



# AppRanger

Copyright © 2008- APPRANGER, Inc. All rights reserved. All content is Proprietary Information of APPRANGER, Inc.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of APPRANGER, Inc. APPRANGER Incorporated assumes no responsibility for any errors that may appear in this document. No part of this documentation may be reproduced without the express prior written permission of the copyright owner.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

AppRanger, and Guardian of your servers® are trademarks or registered trademarks of AppRanger, Inc. in the U.S.A. and certain other countries. Other names and products are trademarks or registered trademarks of their respective holders.

Contact:

AppRanger USA

Phone: (626) 357-3706

Email: [info@AppRanger.com](mailto:info@AppRanger.com)

Web: [www.appranger.com](http://www.appranger.com)

# Table of Contents

<b>Table of Contents</b> .....	<b>ii</b>
<b>Preface</b> .....	<b>ix</b>
Objectives .....	ix
Available Formats .....	ix
Intended Audience .....	ix
<b>Chapter 1 — AppRanger Security</b> .....	<b>1</b>
1.1 Security.....	1
1.1.1 Scan .....	1
1.1.2 Sandbox .....	1
1.1.3 Lockdown .....	1
1.2 Content Monitoring & Filtering .....	2
<b>Chapter 2 — Installing AppRanger Software</b> .....	<b>3</b>
2.1 AppRanger Client.....	3
2.1.1 Manual Installation.....	3
2.1.2 Remote Installation.....	4
2.2 Software upgrade.....	6
2.3 Evaluation License .....	6
2.3.1 Converting to a Paid License.....	6
<b>Chapter 3 — Using AppRanger</b> .....	<b>9</b>
3.1 Basic Management of Client .....	10
3.1.1 Scan .....	11
3.1.2 Reports and Logs .....	13
3.2 Configuration.....	17
3.3 Sandbox .....	22
3.4 Content Filtering and Monitoring.....	26
3.4.1 Web Filter .....	27
3.4.2 Web Monitoring .....	29
3.5 Lockdown .....	30
3.5.1 System Changes.....	30
3.5.2 Enforce Lockdown .....	30
3.5.3 Lockdown Settings .....	31
3.5.4 Create Reference State .....	31
3.6 About .....	31
3.6.1 Reset .....	31

3.6.2 Upgrade .....	31
3.6.3 Live Update .....	31
3.6.4 Miscellaneous .....	31
<b>Chapter 4 — Frequently Asked Questions (FAQ) .....</b>	<b>36</b>



# Preface

## Objectives

This document provides users with detailed information on how to manage and install and manage AppRanger software on servers and desktops. In Chapter 1, we describe security problem addressed by AppRanger, and in subsequent chapters, we describe how to install, use, and manage AppRanger.

## Available Formats

The printed documentation, the on-line HTML Help documentation, and the Web browser documentation all show the same text. The on-line and Web browser HTML versions are the best sources of information because they offer hyperlinks.

For the most current information about AppRanger, visit the AppRanger Web site at <http://www.AppRanger.com>.

## Intended Audience

The intended audiences of this document are administrators who manage a large number of servers and desktop.



# Chapter 1 — AppRanger Security

## 1.1 Security

Newer malware are crafted to bypass the security architecture of anti-virus software. AppRanger's security approach plugs those holes.

AppRanger has three security features to detect, remove, and prevent malware. These features are:

- Malware scanner
- Sandbox to protect applications
- Lockdown to prevent unauthorized changes

### 1.1.1 Scan

AppRanger's malware scanner uses two patent pending methods to find and remove malware/rootkits that are very difficult to find and remove. If there is a rootkit or polymorphic malware on a computer, AppRanger will find it.

Only malware AppRanger may not remove are "file infectors." Those should be taken care by anti-virus software, but in late 2008 AppRanger will support fixing "file infector" malware/virus as well.

AppRanger automatically scans the computer once and day and notifies the user if any malware is detected.

### 1.1.2 Sandbox

AppRanger protects applications like Web browsers, IM clients, e-mail clients, etc. from attacks with sandboxes. Since 75% of all attacks are via applications, these sandboxes are very important for protecting desktops, laptops, and servers. Most of the attacks that can bypass anti-virus will be blocked by AppRanger sandboxes.

AppRanger automatically finds common applications and applies appropriate sandbox. While user configuration is not required, it is possible to customize these sandboxes.

### 1.1.3 Lockdown

The final component of AppRanger security architecture is the "Lockdown" mechanism. AppRanger creates a reference state for the computers and tracks any system changes on a daily basis. If lockdown is enforced, only authorized processes will be permitted to run any unauthorized changes will be rejected.

## 1.2 Content Monitoring & Filtering

AppRanger monitors and filter content at the application. Application sandboxes have access to content (in unencrypted form) transmitted and received by the applications, therefore AppRanger can monitor and filter that content with relative ease.

Currently AppRanger support only two applications for content monitoring and filtering. These applications are:

- Internet Explorer
- Firefox

AppRanger content monitoring report will show hourly statistics about websites visited, time spent, and data downloaded. Content filtering can block websites, disable weblogin to all or specific website, and control files that can be downloaded via that application.

Support for IM content monitoring, filtering, and encryption will be available soon.

# Chapter 2 — Installing AppRanger Software

In this chapter we describe how to install, activate, and upgrade AppRanger software.

## 2.1 AppRanger Client

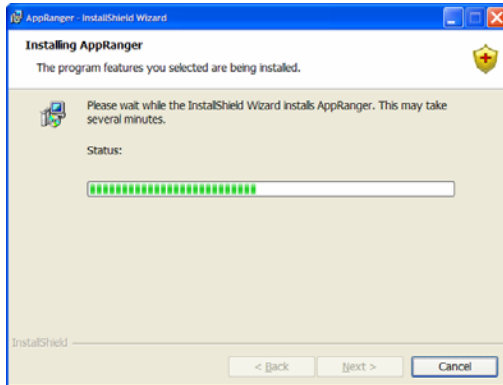
The AppRanger client can be installed via the Web browser by visiting the URL <http://www.AppRanger.com/try.php> and downloading the installer package. In a corporate environment, AppRanger client can be installed remotely by using the central management tool.

### 2.1.1 Manual Installation

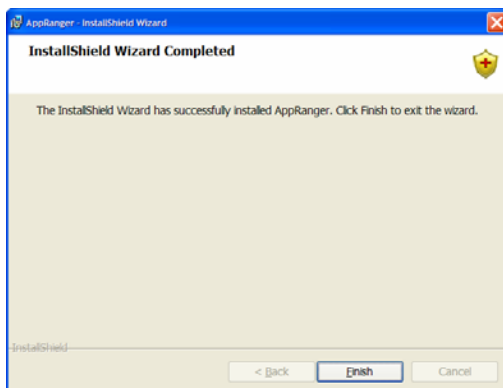
#### License Agreement



## Start Copying Files



## Setup Finished



## 2.1.2 Remote Installation

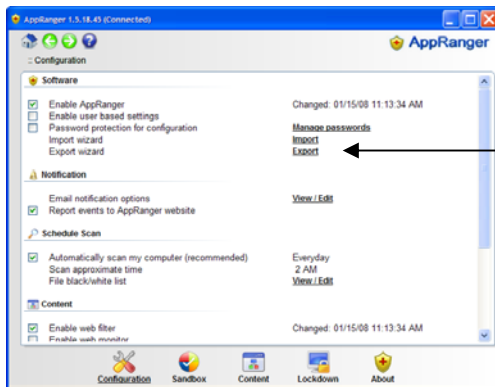
### Via Zenworks, SMS, or Altiris

To install AppRanger client through third party software distribution systems, first extract the msi package from the AppRanger installer package and then use the following command line. To extract the msi package, right click on the AppRanger installer package file and select the extract option.

To make the installation and configuration of AppRanger easy, the AppRanger configuration file can also be loaded as part of installation.

```
msiexec.exe /qn /i AppRanger.msi INI="CONFIGDIR"
```

CONFIGDIR is the full path of the directory (in quotes) where AppRanger configuration files (there are three) are stored.



Click on “Export configuration wizard” button to generate configuration files

Configuration files are generated by using the “Export configuration wizard” option in the “Configuration” tab of AppRanger. See Section 3.2 for more details.

If the “Include activation key” flag is checked while exporting configuration, the activation key will be included in the configuration file. When the configuration file is read in by AppRanger during installation, that key will be used to automatically activate the license.

