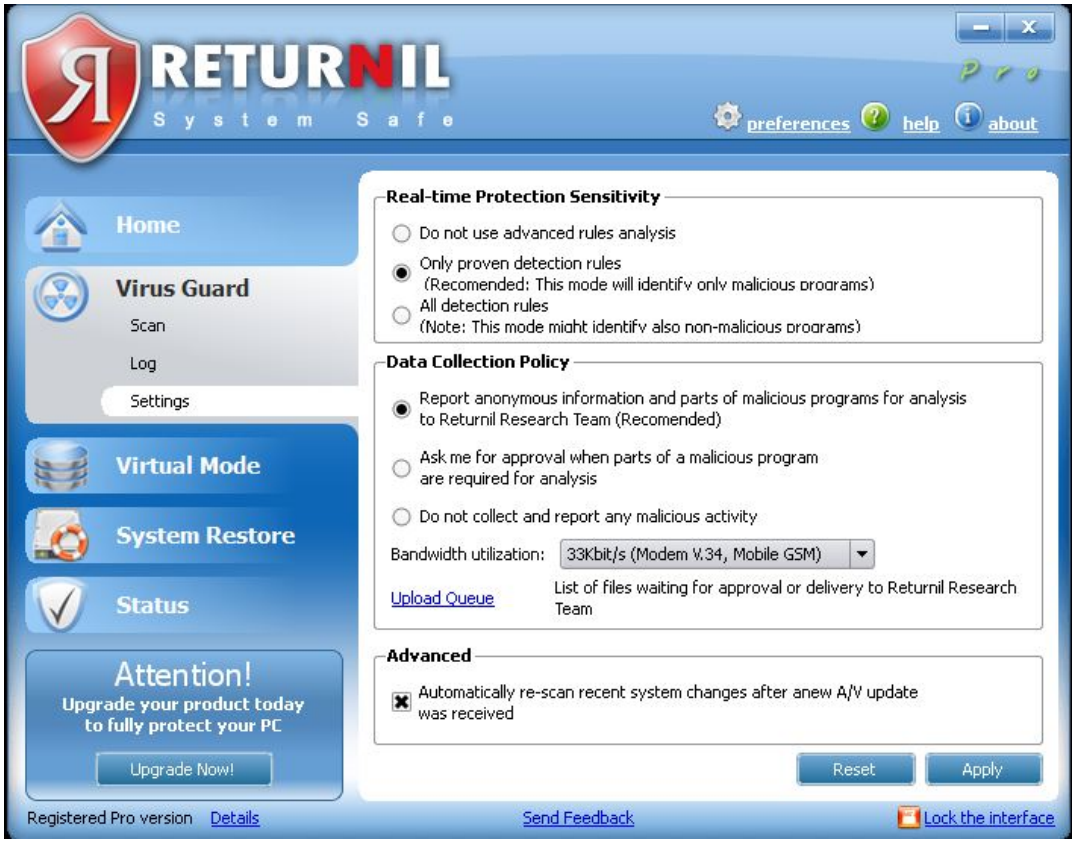
Displays a log of detected malware and its current status

- **Repair** button: Some files that have been quarantined may be repairable at a later time after a relevant signature or heuristics update/upgrade. This button allows you to periodically check to see if you may be able to repair a quarantined file or files.
- **Exclude** button: removes the selected file or files from further detection alerts from the Virus Guard Real-time protection by adding it to the **AV Exclusion List.**

- **Hide** button: removes the selected list items from the log.
- **Export**: exports the log for analysis or backup.
- **List display window**: list of detected malware.
  - **Status**: displays the current status of the listed malware (ex: Quarantined)
  - **Type**: Type of malware detected, ID, and rule used to detect it.
  - **Location**: Original location where the file was first detected

Settings

(Availability: All versions)



Real-time Protection Sensitivity

Configure the appropriate detection sensitivity for the Real-time monitor.

Note

This setting is different than the one for the Full Scan. This sensitivity settings is only for the Real time Virus Guard monitor.

- **Do not use advanced rules analysis**

Excludes the use of any advanced rules. Reduces the likelihood of a false detection or block.

- **Only proven detection rules**

  More sensitive than the preceding mode and includes well proven heuristic detection rules.

- **All detection rules**

  Highest sensitivity and also the mode with the greatest likelihood to present false positive detections.

Data Collection Policy

We need your help to help protect your PCs and networks. What this feature does is to collect information about suspicious files and behaviors that are analyzed by our Artificial Intelligence and Machine Learning Engine to update our Virus Guard and program Self protection features. It also collects information about good files and behaviors that allow greater refinement of malware detection while ensuring known good content updates via **White Listing** helps to minimize and eventually eliminate false positive detections.

- **Report anonymous information and parts of malicious programs for analysis to Returnil Research team (Recommended)**

  All data is sent to our research team automatically for analysis. No personal in formation is recorded. Our only mission and goal is to improve the detection and blocking capabilities of the Antimalware feature and deliver improved security solutions and services for our customers and users.

- **Ask me for approval when parts of a malicious program are required for analysis**

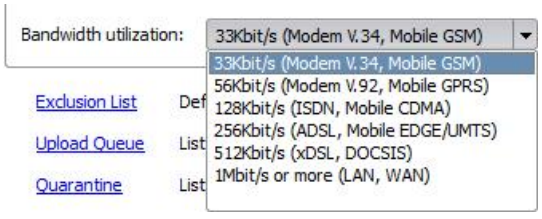
  When this option is chosen, software will send data to our servers, but only when you have given permission for the software to send this information. We guarantee that this information will not contain any personallly identifiable content. The purpose of the data collection is to improve anti-malware and anti-execute defences through server-side malware analysis, not to collect information about you or any other user of your computer.

- **Do not collect and report any malicious activity**

  Selecting this option will terminate data collection. It means exactly that: NO malicious activity information will be collected or sent.

- **Bandwidth utilization**

  Use this to configure the amount of bandwidth you will allow the program to use to send the collected malware data to our servers for analysis.

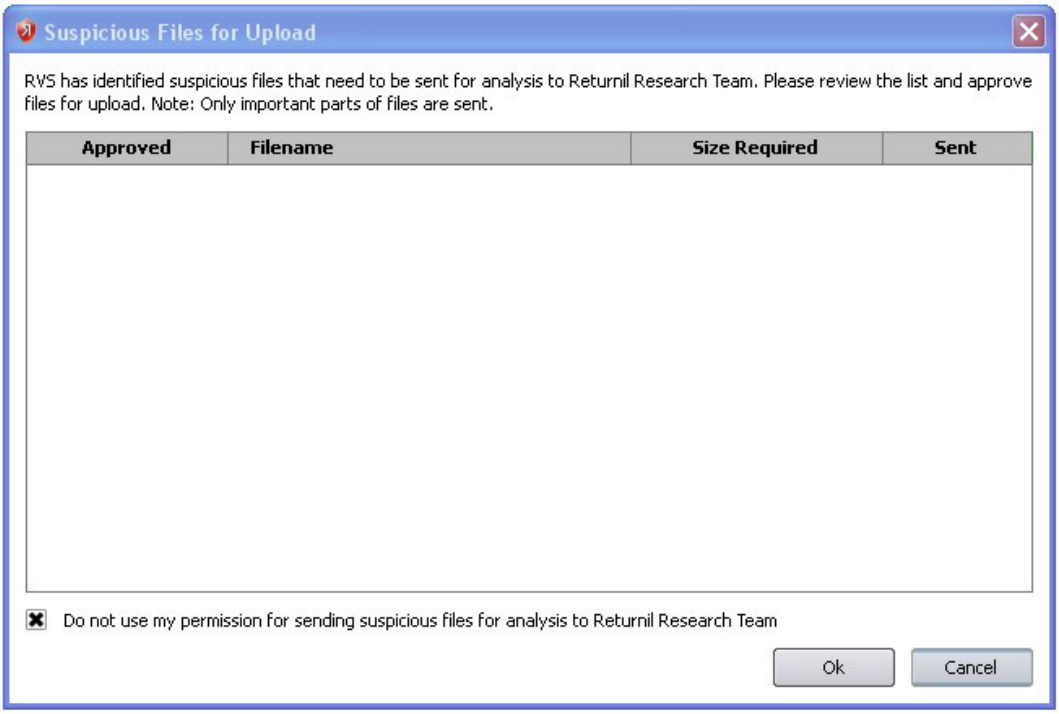


Upload Queue

Displays a list of suspicious files waiting for your approval to upload to our servers.

