Table of Contents

Chapter 1: Introduction

Welcome! VIPRE® Antivirus Premium offers PC users security against more complex and malicious threats with its powerful anti-malware protection, while eliminating the performance and resource problems of many older, traditional antivirus products. The solution combines antivirus, antispyware, anti-rootkit and other technologies into a seamless, tightly-integrated product.

VIPRE (Virus Intrusion Protection Remediation Engine) is uniquely designed to reduce computer frustration with its low system resource usage, faster boot times, few popups, and a broad-range of detection and remediation of viruses, trojans, worms, and spyware.

There are three ways to get information about VIPRE Premium:

The **Quick Start Guide** only covers the basic steps needed to get VIPRE Premium up and running—protecting your computer from viruses, malware, and other unwanted applications right away.

The **Help** is your primary resource for answers to questions you may have while using VIPRE Premium. The Help contains overviews and procedural information about the tasks you can perform in the application, as well as descriptions of each screen and dialog box in the application with detailed information about each field they contain. Whenever you want to know about a screen or dialog box that you are in, you can press F1 on your keyboard or click the **Help button** 

. The applicable help topic will display for that screen.

This **User Guide** contains the same information as the Help structured in a way that is to be used as a reference manual.

http://www.sunbeltsoftware.com/support
support@sunbeltsoftware.com
Toll-free Technical Support: 877-673-1153

System Requirements

Your computer must meet the following system requirements in order to run the application effectively:

Note: This product should not be installed on any type of storage media that may be inaccessible at times. This includes network drives, removable drives, hot- swappable drives, and USB and FireWire (IEEE 1394) drives that may be disconnected.

- Supported Operating Systems:
  - Windows 2000 SP4 RU1
  - Windows XP SP1+ (32- & 64-bit)
  - Windows 2003 Server SP1+ (32- & 64-bit)
  - Windows Vista, Vista SP1+ (32- & 64-bit)
  - Windows 7 (32- & 64-bit)
  - Windows Server 2008+ (32- & 64-bit)

    Note: Installation is not supported on Windows 95, 98, ME, NT 4, Win 2000 prior to SP4 RU1, XP with no SP, Macintosh or Linux computers.

- 400MHZ Computer with 512MB of RAM (memory) and 150MB of available free space on your hard drive.
- Miscellaneous:
  - Microsoft Internet Explorer 6.0 or higher
  - Internet access for definitions updates (Broadband recommended)
  - 2x CDROM if you are having the CD shipped to you (not necessary for online download)
- Supported Email Clients (applies to Email Protection):
  - Outlook 2000+
  - Outlook Express 5.0+
  - Windows Mail on Vista
  - Windows Live Mail
  - SMTP/POP3 (Thunderbird, IncrediMail, Eudora, etc.)
  - SSL supported in Outlook and Outlook Express only

Threats to your Computer

Each year the number of threats to your computer increase exponentially and become more and more complex. This complexity has been categorized into several types. These types are often referred collectively as "malware." Malware, short for malicious software, is clearly hostile or harmful functions or behavior that is used to compromise and endanger individual computers, as well as entire networks. Some common types of malware include adware, rootkits, spyware, trojans, viruses, and worms.

What is adware?

Adware, also known as advertising software, is often contextually or behaviorally based and tracks browsing habits in order to display third-party ads that are meant to be relevant to the user. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results.

What is a rogue security program?

A rogue security program is software of unknown or questionable origin, or doubtful value. A rogue security program usually shows up on websites or SPAM emails as intrusive warnings that claim that your computer is infected and offer to scan and clean it. These should never be trusted. Reputable antivirus or antispyware companies will NEVER use this way of "notifying" you. A rogue security program may appear like an ordinary antivirus or antimalware program, but will instead attempt to dupe or badger you into purchasing the program. While some rogue security programs are the equivalent to "snake oil" salesman resulting in no good, others may actually result in harm by installing malware or even stealing the credit information that you enter and possibly resulting in identity theft. Further, you need to be cautious about closing or deleting these alerts, even when you know they're fake. Tips to protect yourself from fake antivirus programs.

What are rootkits?