To upgrade,

```
msiexec.exe /qn /i AppRanger.msi REINSTALLMODE=voums REINSTALL=ALL  
INI="CONFIGDIR"
```

To uninstall,

```
msiexec.exe /qn /x {9C641D4C-16A6-4DCE-94C3-55B0BE732B0F}
```

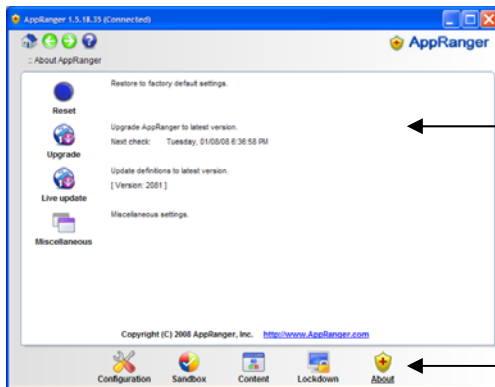
Please note: You should configure SMS to run the above command line from the directory where it copies the installation package.

The AppRanger.msi package can be extracted from the AppRanger\_installer.exe package.

## 2.2 Software upgrade

There are two different methods to upgrade the AppRanger client software.

The first method is to click on the “Upgrade” button from the AppRanger configuration window as shown in Figure below.



STEP 2:  
Click here  
to upgrade  
software

STEP 1: Click  
on “About”

The second method is to download the latest installer package for the AppRanger, and run it.

Click on “Live Update” to obtain latest malware definitions.

## 2.3 Evaluation License

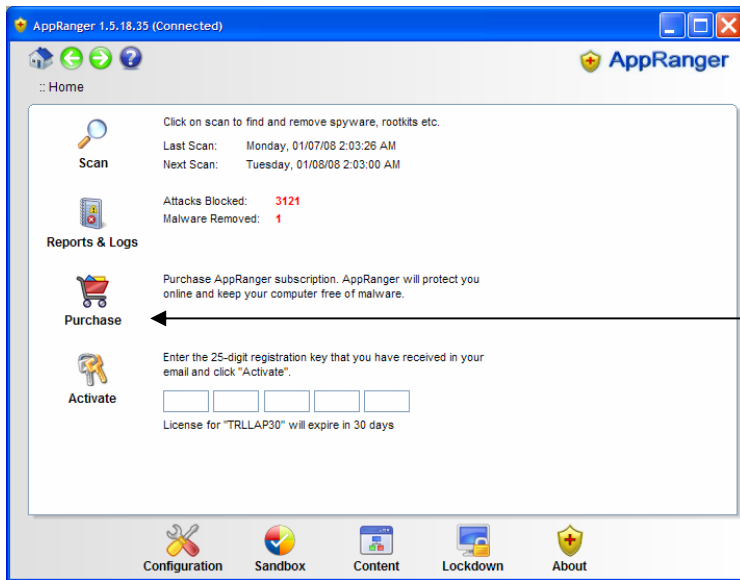
AppRanger software is licensed based on a yearly fee. To obtain an evaluation version of AppRanger client software, please visit [www.AppRanger.com/try.php](http://www.AppRanger.com/try.php).

The evaluation license for AppRanger is valid for 30 days. If the software is not activated during the trial period, it will disable itself at the end of the evaluation period.

During the trial period, AppRanger is fully functional on servers, but on the clients its malware removal feature is deactivated.

### 2.3.1 Converting to a Paid License

Purchasing or renewal of a AppRanger license can be done via e-mail, online, or phone.



## Purchase

To purchase AppRanger:

Install AppRanger (<http://www.appranger.com/try.php>)

Start AppRanger application

Click on “Purchase” button. Follow the instructions

Alternatively, one can go to [www.AppRanger.com/purchase.php](http://www.AppRanger.com/purchase.php) and purchase the product.

## Online and Offline Activation

### Method 1

After you have purchased and installed AppRanger, you will receive an e-mail with the activation link and registration key.

Enter the registration key and click on “Activate” button.

### Method 2

For customers who have purchased AppRanger. Click on “About” and go to “Miscellaneous” and then to “Additional Activation Options” tab.

Click on “License request” button to generate license request file

E-mail the file to [info@AppRanger.com](mailto:info@AppRanger.com)

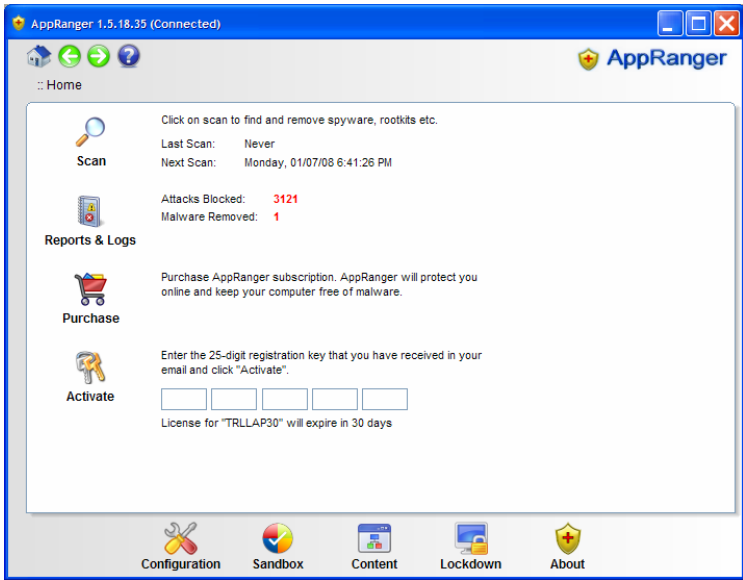
Install the license file you receive by clicking on “Install license” button

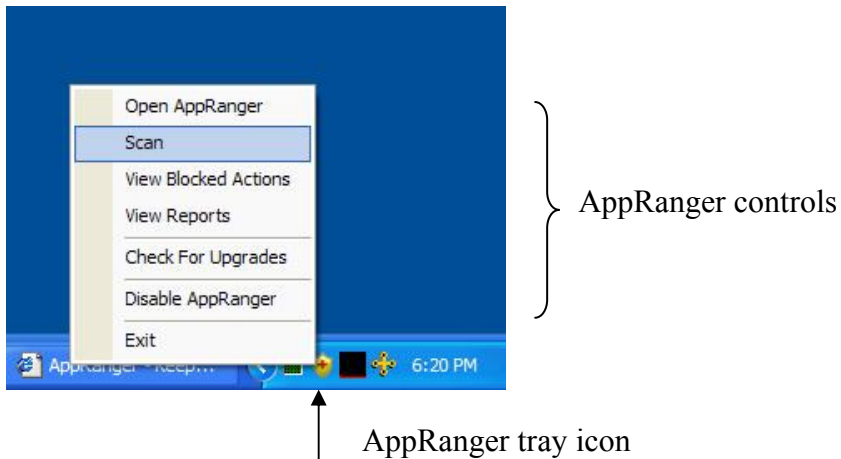
### Method 3

In a centrally managed environment with an AppRanger central manager node accessible to the client, the license can be obtained by entering the name or IP address of the AppRanger Manager node and clicking on the “Request” button.

# Chapter 3 — Using AppRanger

In this chapter we describe how use AppRanger to protect servers and desktops. Figure below shows the basic configuration window for the AppRanger client. The AppRanger application can be started by right clicking on the AppRanger tray icon or double clicking on the AppRanger icon on the desktop.





Most frequently used AppRanger controls are accessible from the AppRanger tray. Right click on the AppRanger icon in the tray to:

- Start scan
- View events blocked by AppRanger
- View Reports
- Check for upgrades (software and definitions)
- Enable/disable AppRanger

To unblock actions AppRanger is blocking, select the “View Blocked Actions” option from the AppRanger tray to view all events blocked by AppRanger. Right click on the action you wish to unblock and select “Allow”. Click on the “Refresh” button if you do not see the blocked event.

### 3.1 Basic Management of Client

AppRanger client installs as an application, driver, service, and tray icon. To scan the computer or make changes to AppRanger settings, start AppRanger application.

From the top level menu of AppRanger, one can perform the following operations:

- Scan computer
- View AppRanger reports and logs

- Purchase or activate AppRanger

Other AppRanger configuration setting can be modified only via the several advanced configuration options shown at the bottom of the AppRanger window.

**APPRANGER BLOCKS DOWNLOAD OF EXECUTABLE CONTENT VIA THE BROWSER. TO PREVENT APPRANGER FROM BLOCKING A DOWNLOAD, PRESS THE "CTRL" OR "SHIFT" KEY.**

### 3.1.1 Scan

To find and remove malware, click on "Scan" button in the AppRanger application as shown below.

AppRanger uses a patent pending method to scan the computer. It will find and remove even the most difficult malware, Trojans, and Rootkits. If you have a rootkit, AppRanger will find it.