- **Suspicious Files for Upload screen**: displays the list of files, approval status, and other statistics.
  - **Approved**: the file has been or has not been approved for upload to our servers.

- **File Name**: Name of the file to be uploaded.
- **Size Required**: size of the file to be uploaded.
- **Sent**: the file has either been sent or is waiting to be sent.
- **Do not use my permission for sending files for analysis to Returnil Research Team**: sends files automatically without bothering the user with requests for permission to send.
- **OK** button: Saves your options and aproval decisions then closes the screen and returns you to the **Virus Guard Settings** screen.
- **Cancel** button: closes the **Suspicious Files for Upload** screen without making any changes to your options settings.



Actions

- **Reset**

  Rests all settings to their installation defaults.

- **Apply**

  Saves your settings changes.

Chapter 5. Virtual Mode

Overview

(Availability: All versions)

The Virtual Mode protection feature is the new name for our virtual protection technology and can be configured to operate manually or automatically depending on your requirements. This is the technology that protects your real system from unwanted and malicious changes.

The overview screen displays the current status of the virtual protection, allows you to activate or deactivate the virtualization, and provides convenient access to the File Manager for saving files while the virtual protection is active.

Virtual Mode button

Turns the virtualization on or off..

- **Green button displaying the text "Stop Virtual Mode"** means the virtualization is currently active and pressing the button will turn the virtualization off following a restart and deactivation of the Virtual Mode Always On option (see below)

- **Red button displaying the text "Start Virtual Mode"** means the virtualization is currently active and pressing the button will turn the virtualization on without a restart of your computer.

Virtual Mode Always On

The **virtual Mode** protection will be active at computer start.

Saving Files

Click the **File Manager** link to open the **File Manager tab** in the **Virtual Mode > Tools** section where you can add files and folders to save to the real disk when the **Virtual Mode** protection feature is active.

Tools

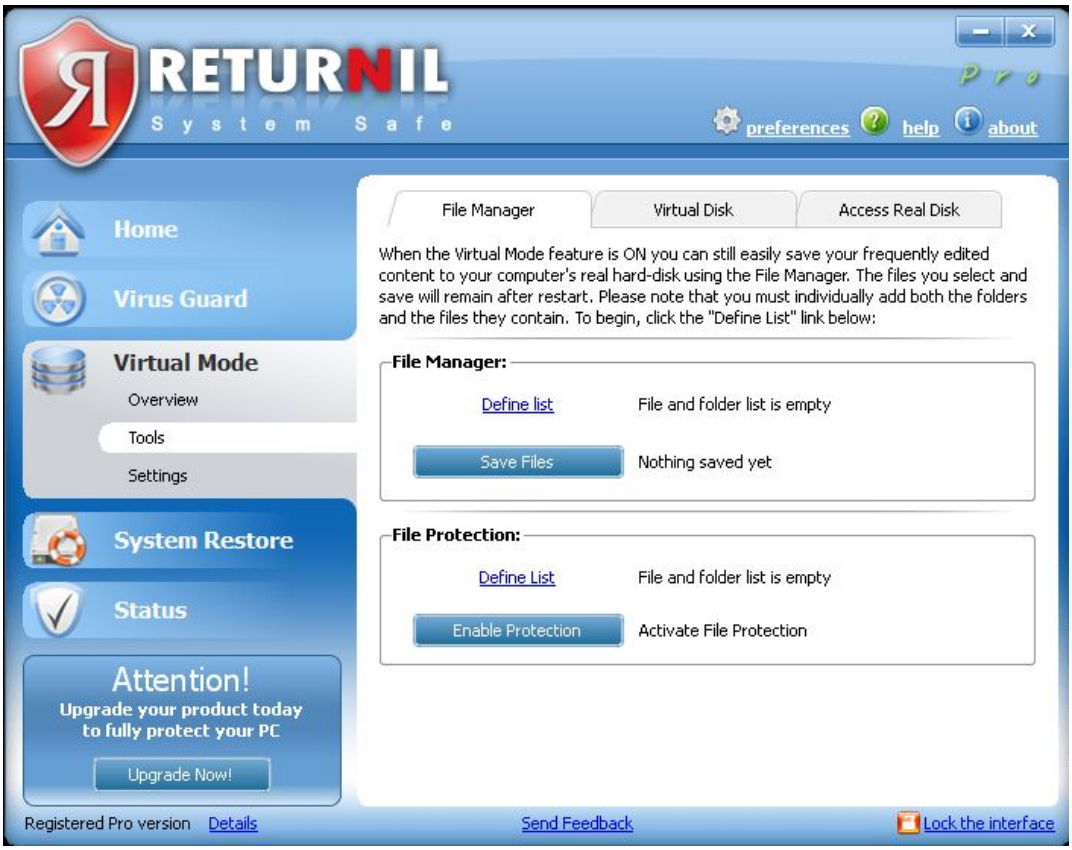
File Manager

(Availability: Paid versions)

The File Manager allows you to save a list of frequently changed files and/or folders to the real disk when using the System Safe virtual protection. Possible uses include updating a shared document on your computer, allowing an administrator to "White list" non-registry changes he/she wants to make without turning off protection on the client system, using custom lists for different situations or users, etc.

Note

The software sees files and folders as unique objects, meaning that if you want to save all the files inside of a selected folder, you must include each of the files in the list individually.



Define List

Displays the number of files and folders on your current list. Click the link to open the File Manager:

- **Main list display window**

  This is the large open space to the upper left of the screen and is where your list will be displayed.

- **Add Files(s)**

  Click to select files to be added to the list.

- **Add Folder(s)**

  Click to select folders to be added to the list.

- **Delete**

  Removes the selected entry from the list.

- **Export List**

  Exports a copy of your current list to a file.

- **Import List**

  Imports a new list from a file.

- **Update List**

  Saves the items in the current list to a previously selected export file. The name of this export file is displayed in the information section at the bottom of the list manager window.

Save Files

Saves the items on your current list to your real disk.

File Protection

(Availability: All versions)

The File Manager allows you to save a list of frequently changed files and/or folders to the real disk when using the System Safe virtual protection. Possible uses include updating a shared document on your computer, allowing an administrator to "White list" non-registry changes he/she wants to make without turning off protection on the client system, using custom lists for different situations or users, etc.

Note

The software sees files and folders as unique objects, meaning that if you want to save all the files inside of a selected folder, you must include each of the files in the list individually.

Define List

Displays the number of files and folders on your current list. Click the link to open the File Manager:

- **Main list display window**

  This is the large open space to the upper left of the screen and is where your list will be displayed.

- **Add Files(s)**

  Click to select files to be added to the list.

- **Add Folder(s)**

  Click to select folders to be added to the list.

- **Delete**

  Removes the selected entry from the list.

- **Export List**

  Exports a copy of your current list to a file.

- **Import List**

  Imports a new list from a file.

- **Update List**

  Saves the items in the current list to a previously selected export file. The name of this export file is displayed in the information section at the bottom of the list manager window.

Enable Protection

Activates the File Protection feature for non-system disks, partitions, and files defined in your File Protection List..