A rootkit is software that cloaks the presence of files and data to evade detection, while allowing an attacker to take control of the machine without the user's knowledge. Rootkits are typically used by malware including viruses, spyware, trojans, and backdoors, to conceal themselves from the user and malware detection software such as anti-virus and anti-spyware applications. Rootkits are also used by some adware applications and DRM (Digital Rights Management) programs to thwart the removal of that unwanted software by users.

What is spyware?

Spyware is software that transmits information to a third party without notifying you. It is also referred to as trackware, hijackware, scumware, snoopware, and thiefware. Some privacy advocates even call legitimate access control, filtering, Internet monitoring, password recovery, security, and surveillance software "spyware" because those could be used without notifying you.

What is a trojan?

A trojan is installed under false or deceptive pretenses and often without the user's full knowledge and consent. In other words, what may appear to be completely harmless to a user is in fact harmful by containing malicious code. Most trojans exhibit some form of malicious, hostile, or harmful functionality or behavior.

What is a virus?

A computer virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as CD-ROMs or flash

drives. Viruses can also spread via email through infected attachments and files. Most viruses include a "payload" that can be anywhere from annoying and disruptive to harmful and damaging; viruses can cause system damage, loss of valuable data, or can be used to install other malware.

What is a worm?

A worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike viruses, however, worms spread without attaching to or infecting other programs and files. A worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through email by sending copies of itself to everyone in the user's address book. A worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some worms may be used to compromise infected machines and download additional malicious software.

Key Features

VIPRE Premium has several key features to protect your computer from malware:

VIPRE Premium core engine

The heart of VIPRE Premium is its core engine, which is used in all of VIPRE Premium's protection methods—email protection, real-time protection, and scans. The core engine works at detecting and removing malware with three layers of detection:

Signature detection

Signature detection is when an exact match is detected against a known good or bad (malware) file. Bad files are immediately blocked to ensure that your computer is not infected; good files are allowed.

Heuristic detection

Heuristic detection is characteristic detection. Heuristics look for known bad patterns inside a file. For example, let's say that a new variation of an existing malware program is released. VIPRE already knows characteristics of the existing file. So, it can use that information to catch the new variation.

Behavioral detection

Behavior detection looks at how a program actually behaves. For example, many malware programs do predictable things to your computer system, such as change your homepage on your browser or insert certain information on your computer.

Security Risk Database

The security risk database contains definitions of known threats and known goods—often referred to as the whitelist and blacklist. The three detection methods use definitions, of which are constantly being updated by SunbeltLabs™ with the help of ThreatNet. For VIPRE Premium to be effective in keeping your computer free from malware, it is important that the frequent updates are downloaded. See Getting Definition and Software Updates for more information.

Scans

Generally, a scan consists of VIPRE Premium reading your computer's drive(s), determining what is a threat, and then either removing or quarantining that threat. The scope of a scan can be customized to target specific areas or files on your computer and can be triggered various ways, including manually and automatically at scheduled times. See About Scans for more information.

Scans are performed based on the VIPRE Premium and MX-Virtualization engines.

VIPRE Premium engine

VIPRE Premium (Virus Intrusion Protection Remediation Engine) is uniquely designed to reduce computer frustration with its low system resource usage, faster boot times, few popups, and a broad-range of detection and remediation of viruses, trojans, worms, and spyware.

MX-Virtualization engine

MX (Malware Execution)-Virtualization is a new heuristic detection technique for finding malware by running a suspect program in a controlled setting (emulated environment) that is isolated from doing any harm to the PC. This emulated environment uses only a small amount of memory and mimics many core Windows functions, such as the Windows registry, file system, and communications interfaces to see what the malware is trying to do. The actions of the malware are then analyzed for behavioral characteristics common to malware. By analyzing malware in this fashion, VIPRE

Premium is able to detect many types of malware without the necessity of creating a constant stream of dedicated unpackers and signatures for each variant of a piece of malware.

Active Protection

Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system.

Email protection

Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything. When an infected email attachment is detected, VIPRE Premium will attempt to clean it, ridding the attachment of its infection. If the infection is so severe that it cannot be cleaned, the entire attachment is quarantined. VIPRE Premium notifies you of detections and any actions that may be required by you.

FirstScan

FirstScan is a cleaner that runs at boot time (when your computer is booting up/turning on). This proprietary technology bypasses the Windows operating system to remove malicious hidden processes, threats, modules, services, files, Alternate Data Streams (ADS), rootkits, and registry keys on your computer. FirstScan does not run every time you start your computer; instead, it is only triggered by a locked malware file during the cleaning after a scan.