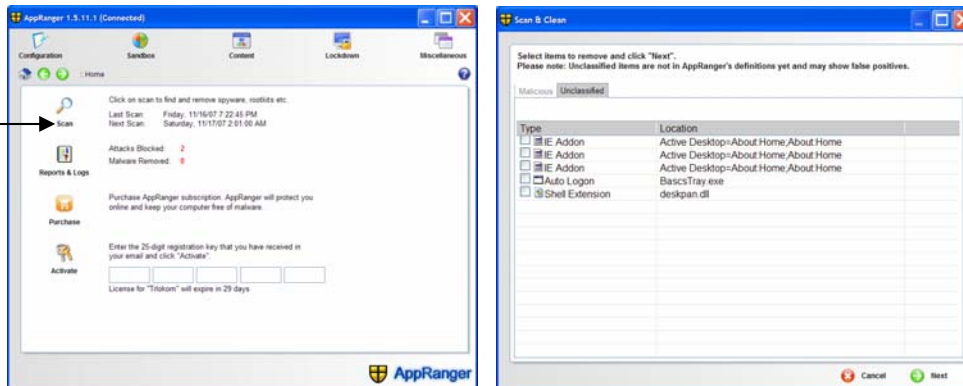
There are four scan modes:

- Quick scan
  - o Full scan of computer memory and processes. Limited scan of registry and file system.
- Quick scan with "Deep Clean" (Recommended)
  - o Full scan of computer memory and processes. Limited scan of registry and file system. Uses "Deep Clean" method to remove malware.
- Full scan
  - o Full scan of computer memory, file system, and processes. Limited scan of registry and file system. Uses "Deep Clean" method to remove malware. This scan can take several minutes.
- Kernel scan
  - o Scan of kernel memory only. Helpful in finding rootkit hiding in kernel. This option should be used only if other scan modes cause crashes.

Quick scan with "Deep Clean" is recommended. It is fast and can remove any active malware or rootkit.

The scan will take a few minutes and you may see small pauses in between. Please wait for the scan to finish and at that time a window will pop up with the results. A typical scan should take around 5 minutes, if that. If the scan does not start in 1 minute, click on "Cancel" and start scan again.

Kernel scan should only be used if quick scan or full scan results into a blue screen crash. If that happens, it is very likely that there is a rootkit and the kernel scan will help you determine which one. Quick scan with deep clean is most effective in cleaning.

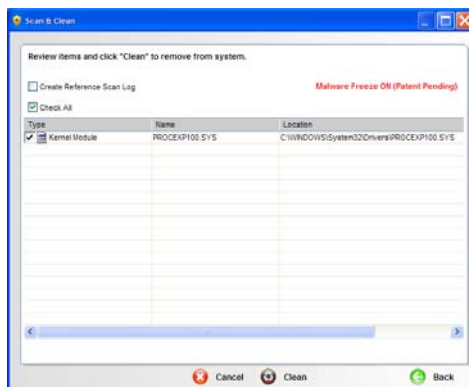


Window on the right shows the scan results. The results are displayed under two tabs labeled, "malicious" and "unclassified".

- Any item in the "malicious" list can be deleted.
- The "unclassified" list may or may not contain malware.

Items listed there just have not been processed and properly classified by AppRanger. However, if the computer is infected with malware, it's most critical component will be listed here even. This enables an expert to remove any malware from the PC.

Right click on an item to add it to black/white list and double-click on it to view its properties.



After selecting the items to delete, click on "Next". All the items that AppRanger will delete will be displayed on the new page. Check the items one more time.

“Create Reference Scan Log” if you wish to keep the current state as a reference state (items marked for deletion will not be part of the reference state).

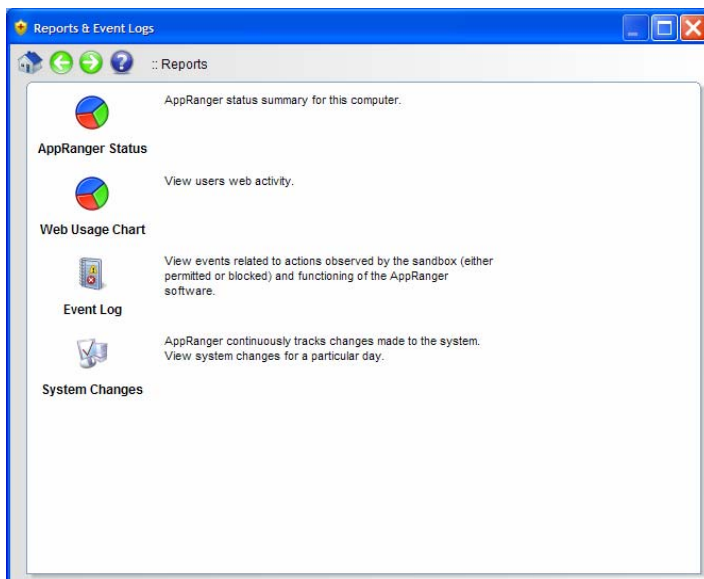
Click on “Clean” button to remove the selected items. AppRanger may reboot the PC to remove the selected items.

### 3.1.2 Reports and Logs

AppRanger tracks state of the computer and provides that information in easy to read reports. These reports are:

- AppRanger status
  - o One page summary of computer system state.
- Web usage chart
  - o HTML report of Web browsing.
- Event log
  - o Events observed or blocked by AppRanger.
- System changes
  - o Daily report on changes observed to computer system state.

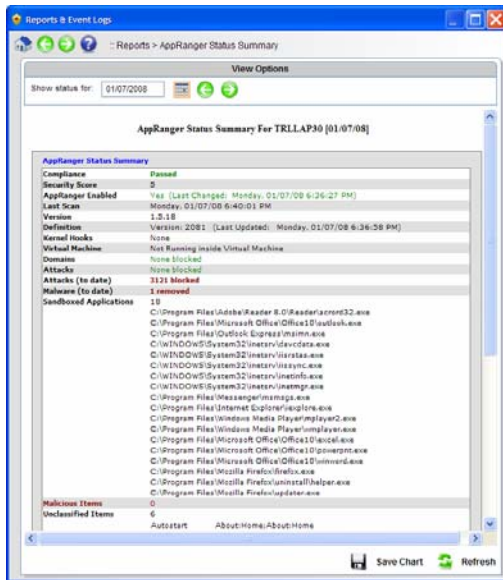
AppRanger supports Syslog compatible logging.



## AppRanger Status

AppRanger tracks the state of the computer and displays that information in an easy to read report. This report can be used to meet HIPPA, Sox, PCI compliance.

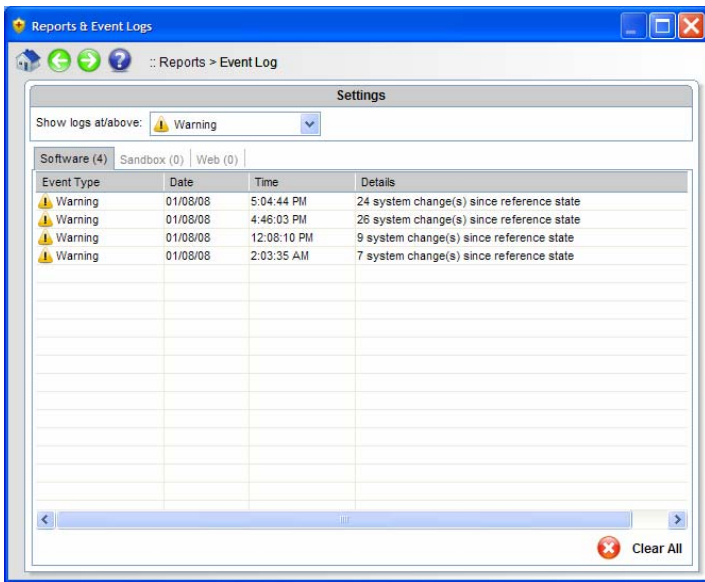
The daily reports shows AppRanger software status, protected applications, attacks blocked, malware detected, and unclassified applications. Click on the arrows to change the date.



## Event Log

If AppRanger blocks an action, it will be displayed here.

To unblock the action, right click on the event and select "Allow."