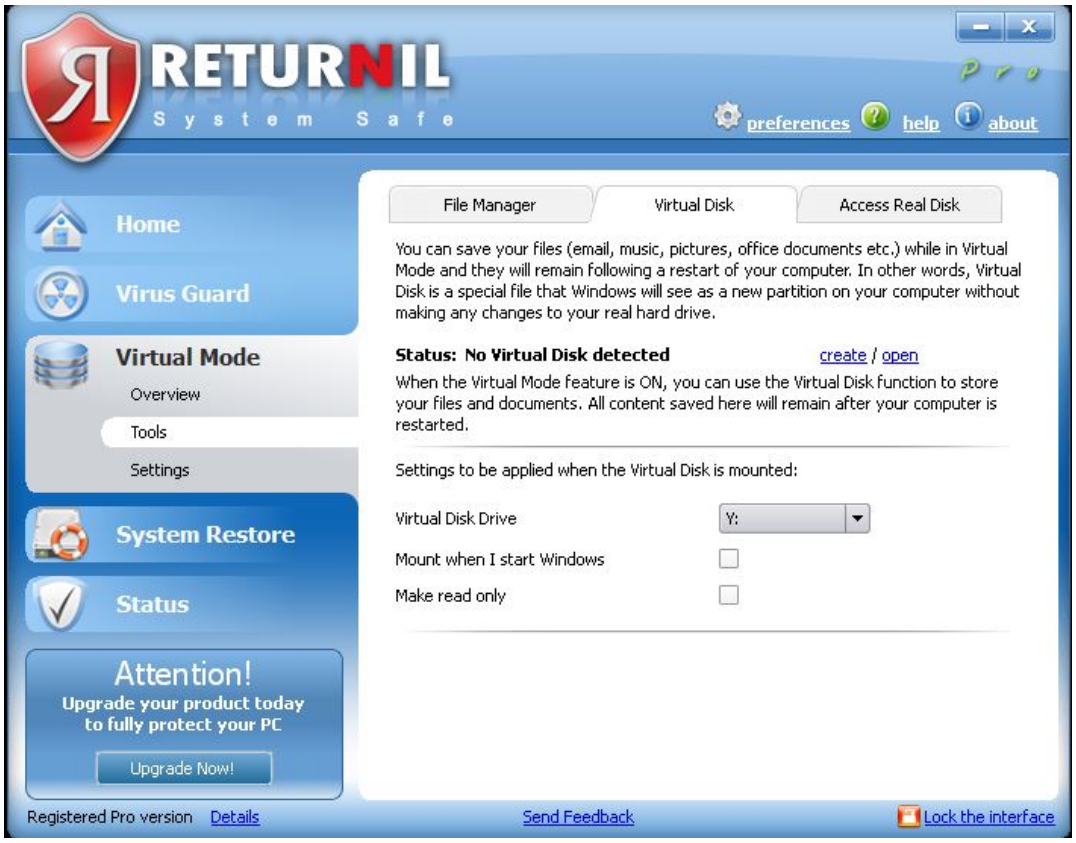
Virtual Disk

(Availability: All versions)

Use the options below to configure your Virtual Disk. This is a convenience feature and is designed to provide you with an additional place to save files when the System Safe virtual protection is turned on. If you are uncertain about what to do here, simply keep the suggested settings and then see if they were appropriate for your environment. If not, change them as required at a later time.

Tip

You **DO NOT** need to create a Virtual Disk to use the System Safe protection and the Virtual Disk can be used whether the protection is on or off.



Status

Displays a message about your Virtual Disk.

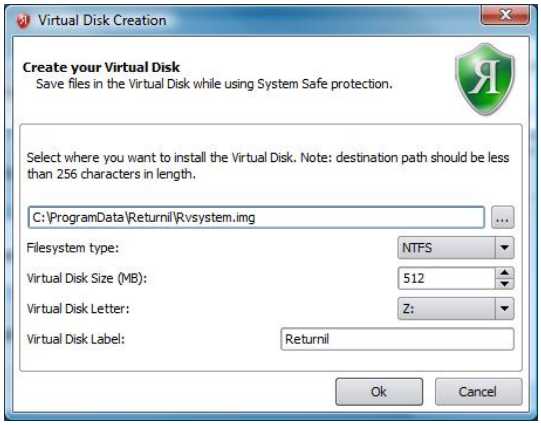
- **No Virtual Disk detected**

  This means you have either not created a Virtual Disk or you have stored your Virtual Disk in a different location than the one configured.

  - **Create:** Click to open the Create Virtual Disk screen.

Note

Clicking the "**open**" link will allow you to navigate to where you may have a backup or saved copy of an existing Virtual Disk.



- **Installation path:** Use the button on the left to specify where you want Returnil to create the Virtual Disk.
- **Filesystem type:** Choose between NTFS and FAT32.
- **Virtual Disk size (MB):** Specify the size of the Virtual Disk in MB (Ex: 1 GB = 1000 MB).

  ### Note

  The Virtual Disk must be at least 32 MB!

- **Virtual Disk letter:** Specify the drive letter for your Virtual Disk.
- **Virtual Disk Label:** Specify an appropriate volume label for the Virtual Disk. Default is "Returnil".
- **OK:** Click to save your settings and create the Virtual Disk. During the creation process, you will see a disk formatting screen. To complete the creation process you should select the appropriate options and then click the "OK" button when the format is complete.
- **Cancel:** Click to cancel the operation and not create a Virtual Disk.

- **Virtual Disk Drive**

  When the Virtual Disk is mounted this section will show this and display the current drive letter assigned to the Virtual Disk.

  - **Close**: Click to dismount the Virtual Disk.

- **Virtual Disk not mounted**

  This means that you have a Virtual Disk, but it is currently not mounted or alternately, not open or accessible.

  - **Open**: Click to mount the Virtual Disk.

Virtual Disk Drive

Shows the current drive letter assigned to the Virtual Disk and allows you to select alternate drive letters should the need arise. The change will take effect after dismounting and then remounting the Virtual Disk.

Mount when I start Windows

Forces Returnil to always mount (open) the Virtual Disk when Windows starts, regardless of the user logged in.

Make Read only

Restricts access permissions to read-only access following a dismount and then remount of the Virtual Disk.

Access Real Disk

(Availability: Paid versions)

Important

Requires that **Virtual Mode** protection is **ON**

This is a powerful tool that allows you to access and make changes to the real system while using the System Safe protection feature. You can move files from the Virtual System to the Real System or vice-versa.

Browse Files

Click to access the system's file manager.

- **Real system partition**

  Use to interact with specific file or folders on your Real System.

- **Virtual system partition**

  Use to interact with specific files or folders present in your Virtual System.

- **To move files**

  ### Important

  Please make sure that the target directory matches the originating directory.

  - **From Virtual to Real:** Select a file from within the Virtual System tree and the equivalent directory in the Real System tree. Next, right click the selected file in the Virtual tree and choose the **"Copy file to"** option to copy the file to the Real System.

  - **From Real to Virtual:** Select a file from within the Real System tree and the equivalent directory in the Virtual System tree. Next, right click the selected file in the Real tree and choose the **"Copy file to"** option to copy the file to the Virtual System.

Browse Registry

Allows you to open and edit both Real and Virtual System registries in a similar way to moving files between the systems.

Settings

(Availability: All versions)

Additional Protection Options (Anti-Execute feature)

- **Allow programs to run normally**

  As implied, programs will not be blocked or prevented from running unless they are detected specifically by the **Virus Guard** Real-Time monitor.

- **Trust system services from real disk only**

  Allows some flexibility between "block nothing" and "block all". A good example here would be the addition of a plugin to your browser to evaluate its functionality. Though it would be removed at restart of your computer when the Virtual Mode protection is active, it will not be blocked but other, unknown and newly introduced programs would be blocked.

- **Trust programs from the real disk only**

  This is the most restrictive setting and will block anything not already known.

Exit from Virtual Mode

Options for what will happen to changes following a restart of your computer with the **Virtual Mode** protection active.

- **Drop all changes (Recommended)**

  This is the default option as well as the most secure configuration. All changes not specifically saved to your real disk will be lost at restart of your computer when you have the System Safe feature turned on.

- **Save all changes**

  As the text implies, this option will save all changes to the real hard disk and would be as though the virtual protection was not on.

  ### Important

  This is an advanced feature and should only be used by experienced computer users who are 100% confident that the changes they are allowing are appropriate. Others should simply turn the protection off and then make changes to the system.

Advanced

- **Wipe all disk changes at computer startup**

  This option, when activated, will force the product to wipe the **Virtual Mode** protection cache (where changes are stored when the protection is active) at computer startup.