ThreatNet

ThreatNet™ is a worldwide network of thousands of CounterSpy®, VIPRE Antivirus, and VIPRE Antivirus Premium users sharing and identifying potentially dangerous program files (both through manual submissions and automatically), resulting in the blocking of new malware almost as quickly as it is released into the wild. ThreatNet also enables Sunbelt Software to track new outbreaks and compile statistical information.

VIPRE Premium Firewall

The VIPRE Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. It can be run in either "Simple" or "Learning" modes. See About the Firewall for more information.

Tips to protect against fake antivirus programs

Use of fake antivirus and antispyware software is a fast growing scam, especially as more people become aware of the dangers of spyware, adware, and malware. By following the tips below you can better protect yourself from becoming the next victim of scams, identity thieves, and hackers.

Tips to protect you against fake (rogue) antivirus programs:

- Set the security settings of your browser (e.g. Internet Explorer, Firefox, etc.) to a higher level and keep it always up to date with security patches.
- Keep your computer up to date with the latest antivirus AND antispyware software.
- Never open an email attachment unless you are POSITIVE about the source.
- Avoid questionable websites. Some sites may automatically download malicious software onto your computer.
- Although fake security software may closely resemble the real thing, it's rarely an exact match. Look for suspicious discrepancies.
- Do NOT click on any popup that advertises antivirus or antispyware software. Fake antivirus programs often mimic well-known brands such as AVG, McAfee, and Norton. For a frequently updated list of fake programs, go to SunbeltLabs™ and search for "rogue security program." You can also visit the Rogue Antispyware blog for discussions on the latest fake security software threats.
- If a virus alert appears on your screen, do NOT click on it with your mouse to attempt to close or cancel it. Instead, on your keyboard press Ctrl + Alt + Delete to view a list of Applications currently running. Select the browser (e.g. Internet Explorer, FireFox, etc.) that just displayed the alert from the list of running Applications, and click End Task. This will safely close the browser without installing the fake program, allowing you to reopen it and continue using the program.
- Do not download freeware or shareware unless you know it's from a reputable source (e.g. Download.com). Often, freeware and shareware programs come bundled with spyware, adware, or fake antivirus programs.

If your computer seems to be infected by rogue software, stop work immediately and run a deep system scan. If you continue to use the infected computer, you may further damage the machine and provide identity thieves with more information about you. Don't hesitate to contact Sunbelt's Technical Support (877-673-1153) for assistance.

Starting VIPRE Premium

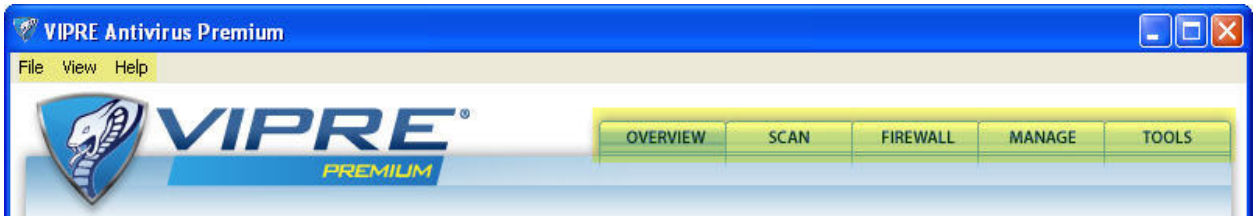
You can start VIPRE Premium two ways:

- Double-click the **VIPRE Premium** icon shortcut (pictured below) on your desktop.

- Click **Start** and then select **Programs>Sunbelt Software>VIPRE Antivirus Premium>VIPRE Premium**.

Touring the VIPRE Premium Interface

The VIPRE Premium interface uses tabs to display screens from which all work is completed. In addition to the tabs there are also links on the Overview page that open the same pages as the tabs.



Toolbar Menu

The standard toolbar menu offers one way to access functions within VIPRE Premium. Options include:

- **File**: Allows you to open the Settings dialog box where you can configure all of the detailed settings, or Exit VIPRE Premium.
- **View**: Allows you to go directly to whichever screen you need to. (See list under Tabs below for all screens.)
- **Help**: Allows you to open the Help system, run the Setup Wizard, send a file to Sunbelt Software for analysis, register VIPRE Premium, or view the About VIPRE Premium dialog box.