## Web Usage Chart

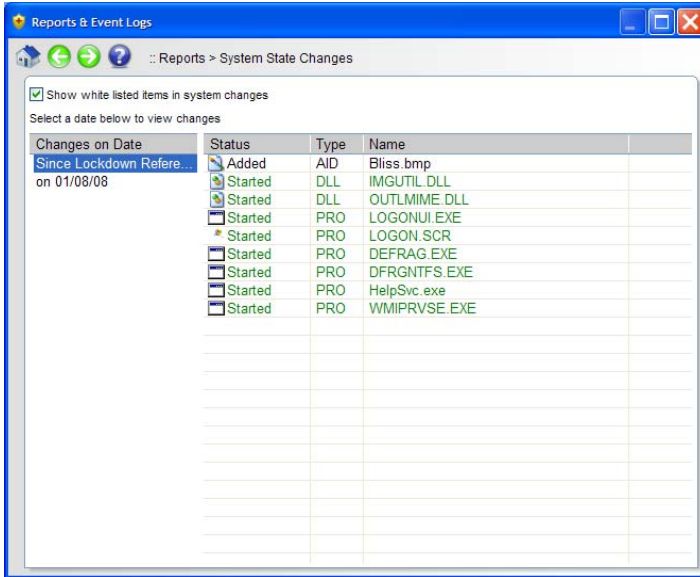
AppRanger tracks Web browsing activities of users. Daily chart shows URLs visited, time spent browsing the Web (by hour), pages viewed, data downloaded, and attacks blocked,



## System Changes

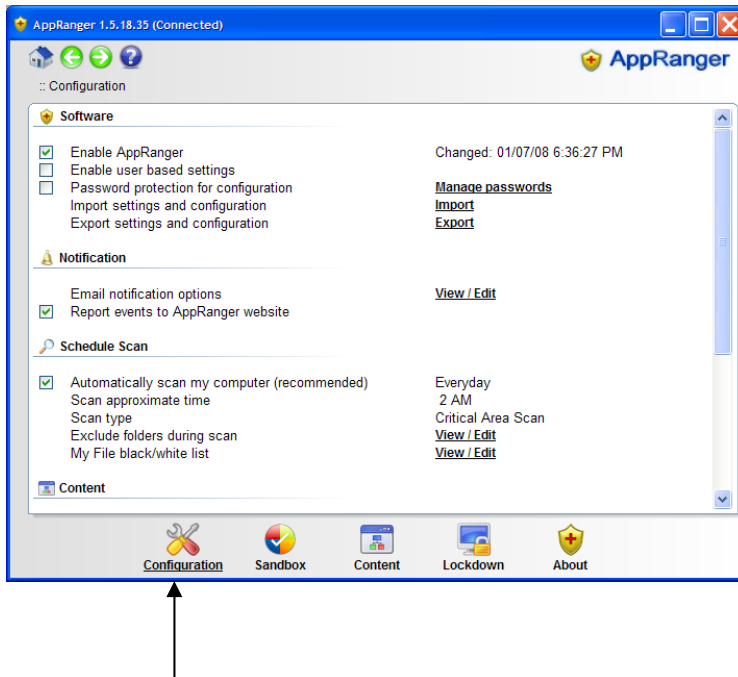
AppRanger tracks daily changes to the system state of the computer. Click on a date to view system changes on that day.

If an undesirable activity takes place on the computer, “System changes” helps track down the day changes took place. Double click on any change shown to view details about that change.



## 3.2 Configuration

Click on the “Configuration” icon to view and change AppRanger settings.



### Software

Under this section are the settings to enable/disable software and import/export of configuration.

By default AppRanger is enabled and default configuration is for the computer and not for a specific user.

Check the “Enable user based settings” if you wish to set sandbox and content rules for users. Please note that certain AppRanger settings and black/white lists are common to all users.

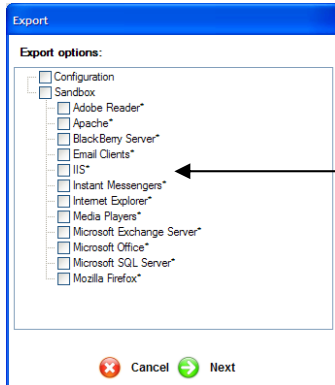
### Export Configuration

Export AppRanger settings, sandbox configurations, file black/white list, and URL black/white list.

Use this option if you have a complex setup for AppRanger so that you can restore it easily in case of a reinstall. In a large network use this to configure AppRanger settings for group of users.

AppRanger will export three files to the directory specified by the user:

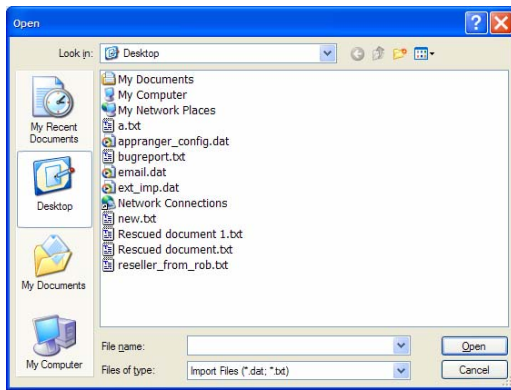
- url.dat (Black/white list of URLs)
- file.dat (Black/White list of files)
- cfg.dat (AppRanger configuration)



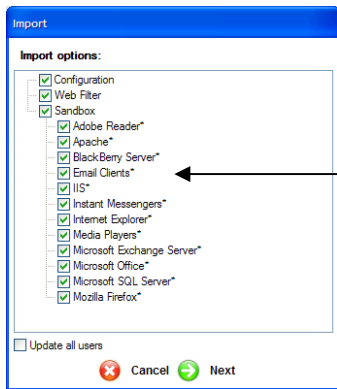
Check items  
to be  
exported

### Import Configuration

Import AppRanger settings, sandbox configurations, file black/white list, and URL black/white list. AppRanger will prompt the user to provide the directory and look for one or more of the following three files url.dat, bw.dat, and cfg.dat.



AppRanger will check the files and display information that it can import. Uncheck the part you do not wish to import. By default, AppRanger will apply the new settings to all users (if user based settings are enabled) and the machine.

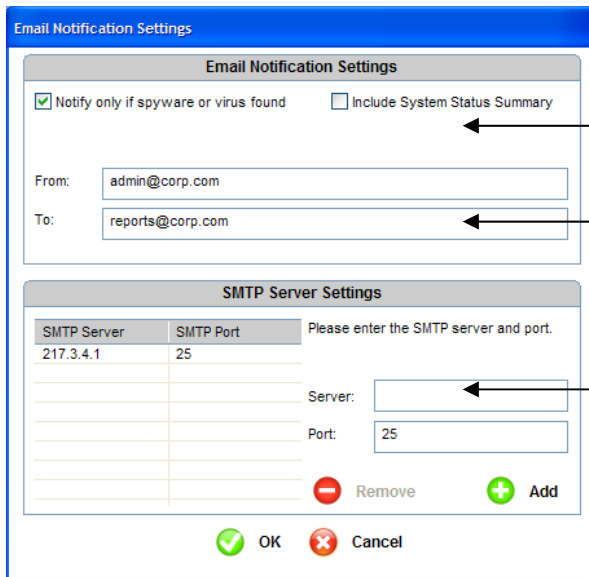


Check items to be imported

If the three configuration files are placed in the following directory "C:\Documents and Settings\All Users\Application Data\AppRanger\ExtDefn", AppRanger will automatically import them.

### Notification

AppRanger can send daily reports via e-mail. Enter the SMTP server (should not require authentication) information along with the e-mail address of the recipient.



Notification options

e-mail recipient

Enter SMTP server name or IP address and click on "Add"

## Scan

AppRanger scans the computer daily at 2AM. Time, frequency, and type of the scan can be changed here. AppRanger has four scan modes:

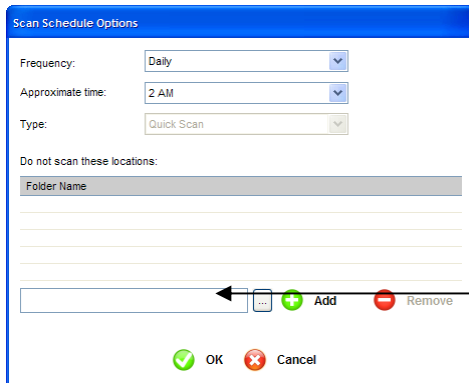
- Quick Scan
- Quick Scan with Deep Clean (recommended)
- Full Scan
- Kernel Scan (only checks for hooks in kernel)

Quick scan with deep clean can remove any malware or rootkit.

AppRanger also permits exclusion of folders from scan and can use a user defined black/white list that will override AppRanger's definitions during scan.

### Excluded folders

Enter the full path of the folder to be excluded or navigate to it and then click on "Add" button. Contents of the excluded folder will be skipped during the scan.

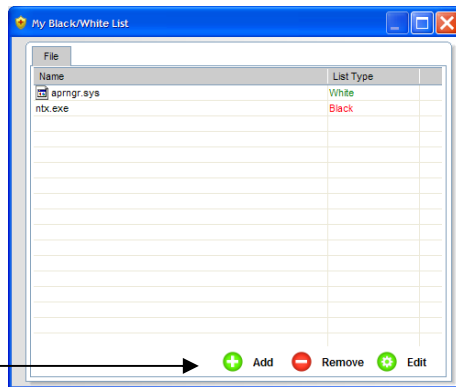


Enter path of the folder to be excluded from scan and click on "Add"

### File Black/White list

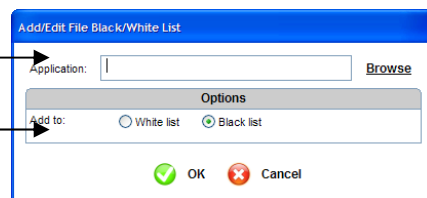
User can specify a black/white list of applications that AppRanger will use during scan and for enforcing sandbox security. Full path of the applications must be provided.