- **Percentage of free disk space used for the Virtual Mode**

Use the up and down arrows to change the amount of free space you will allow the product to use when the **Virtual Mode** protection is active.

Note

The less space allowed (default is 50%), the sooner your cache will fill and force you to restart your computer to reset the **Virtual Mode** protection cache.

- **Protected disk**

  Displays the disk being protected by the **Virtual Mode** protection feature.

Actions

- **Reset** button

  Resets the options and configurations to their installation defaults.

- **Apply** button

  Use this after editing your preferences in this section to save your changes.

Chapter 6. System Restore

Overview

(Availability: Paid versions)

Displays status fo the Real-time Restore Analysis monitor. This section of the program also allows you to start and stop the Analysis monitor, restore your system to an earlier time, restore selected files from the previous snapshot that may be missing in the one you restored to, and restore damaged system files.

Real-time Restore Analysis

Monitors your system files for changes so you can restore them to a previous time if required.

- **Green button displaying the text "Turn Off"** means the restore monitor is currently active and pressing the button will turn the feature off.
- **Red button displaying the text "Turn On"** means the restore monitor is currently inactive and pressing the button will turn the feature On.
- **Full Restore**

  Choose from a list of available snapshots to restore your system to an earlier period in time due to damage or malware infection.

- **File Recovery**

  Click to open the user file recovery screen where you can choose from a list of files from your previous snapshot to restore to the current system.

Full Restore

Click to choose from a list of available snapshots to restore your system to an earlier period in time due to damage or malware infection.

File Recovery

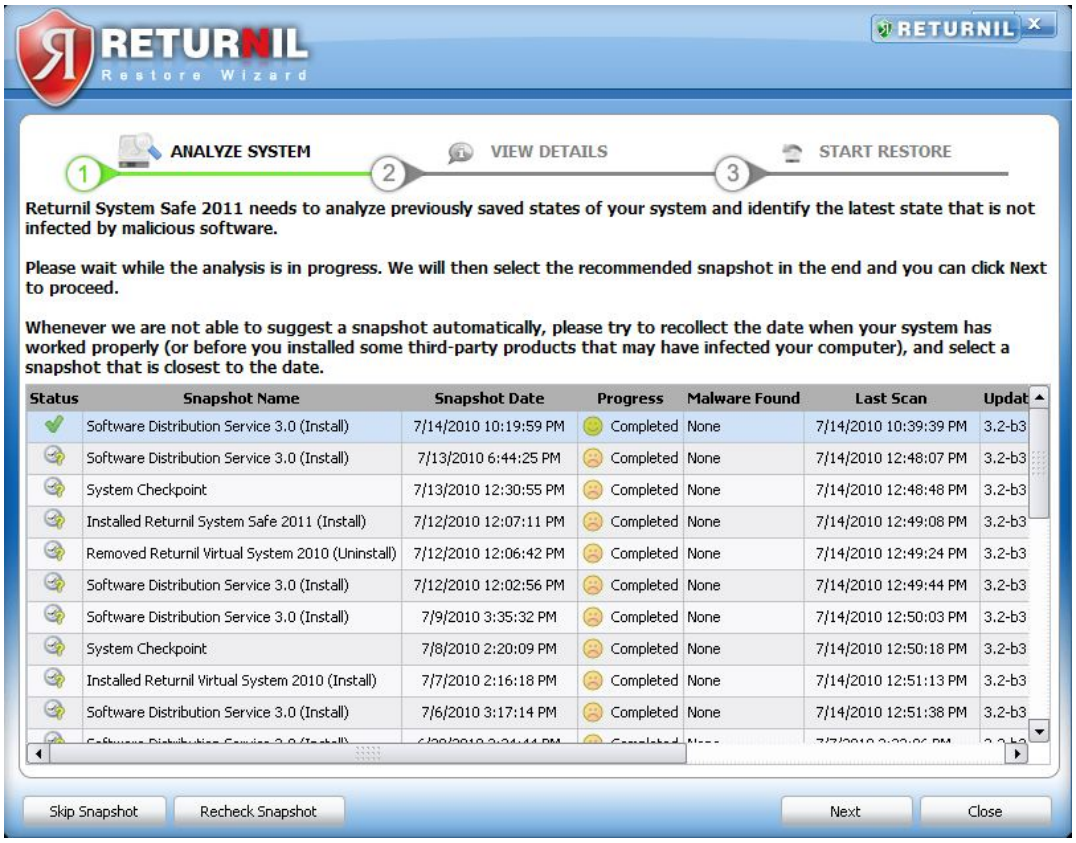
Click to open the user file recovery screen where you can choose from a list of files from your previous snapshot to restore to the current system.

Full Restore

(Availability: Paid versions)

Analyze System

Choose from a list of available snapshots to restore your system to an earlier period in time due to damage or malware infection.



- **Status**

Displays whether a selected snapshot has been scanned with current, updated definitions. A green checkmark means the snapshot is clean and has been scanned by the Virus Guard. . Potential statuses:

- **Clean**. No infections found in the snapshot.
- **Dangerous**. Malware detected in the snapshot.
- **Expired**. Analysis was performed using an outdated A/V definitions file.
- **Unknown**. Analysis of the snapshot has not been performed.

- **Snapshot name**

  As the title of the column implies.

- **Snapshot date**

  As implied.

- **Progress**

  Indicates the status of the snapshot analysis with the following potential states:

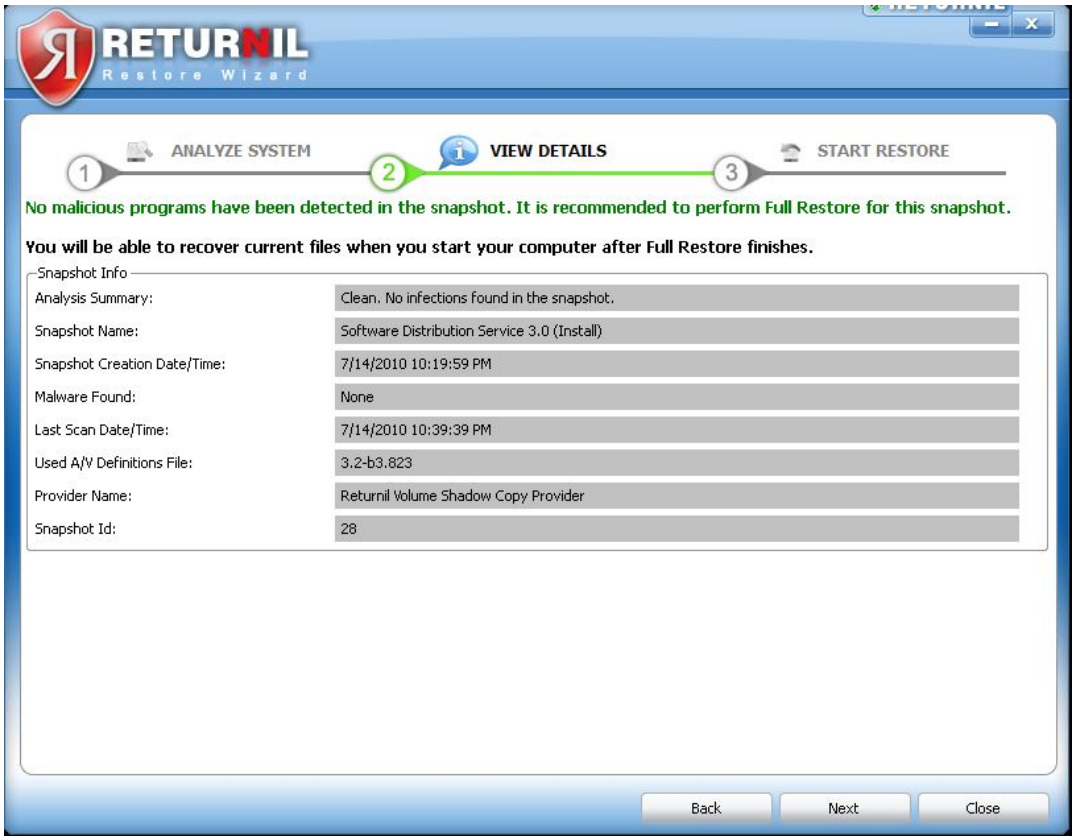
  - **Queued**: (Default state) Tthe snapshot is awaiting analysis and will be analyzed after all newer snapshots have been checked if newer snapshots have been found to be infected.
  - **Analyzing**: The snapshot is being analyzed now.
  - **Skipped**: The snapshot has been marked for omission from analysis. Queued snapshots become skipped if a good snapshot has already been detected. Alternatively, it may be possible to have skipped the snapshot manually.
  - **Cancelling**: The snapshot analysis has been interrupted by the user and the analysis is in the process of stopping.
  - **Completed**: The snapshot has been analyzed.
  - **Forced**: A manual analysis of the target snapshot has been requested, so it will be analyzed in any case regardless of whether a good snapshot has been identified or not.