Click on “Add”  
to create a new  
black/white list  
item entry



Application name  
or full path

Application  
classification



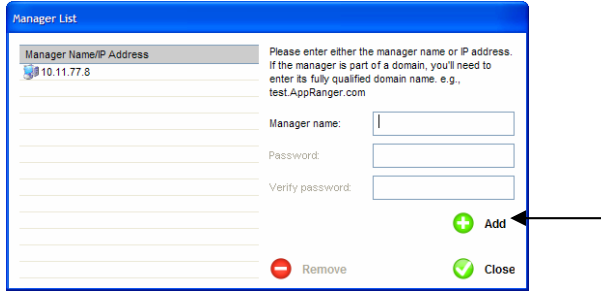
## Content

Main settings for content monitoring and filtering.

- Enable or disable Web filter
- Enable or disable Web monitoring
- Use AppRanger’s black/white list for Web filtering
- Block sites that seem suspect
- Block sites that are source of adware
- Filter our paid advertisements from search engine results

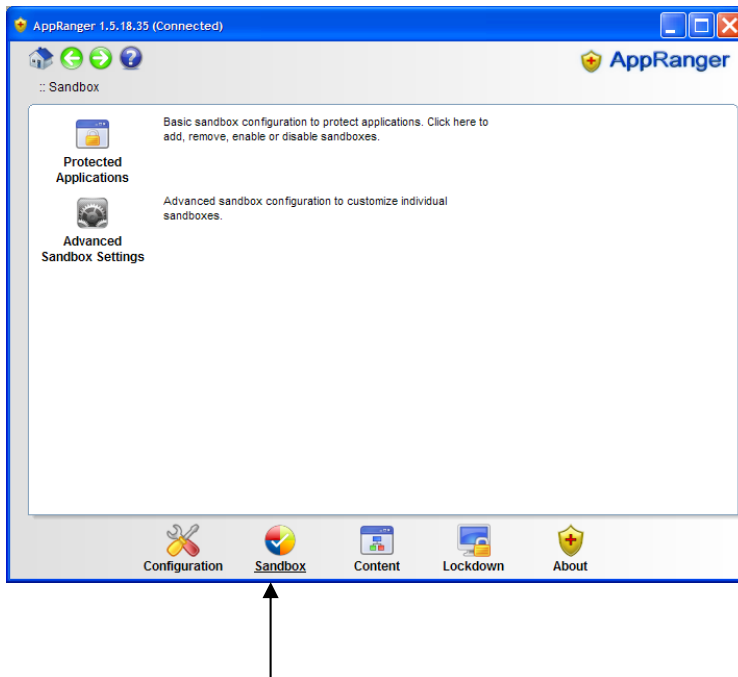
## Management

“Allow user to override sandbox” flag enables the users to use the “CTRL” or “SHIFT” key to bypass sandbox blocking of an action.



Check the “Enable central management” flag to permit central management of the policies. Any manager that can send policies to AppRanger must be in the manager list shown above. Click on “Add” button to add IP address or name of a manager to the list. If a computer is centrally managed, it will receive updates/upgrades from manager only.

## 3.3 Sandbox



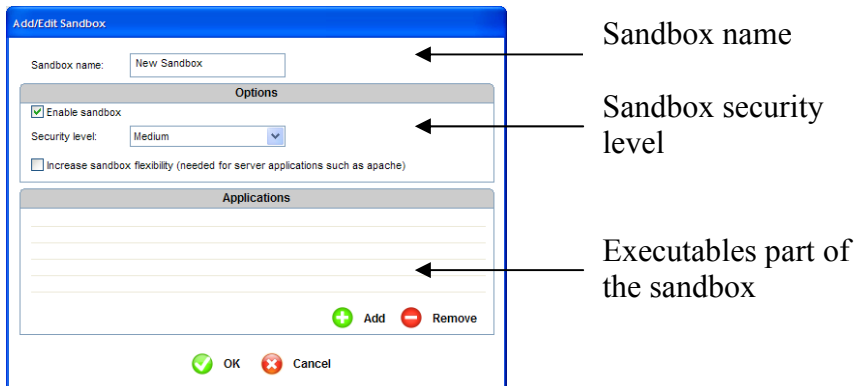
Click on the “Sandbox” icon to view, add, or change protection settings for applications.

## Protected Applications

AppRanger automatically detects common client and server applications and protects them with appropriate sandboxes.



Click on the "Add" button to add a new sandbox.



Type a name to identify the sandbox. Default security setting for new sandboxes is "Medium."

Check the "Increase sandbox flexibility" if there are several binaries in the sandbox or the protected application is a server application. Click on "Add" button to add new binaries to the sandbox.

"High" setting for AppRanger sandbox has a special anti-virus feature that prevents that application from infecting any file.

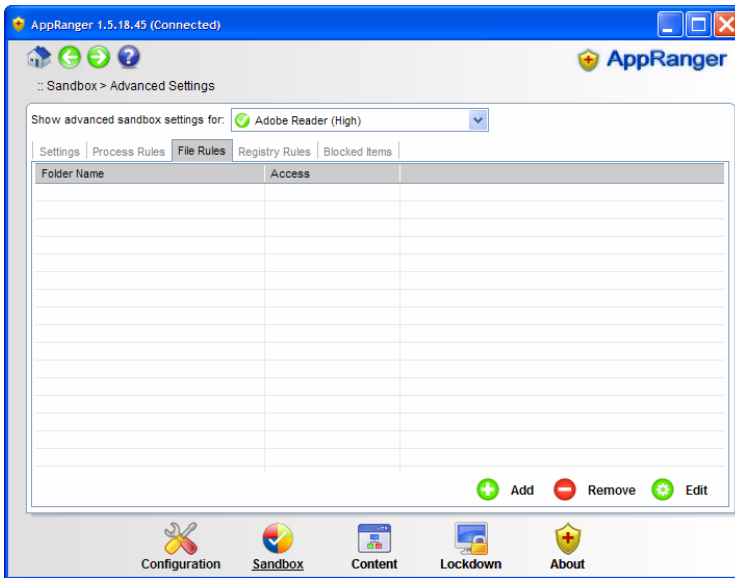
**If you download an installer via browser, do not run it directly from browser as AppRanger will block many actions of the installer. First save the installer to disk, and then run it by clicking on it.**

## Advanced Sandbox Settings

If the default security settings provided by AppRanger are not sufficient (“High” should be sufficient for even the most paranoid), one can further customize sandbox settings.

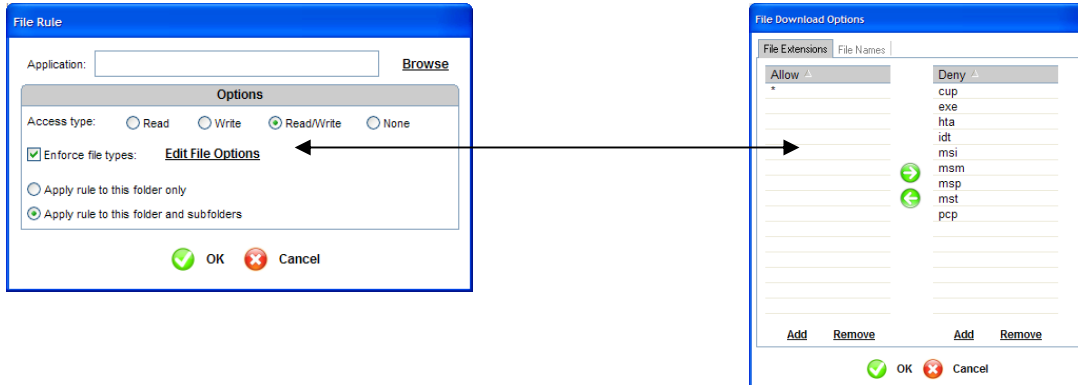


From the dropdown menu, select the sandbox you wish to customize. Click on the tab corresponding to the rule you wish to customize (file, registry, process, etc.). Add the rule by clicking on the “Add” button.

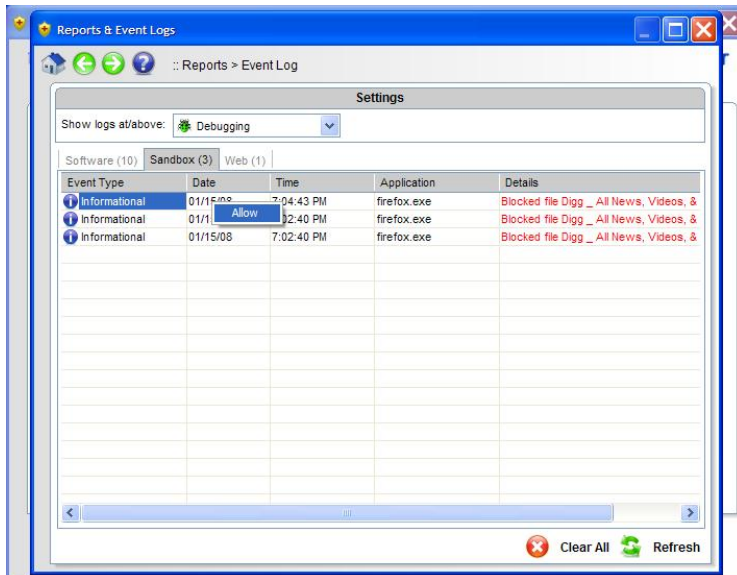


As an extension of file rules, AppRanger can block download of specific file name or extension by applications.

AppRanger can control application access to directories and type of files that can be written to those directories. Check “Enforce file types” to control which file type can be downloaded or modified by that protected application.

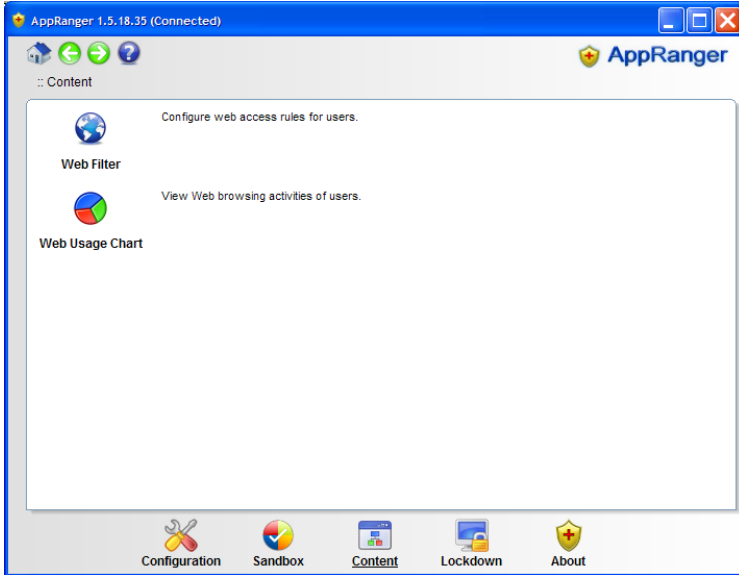


The “Blocked items” tab will show all actions blocked by the sandbox. These actions can be unblocked by right clicking and selecting “Allow.”



### 3.4 Content Filtering and Monitoring

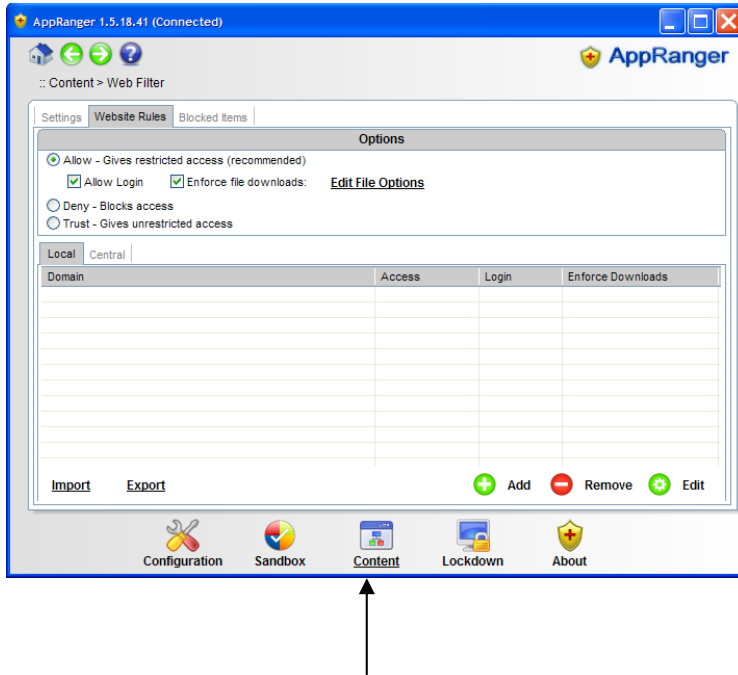
AppRanger monitors and controls Websites user can access or log onto.



Click on the "Content" icon to view AppRanger content monitoring and filtering options.

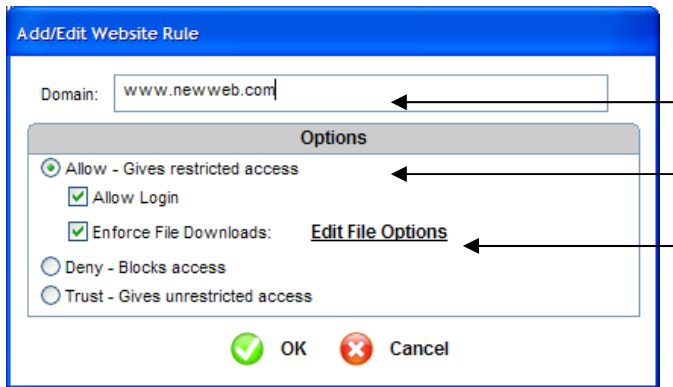
### 3.4.1 Web Filter

Control user access to Websites and block website viewing, Web logins, and content download.



Select the "Website Rules" tab to configure rules for Web access. Default setting allows access to all Web sites. The default for website access can be changed to "Deny" and then access will be permitted to only those sites for which there is a specific rule.

To add an access rule for a specific website, click on the "Add" button. Select "Allow", "Deny", or "Trust" option for access to the website. If "Trust" is selected as the access option, AppRanger will not block any activity from the URL and therefore use the "Trust" setting with utmost care.



Website URL

Access rule

{ Weblogin rule  
File download rule

To control the “weblogin” (for IE only, FF support to come soon) and file downloads from a website, click on “Edit File Options” to configure what files can be downloaded from that URL. Default setting for AppRanger allows all Web logins and blocks downloading of executable content.

If AppRanger blocks login attempts to local router/firewall and you must add the router/firewall IP address to the list and allow Web logins to it.

## 3.4.2 Web Monitoring

### Web Statistics

In addition to blocking and permitting access to Web sites, AppRanger keeps hourly statistics about all the Web sites visited by the users.

The charts show the hourly Web site usage for the users and all the Websites visited. This information can be displayed as charts at the AppRanger management console. Sites with zero page counts are typically advertisements.



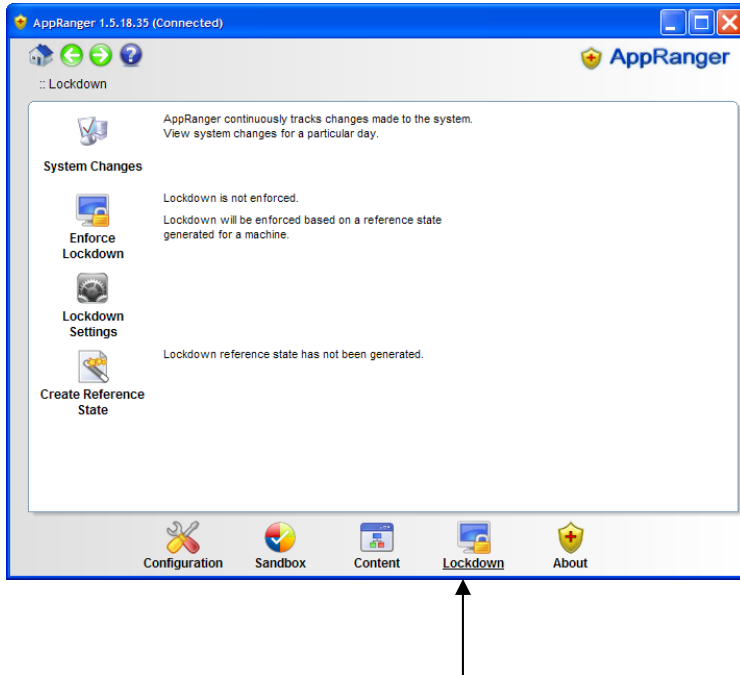
Date. Use arrows or calendar to select date

Hourly statistics. Place cursor on bar to view the URL

Total time spent and pages viewed on each website.