- **Malware Found**

  Indicates whether malware was found during the scan. If there was no detection, this section will show the word "none".

View Details

Displays details specific to the snapshot you have chosen from the restore point list.



- **Analysis Summary**

  Displays the status of the chosen snapshot.

- **Snapshot name**

  As implied.

- **Snapshot Creation Date/time**

  When the chosen snapshot was made.

- **Malware Found**

  The View Details tab will list the identified infections if they have been found during analysis.

- **Used A/V Definitions file**

  Check this to make sure the definitions used for the scan of the chosen snapshot were the most current. If it is not the most recent signature file we recommend that you return to the main screen, update your definitions, rescan the wanted snapshot and then return to this screen to resume the restoration process.

- **Provider name**

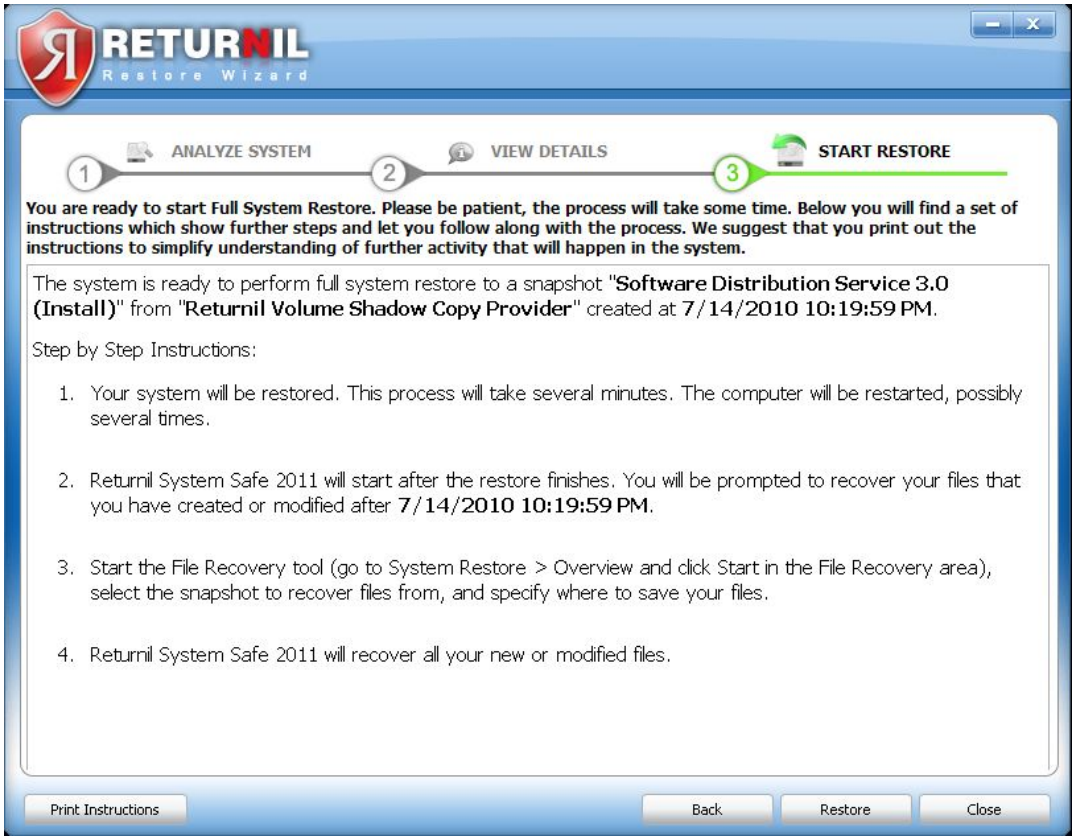
  As implied. For more information about providers, please see the *System Restore > Settings* section of the manual

- **Snapshot ID**

  Number assigned to the snapshot by the Returnil System Restore list. This number will be its place in the ordered System Restore snapshot list.

System Restore

Displays instructions on how to restore to the snapshot you chose at the beginning of this process



- **Restore** button

  Moves you to the next screen in the Full System Restore process

- **Back** button

  Takes you back to the previous screen.

- **Print instructions** button

  Prints the instructions shown on the Start Restore screen for future reference.

- **Restore** Button

  Begins the automated process of restoring your system to the chosen snapshot.

- **Close** button

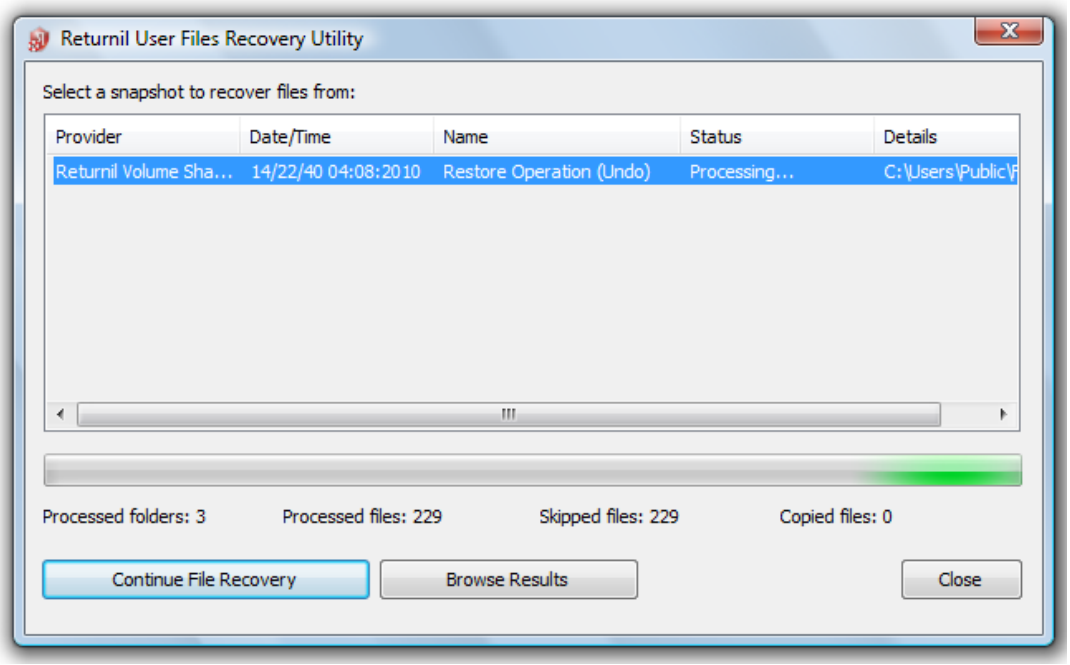
  Closes the Full Restore screens without restoring to the chosen snapshot.

File Recovery

(Availability: Paid versions)

Returnil User Files Recovery Utility

Choose from a list of available snapshots to restore your user files to an earlier period in time due to damage or malware infection.



- **Provider**

  Displays the source of the listed snapshot.

- **Date/Time**

  The date and time of creation for the listed snapshot.

- **Name**

  Assigned name of the listed snapshot.

- **Status**

  Indicates the status of the snapshot analysis with the following potential states:

  - **Queued**: (Default state) Tthe snapshot is awaiting analysis and will be analyzed after all newer snapshots have been checked if newer snapshots have been found to be infected.

- **Analyzing**: The snapshot is being analyzed now.
- **Skipped**: The snapshot has been marked for omission from analysis. Queued snapshots become skipped if a good snapshot has already been detected. Alternatively, it may be possible to have skipped the snapshot manually.
- **Cancelling**: The snapshot analysis has been interrupted by the user and the analysis is in the process of stopping.
- **Completed**: The snapshot has been analyzed.
- **Forced**: A manual analysis of the target snapshot has been requested, so it will be analyzed in any case regardless of whether a good snapshot has been identified or not.

- **Details**

  Information about the listed snapshot.

- **Processed folders**: number of folders found within the listed snapshot.
- **Processed files**: number of files found within the listed snapshot.
- **Skipped files**: number of files not requiring restoration.
- **Copied files**: Number of files restored
- **Start Recovery button**: starts the file recovery process.
- **Browse Results**: Allows you to check the listed snapshot for the files you want to recover.
- **Close Button**: Closes the file restoration window.

Settings

(Availability: Paid versions)

This basic setting screen will allow you to choose which system restore provider you'd like to use for your restore point creations.

Providers

Lists system restore providers which are present on user's computer system and are compatible with Returnil's products

- Returnil Volume Shadow Copy

  Restores the system using existing Windows Restore Points.

Actions

- **About** button

  Displays the copyright and versioning information of selected provider.

- **Configure** button

  Opens the configurations menu for the selected provider.

Chapter 7. Status

(Availability: All versions)

Protection status

- **Real-time protection**

  Indicates whether the Virus Guard's Real-time Protection is Enabled or Disabled .

  - **manage** link

    Opens the **Virus Guard** > **Scan** screen.

- **Virus Definition Update**

  Indicates the current version of the definitions database installed and the date it was released.

  - **update now** link

    Forces the product to request a definition file update from our servers. if no update is available you will receive a message indicating this or the definition and status display will update as appropriate after the new signatures have been downloaded and applied.

- **Virtual Mode**

Displays whether the Virtual Mode protection is started or stopped.

- **manage** link

  Opens the **Virtual Mode Overview** section so you can activate or deactivate the **Virtual Mode** protection feature.

  ### Note

  Turning the **Virtual Mode** protection **OFF** will require a restart of your computer. Turning the **Virtual Mode** protection **ON DOES NOT** require a restart of your computer.

- **System Restore**

  Indicates whether the Real-time Restore Analysis monitor is enabled or disabled.

  - **manage** link

    Opens the **System Restore** > **Overview** section where you can change enable/disable the **Real-time Restore Analysis** monitor, start a full system restore, or restore a file from a previous snapshot.

Product status

- **Product version**

  Version and build number for the program.

- **Product Update**

  Date the program version was last updated.

- **Upgrade Now link**

  Opens a product selection and description page on our website where you can purchase a new version of your software or upgrade your current copy to one with more features.

License status

- **Type**

  ### Note

  Those wanting an equivalent solution or subscription upgrade for the older RVS 2010 Enterprise Classic and RVS 2010 Home Classic versions should contact your sales representative or reseller to purchase licensing for the new Returnil Virtual System Lite 2011 product line.

  Version of the program.

  - **Free:** Unregistered free version. Major limitations apply.
  - **Home Free:** Registered free version.
  - **Trial:** Full functionality for 30 days. If not licensed within the trial period, the software will revert to the unregistered free for home use version.
  - **Pro (for home):** Paid consumer version.

  - **Pro (for business):** Business, Education, Non-Profit version for small to large networks WITH Antimalware capability.

- **Expiration date**

  Date your current licensing subscription expires.

- **Buy Now button**

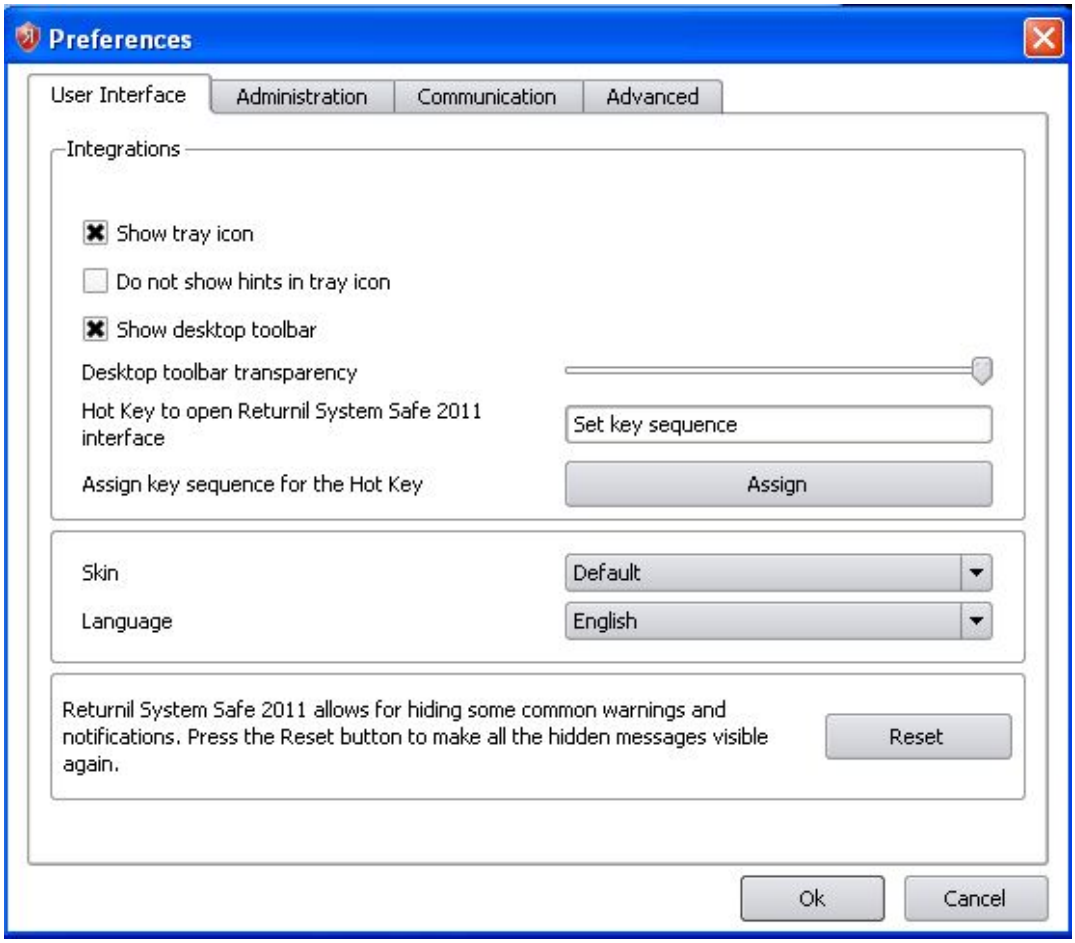
  Opens the product renewal page at our website.

Chapter 8. Preferences

User Interface

(Availability: All versions)

To open the Preferences menu, click the **Preferences** link in the upper right corner of the program's interface. This section allows you to change options that are specific to the program interface:



Integrations

- **Show tray icon**

  Displays an icon in the section of your Windows task bar next to the system clock.

- **Do not show hints in tray icon**

  Deactivates tray icon messages for silent operation of the client.

- **Show desktop toolbar**

  Displays the product's notification toolbar.

- **The slider**:

Allow you to set the level of transparency in the desktop toolbar.

- **All the way to the left:** toolbar is completely transparent.
- **All the way to the right:** toolbar is completely opaque.

- **Selected Hotkey**

  Displays the chosen key combination that will open the product's interface.

- **Assign key sequence**

  Click to assign the appropriate combination of keys for the Hotkey feature.

Other options

- **Skin**

  Allows you to change the appearance of the program.

  ### Note

  Alternate skin designs may not be available in all builds.

- **Language**

  Select a supported language for the interface.