## 3.5 Lockdown

AppRanger enables lockdown of the computer to prevent unauthorized software from running on the computer and from undesirable changes from taking place.



Click on "Lockdown" to view options for enabling and configuring lockdown options.

### 3.5.1 System Changes

AppRanger tracks and logs daily changes to the system. These changes can be viewed by clicking on the dates from the "System Changes" tab.

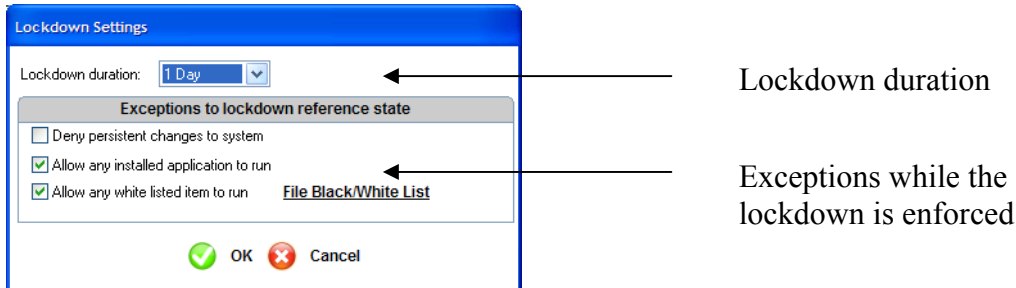
### 3.5.2 Enforce Lockdown

AppRanger will enforce the reference scan state and prevent unauthorized processes from starting and installing. When the lockdown is enforced, even the automatic update may get blocked unless a rule is explicitly set for automatic updates to go through.

### 3.5.3 Lockdown Settings

Exceptions can be made to allow known good applications to run during lockdown. AppRanger default duration for enforcing lockdown is one day, but this duration can be increased.

To prevent installation of any new programs, check the “Deny persistent changes to system” flag.



### 3.5.4 Create Reference State

Click on this button to create a baseline reference state of the computer. AppRanger will use this reference state to track system change and to enforce lockdown.

## 3.6 About

Click on “About AppRanger” tab to view the product information. From this page, the user can activate the AppRanger license, upgrade the software, update the definitions, and restore the AppRanger settings to the factory default.

### 3.6.1 Reset

To restore AppRanger settings to factory defaults, click on “Reset.”

### 3.6.2 Upgrade

To manually upgrade AppRanger to the latest version, click on “Upgrade.”

### 3.6.3 Live Update

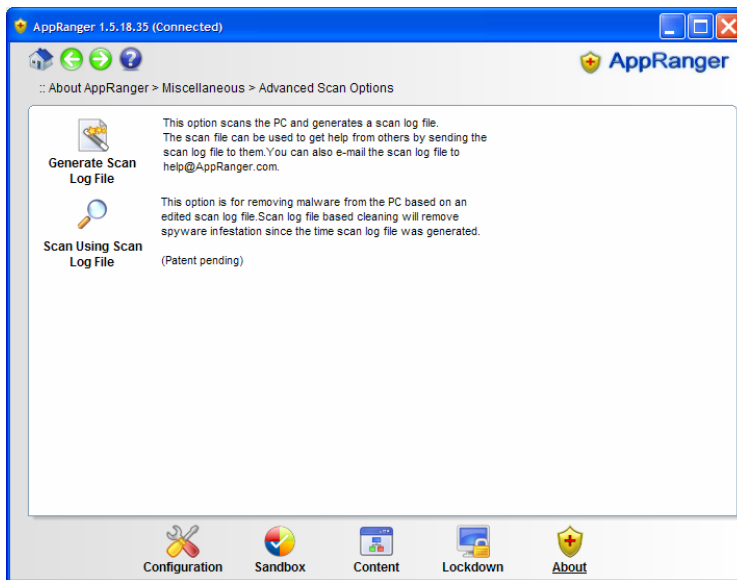
Manually upgrade AppRanger definitions to the latest version by clicking on the “Upgrade” button.

### 3.6.4 Miscellaneous

Under the “Miscellaneous” section are four advanced options:

- Advanced scan
- Additional activation options
- Behavior monitor settings
- Behavior analysis

## Advanced Scan Options



### Generate Scan Log

If the user is unable to remove malware from the PC because one of the malware is not in AppRanger's database and the user is not able to manually identify it, then use the generate scan log option to create a snapshot of your PC.

This option scans the PC and generates a log file that lists all the known malware and suspect items. It also lists items that will survive reboot. Send the Scan log file to AppRanger if you have Platinum support or show it to an expert who can identify malicious items and mark them for removal. Once malicious items have been identified, the same Scan log file can be used to clean the PC of malware.

### Scan and Clean Using a Scan Log File

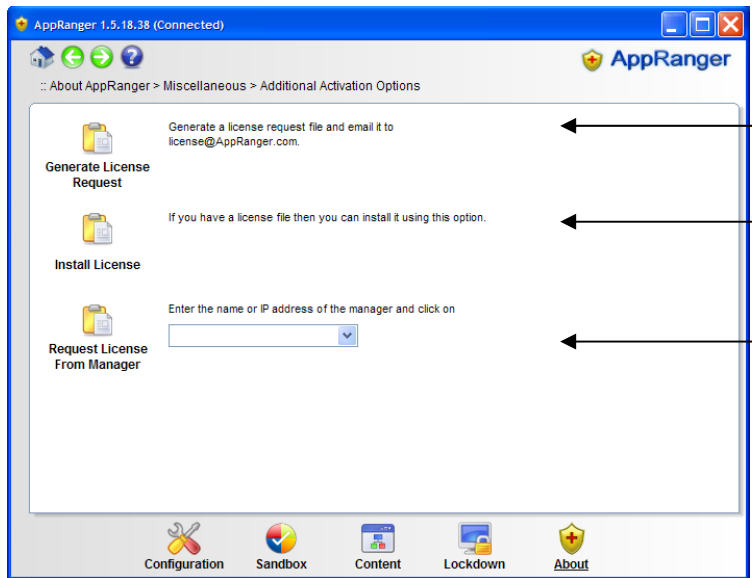
This is another unique and patent pending feature of AppRanger.

This option should be selected if you have a scan log file that has been edited and malicious items have been marked for removal. Select this option and you will be

prompted to provide the located of the edited Scan log file. After the file is read in, AppRanger will display a list of items that will be removed. Please audit the list carefully. AppRanger will then use the “Malware Freeze” technology to automatically remove the malware.

As a safety feature, the Scan log file can only be used to clean the PC it was originally generated on.

## Additional Activation Options



The screenshot shows the AppRanger 1.5.18.38 (Connected) window. The main content area is titled "Miscellaneous > Additional Activation Options" and contains three sections:

- Generate License Request:** "Generate a license request file and email it to license@AppRanger.com." An arrow points to this section with the label "Click here to generate license request file".
- Install License:** "If you have a license file then you can install it using this option." An arrow points to this section with the label "Click here to install license file".
- Request License From Manager:** "Enter the name or IP address of the manager and click on" followed by a text input field and a dropdown arrow. An arrow points to this section with the label "Enter the IP address or name of the manager and click on 'Request License from Manager' button".

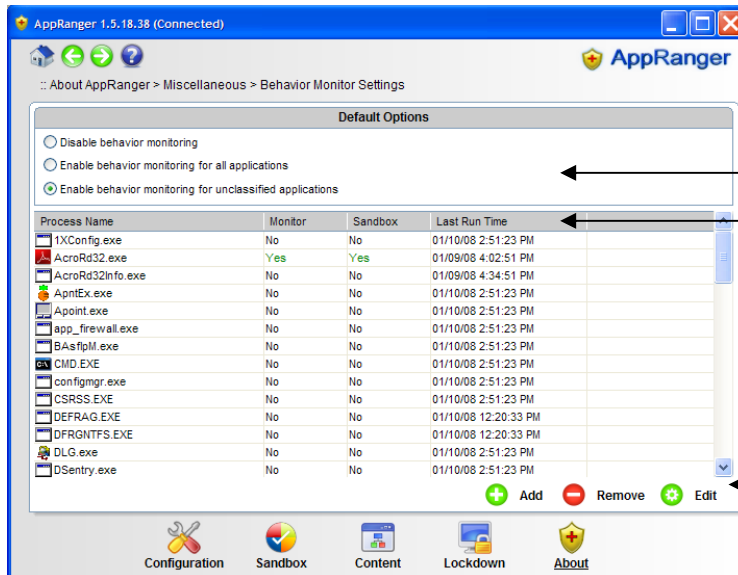
At the bottom of the window, there is a navigation bar with icons for Configuration, Sandbox, Content, Lockdown, and About.