  ### Note

  Available localizations (languages) may not be the same as those available during the installation. If your chosen language is not included, it may be updated in a future release or upgrade. If you would like to offer a translation, please contact us at support-tech@returnil.com for instructions on how to create and submit a localization for the product's interface. **Please understand that inclusion of a submitted translation may be delayed pending quality assurance review.**

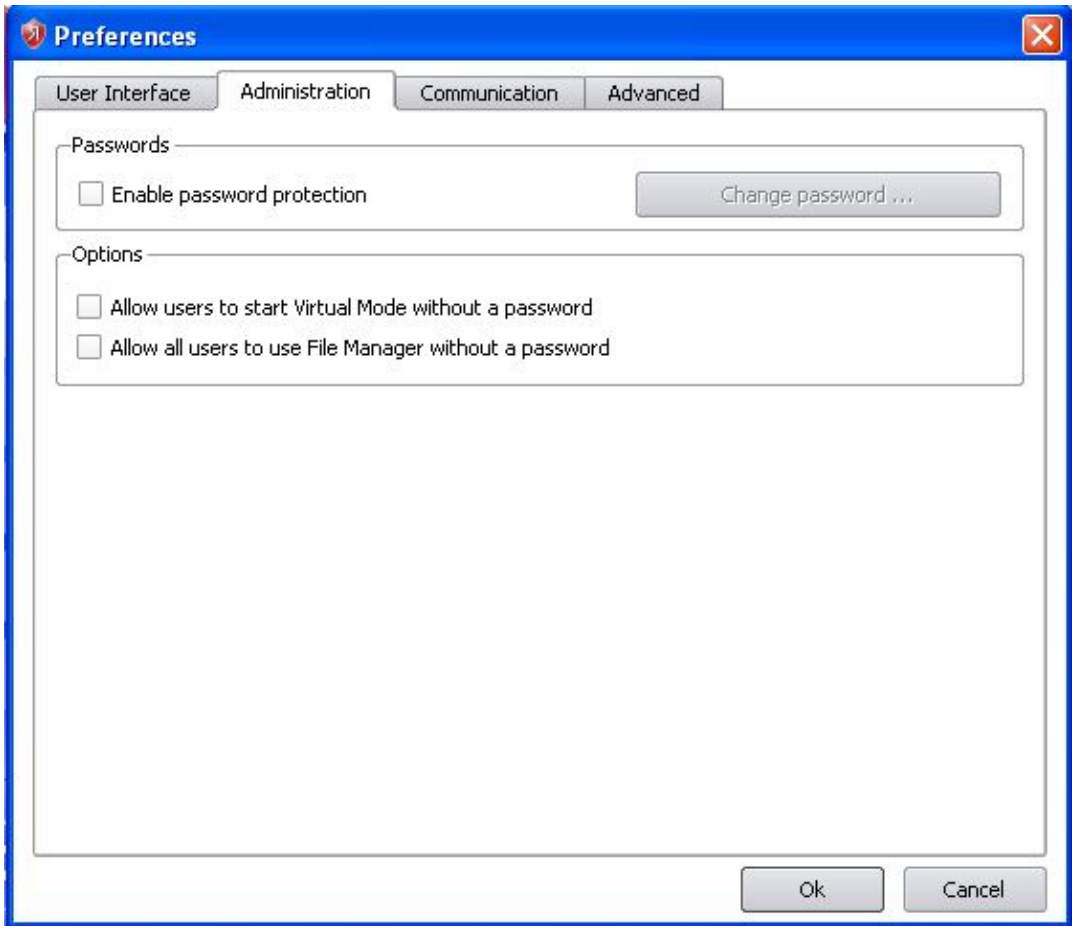
- **Reset** button

  Un-hides messages you may have hidden in the past.

Administration

(Availability: All versions)

Allows you to set supported program administration options.



Passwords

(Availability: All registered versions)

- **Enable password protection**

  Restricts access to the program and/or program settings.

  ## Note

  The default password is a blank space if you do not configure one!

- **Change password… button:**

  Opens the password configuration screen.

Options

- **Allow users to start Virtual Mode without a password**

  Allows all users to activate the **Virtual Mode** protection without the need to enter a password.

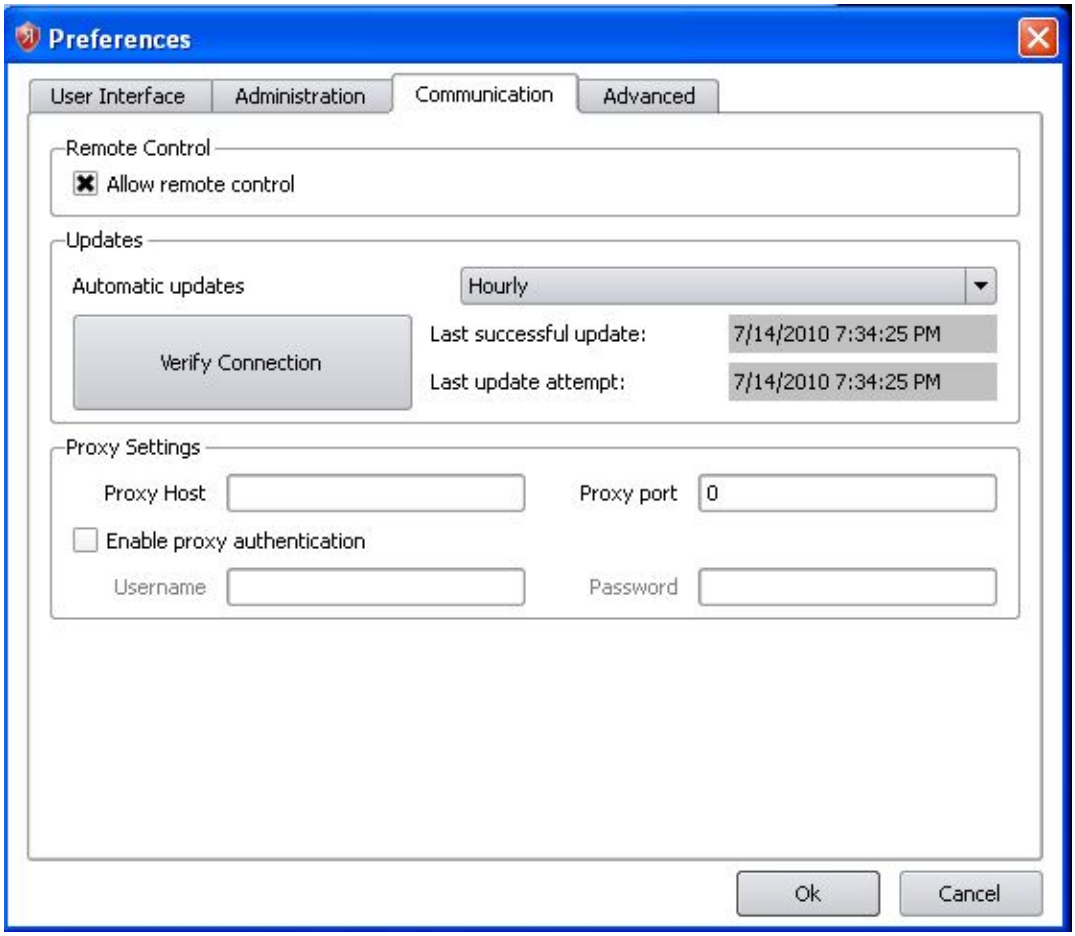
- **Allow all users to use File Manager without password**

  Allows users to make changes to the current File Manager as well as to allow them to import or export File Manager lists.

Communication

(Availability: All versions)

Allows the authorized user to configure various client communication options.



Remote Control

If the option **Allow remote control** is checked:

- For Home versions, this allows customer support to do remote recovery of some product features by user request, e.g. recover from forgotten password.
- For Enterprise versions, this allows customers to manage their software clients remotely (turn on/off protection, manage licensing and other features etc).

Updates

Allows you to configure when the Virus Guard feature checks the internet for malware signature updates as well as to display information regarding when the check was last made and when the next check will be performed.

- **Automatic updates**

  Click to configure the time intervals when the Virus Guard feature will check for updates automatically. (Hourly, Daily, Weekly, Monthly, Never - Use this option to deactivate automatic updating)

- **Verify Connection**

  Initiates communication with the management console to verify your connection.

  - **Last successful update:** Displays the date/time the last successful update was made.
  - **Last update attempt:** Displays the last date/time an automatic update was attempted.

Proxy Settings

Configure the proper settings if you use a proxy server to connect to the internet. If you are unsure of what these settings are, please contact your administrator or service technician for assistance.

- **Proxy Host**

  Enter you Host information here.

- **Proxy port**

  Enter the appropriate port.

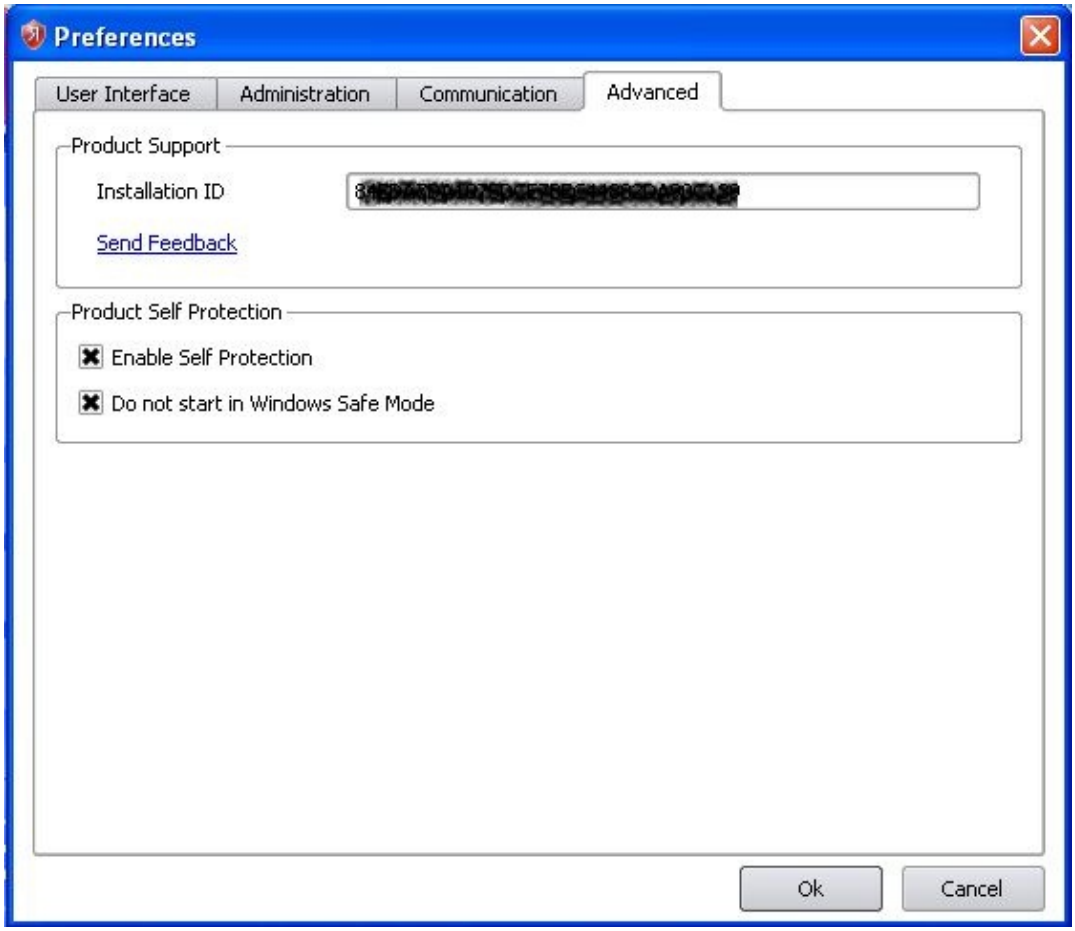
- **Enable proxy authentication**

  Activate this if your proxy requires authenticated login.

  - **Username:** Enter the appropriate username.
  - **Password:** Enter the appropriate password.

Advanced

(Availability: All versions)



Product Support

- **Installation ID**

  Internal product support identification code for that copy of your software.

- **Send Feedback**

  Opens a support page on our website where you can submit problem reports for the program.

Product Self Protection

- **Enable self protection**

  This option hardens the program's virtual mode protection against specific types of malicious content that can bypass unprotected virtualization solutions. We highly recommend that you do not deactivate this option.

- **Do not start in Windows Safe Mode**

  Deactivates the self protection and Virtual Mode feature while in Windows Safe Mode.

  ## Note

  Please us this option wisely. It should be considered only if some not trusted people have access to the computer in question.

Chapter 9. License Registration

(Availability: All versions)

Details of Current Registration

Displays current licensing and subscription expiration information. Click the "**product registration**" link in the Status > Overview > License Status section to open the License Registration screen:

- **Status**

  Displays the current registration status for your software.

- **Type**

  Displays the version name for your product copy.

- **Owner**

  Displays the registered owner for your software.

- **Expiration**

  Displays the end date of the current product subscription.

Registration Type (step 1)

Enter the appropriate information to activate the features for your current license type. If you choose not to register your copy of the software, it will default to the unregistered free for home use version which will have fewer available features.

- **I have a valid license number for this product**

  Select this option, enter your license number in the space provided and then proceed to the registration details section (step 2). Only available for paid editions. For Free and Trial editions, no license is necessary.

- **Trial version (Recommended)**

  If you do not yet have licensing and wish to evaluate the software before purchasing a subscription, check this option and then proceed to the registration details section..

- **Free version**

  If you do not yet have licensing and are only interested in using the freeware version of the software, check this option and then proceed to the registration details section

  - **comparison chart** link

    This will take you to our website where you can find a convenient chart comparing the different versions of our software. In the chart you will see at a glance the different feature sets available in the various solutions we have available for the customer to choose from.

- **"forgot your license number?"** link

  Opens a page on our registration server where you can have a reminder e-mail sent to your registered email address with your licensing information.

Note

The license number recovery service on the server is not available to holders of promotional licensing. If you fall into this group, please contact Returnil technical support for assistance.

Registration Details (step 2)

- **Name**

  Enter the name you want the product registered to or the name you used to purchase your license subscription.

- **Email**

  The email address the product should be registered to.

  ### Note

  The chosen address must be capable of receiving emails as you will be sent a registration confirmation link to complete the registration!

- **Register**

  Click here to register the software. The registration might take a few minutes to complete. You will see Request Pending status on the bottom left corner of your screen until the registration was successfully completed.

- **Purchase**

  Click this button to open a purchase page at our online e-commerce provider.

- **Cancel**

  Click to cancel the registration and close the screen.

Chapter 10. Contact Us

For additional information, support material and specific contacts, please consult our website a www.returnilvirtualsystem.com/support [http://www.returnilvirtualsystem.com/support] .

Chapter 11. About Returnil

Overview

Returnil is a privately held company with offices in Helsinki, Finland; St. Petersburg, Russia and Nanjing, China. Founded in 2007, Returnil is led by a strong executive team with years of experience in managing and developing security companies and products. Returnil's unmatched team and technology is backed by the VTB - Venture Fund, Russia's first venture capital fund, with a successful track record in investing primarily to high-growth companies dealing with IT, nano- and biotechnologies and other areas requiring high-tech innovation. Our strong financial backing guarantees our customers' and partners' sustainability and the continual development of our security software products.

Strategy and Mission

Returnil aspires to be the most innovative security solution provider for enterprises of all sizes and for home users. Based on its reliable virtualization solution - a system virtualization solution coupled with Anti-virus that ensures a simple, smart and strong approach to information security, the mission of Returnil is to provide the crucially needed last line of defense against the ever growing threats of the online world.

Leading IT Security Partner

With more than 100 partners around the world, our products are available through our online store at the Returnil website, resellers, ISPs and also as an OEM solution. Our products are actively used by individual users, small businesses, large enterprises, non-profit organizations, schools and Universities, government agencies, as well as by OEMs.