In addition to the 25-digit key based activation, AppRanger offers two more activation options.

First option is to generate a license request file and e-mail it to [info@appranger.com](mailto:info@appranger.com).

Second option is applicable to enterprise users that have a central management station for AppRanger. Enter the IP address of name of the central management station and click on “Request License From Manager” to obtain the license.

## Behavior Monitor Settings



1- Select setting for application behavior monitoring

2- List of applications seen by AppRanger

3- To change behavior monitor setting for application, select application and click on edit

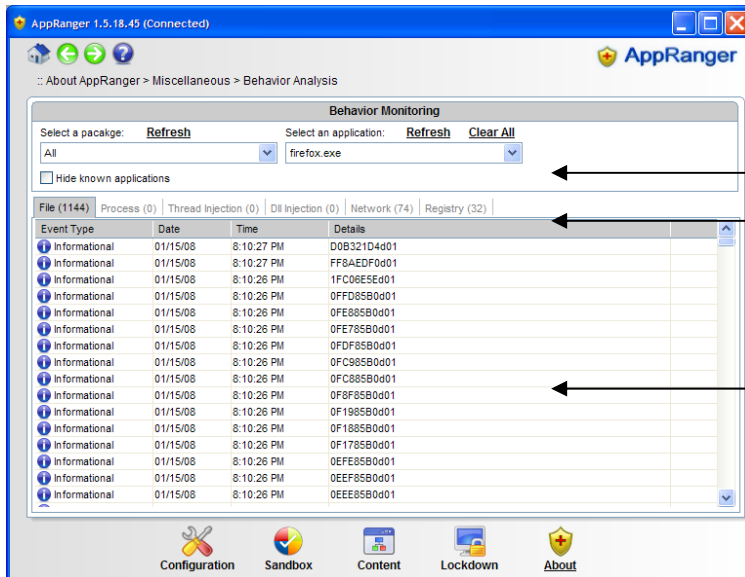
Default setting for AppRanger is to monitor behavior of all “sandboxed” and “unclassified” applications. There are two more options for default settings:

- Monitor behavior of all applications
- Disable behavior monitoring

Setting the default to monitor behavior of all applications results into increased memory usage.

Custom settings can be applied for monitoring or ignoring behavior of applications. Select the application in the list and click on “Edit” to configure behavior monitoring setting for that application.

## Behavior Analysis



1- Select application. Click on “Refresh”

2- Select appropriate tab to view application behavior

3- Double click to view action details

To view the behavior of applications running on the computer, click on the “Behavior Analysis” button under “Miscellaneous” section. Select the application who behavior you wish to view from the drop down menu and then click on the “Refresh”. AppRanger will show the observed behavior of that application in the tabs.

AppRanger does not show the white listed applications in the drop down menu. Uncheck the “Hide known good applications” to view white listed applications in the drop down menu.

Double click on any displayed entry for application behavior action to view details.

Click on “Clear All” to clear the cache that keeps the observed behavior results.

# Chapter 4 — Frequently Asked Questions (FAQ)

Basic FAQ

## **What is AppRanger?**

AppRanger is a security solution that protects servers against hacks. AppRanger finds and removes rootkits, protects server applications against attacks, tracks changes to the server, and helps in reporting for HIPPA, PCI, and SOX compliance.

## **Do I need AppRanger if I have anti-virus on my server?**

Yes. Security for servers requires a much more comprehensive and sophisticated approach and anti-virus does not address them. AppRanger not only addresses the key server security issues, it also overcomes the ineffectiveness of anti-virus against newer attacks, malware, and rootkits.

## **Do I need AppRanger if my server is behind a firewall?**

Yes. Firewalls are ineffective against attacks that target server applications. AppRanger will protect your server applications against attacks and 75% of all attacks are via applications.

## **Will AppRanger help in preventing Citrix servers from getting infected due to users clicking on malicious links?**

Yes. AppRanger will block attacks that come in via applications like the Web browsers, e-mail, IMs, etc. With AppRanger protection, the server will not get infected even if a user clicks on a malicious link or opens an infected attachment.

## **Does AppRanger work with VMware?**

Yes. AppRanger protects servers operating in a virtualized environment. With AppRanger protecting the servers, attacks on server applications and zero-day worm attacks can be blocked even if patches have not been applied.

## **How do I download AppRanger?**

[Click here](#) to download

## **What platforms are supported by AppRanger?**

Currently AppRanger only supports 32-bit versions of Windows (W2K, XP, Vista, W2K3).

## **How do I upgrade AppRanger?**

AppRanger automatically upgrades itself periodically. To manually upgrade AppRanger, click on the "Upgrade" button in "Miscellaneous->About AppRanger."

## **How do I activate AppRanger license?**

Start AppRanger, enter the 25-digit activation code, and click on "Activate" button.

## **AppRanger has blocked something I was trying to do. How do I allow that action?**

Right click on the AppRanger icon in the tray and select "View Blocked Actions." Find the event that was blocked, right click on the event and select "Allow." After that AppRanger will add a rule and that action will not be blocked.

## **I used AppRanger to scan my server and found several items in the "Unclassified list." What should I do?**

Items in the "Unclassified list" may or may not be bad. Please exercise caution in deleting items from the "Unclassified list" as you may end up deleting key items and cause system instability. Before you mark any item in that list for deletion, double click on it to view its properties.

## **I used AppRanger to scan my server and found some items that say "IDT compromised" and "SSDT compromised." What does this mean?**

If AppRanger scan shows say "IDT compromised" or "SSDT compromised," then you either have an anti-virus program installed on the server or you have a rootkit.

## **Advanced FAQ**

### **I get error 1721/2 when I try to install AppRanger?**

This error happens if the user installing AppRanger does not have administrative privileges or some other software block AppRanger from installing correctly.

### **How can I upgrade the AppRanger software?**

Right click on the AppRanger icon in the tray and select “Check for Upgrades.” AppRanger will check for software and definition updates.

### **How do I disable AppRanger?**

Right click on the AppRanger icon in the tray and select “Disable AppRanger.”

### **How can I prevent a user from changing the settings for AppRanger?**

Password protecting the AppRanger application from the “Configuration” tab.

### **How can I prevent users from downloading executables via the browser?**

AppRanger blocks download of executable files.

### **How do I remove spyware/malware/rootkits using AppRanger?**

Start AppRanger application and click on the “Scan” button. After the scan finished, check all items in the “Malicious” list. Examine items in “Unclassified” list and, if you are really sure, check the items from the unclassified list that you wish to be removed. Click on “Clean” button. AppRanger will remove malicious items and reboot the PC. Ignore all warnings while the PC shuts down.

### **What is “Malware Freeze”?**

“Malware Freeze” is a patent pending method developed by AppRanger to get rid of spyware and rootkits that are otherwise impossible to remove.

### **I am unable to access a Website?**

If AppRanger is blocking access to the Website there will be a log in the event logs. Right click on the AppRanger icon in the tray and select “View Blocked Actions.” Navigate to the “Web” tab, find the blocked event, right click on it and select “Allow.”

### **I am unable to download a file?**

Default of AppRanger is to block download of executables (.exe, .dll, .bat) and installer (.msi, .msm, .msp, .mst, .idt, .cub, .cab, .inf, .pcp).

Right click on the AppRanger icon in the tray and select “View Blocked Actions.” Navigate to the “Web” tab, find the blocked event, right click on it and select “Allow.”

### **Can AppRanger reduce advertisements displayed on a Web page?**

Yes. AppRanger has an internal list of several thousand adware sites. To block these sites, enable the “Block known adware sites” option from “Content→Web Filter” tab.

AppRanger can also filter the advertisements from search engine results.

### **How do I activate AppRanger client license?**

AppRanger client license can be activated manually at the client or from the AppRanger central manager. To activate the license manually at the client:

#### Method 1

- Start AppRanger application. Enter the 25 character key (5 characters in each edit box), and click on the "Activate" button

#### Method 2

- Install AppRanger.
- Generate license request file by clicking on "Generate license request" button in "About→Miscellaneous→Additional Activation Options" tab. Send the file to [info@AppRanger.com](mailto:info@AppRanger.com)
- Install the received license file by clicking on "Install license" button in "About→Miscellaneous→Additional Activation Options" tab

#### Method 3

- Install AppRanger. Start AppRanger application.
- Navigate to "About→Miscellaneous→Additional Activation Options" tab.
- Enter the name or IP address of the central management node
- Click on "Request license from manager" button

### **How can I add sandbox for a custom application?**

Start AppRanger application and click on the "Sandbox" icon. Click on "Protected Applications" tab and then on the "Add" button. Provide the name of the sandbox, select the security level, and enter application path.

### **What is the recommended security level for sandbox?**

Recommended security level for sandboxes is "Medium."