Note: Clicking the **Help** icon in the lower-left corner of the screens displays the help topic for the screen in which you are currently working.

Tabs

The four tabs contain the main functions of the system, with some tabs containing sub-areas that link you to other screens. The breakdown is as follows:

Note: For more information on any VIPRE Premium screen or dialog box, refer to Appendix II.

- **Overview**: use this screen to get a quick status look at VIPRE Premium and to quickly access the application's main functions.
- **Scan**: go here to run a scan on your computer.
- **Manage**: go here to work with the results of scans and to schedule scans to run automatically.

  - **History**: allows you to work with history events, including scan, AP, email, and system events.
  - **Quarantine**: allows you to work with quarantined items.
  - **Always Blocked**: allows you to work with always blocked items.
  - **Always Allowed**: allows you to work with always allowed items.
  - **Schedule Scans**: allows you to schedule scans on your computer to occur automatically.
- **Tools**: go here to access areas of your computer that you don't normally use or see.
  - **Secure File Eraser**: allows you to add an "Erase Files" option to your Window's Explorer menu to .
  - **History Cleaner**: allows you to remove browsing and search histories from specific applications.
  - **PC Explorer**: allows you to view normally hidden settings of files, applications, and web sites based on eight different criteria within your computer.

System Tray Icons and Messages

VIPRE Premium uses icons in your system tray with different colors signifying the following:

- **Green** indicates that an active scan is running.
- **Red** indicates that the service is not running and that an error occurred.
- **Gray** indicates that VIPRE Premium is idle (not scanning) and that Active Protection (AP) and/or Email AV Protection is disabled.
- **Blue** indicates that VIPRE Premium is idle and that AP and Email AV Protection are both enabled, actively protecting your computer.
- **Yellow** is the Warning icon alerting you to events, such as the completion of a scan, an update is ready to be installed, or errors. Double-click to open the newest item in the System history.

> **Note:** If you get any errors while running VIPRE Premium, please call Sunbelt Software's Technical Support (877-673-1153).

You can hover your mouse arrow over the icons to display hover text displaying the status of VIPRE Premium. VIPRE Premium will also display messages notifying you of the status of scans and updates, as well as the most recent Definitions version and when it was downloaded.

You can also right-click on the primary icon to open/shutdown VIPRE Premium, check for updates, enable/disable Active Protection, run/abort/pause/resume a scan, as well as select to show/hide the balloon notifications.

Chapter 2: Configuring Settings

Configuring all of VIPRE Premium's settings can be done from one location - the **Settings** dialog box (**File>Settings**). Typically, once you make these configurations, you will not need to make them again.

You can make configurations to the following:

Note: These items are covered in greater detail in the sections that follow.

- **Updates**: You can check for and get updates for VIPRE Premium manually and set automatic updates to do the same at preset intervals. When VIPRE Premium checks for updates, it looks for both definitions and software, if available. See updating VIPRE Premium
  - **Proxy Settings**: If you use a proxy to connect to the Internet, enter the information here. For most home users, this screen won't apply because a Proxy is generally used in corporate networks. If you think you may need to use a proxy and do not know how to acquire the necessary information, you can consult your Internet Service Provider (ISP) or network administrator to obtain proxy information. See setting up your proxy settings
  - **ThreatNet™**: ThreatNet is a worldwide network of thousands of CounterSpy, VIPRE Antivirus, and VIPRE Antivirus Premium users sharing and identifying potentially dangerous program files (both through manual submissions and automatically), resulting in the blocking of new malware almost as quickly as it is released into the wild. ThreatNet also enables Sunbelt Software to track new outbreaks and compile statistical information. See about ThreatNet
- **Scan options**: You can run a simple scan on your computer using the default settings or you can customize how scans are run on your computer in selecting from options for running a Quick, Deep System, or Custom scan. See Scanning for malware.
- **Active Protection**: AP is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system. See configuring Active Protection
- **Email Protection**: VIPRE Premium supports the following email programs: MS Outlook 2000+, Outlook Express 6.0+, and Windows Mail on Vista. Any POP3/SMTP client is also supported. See enabling email protection
- **Power**: You can set how VIPRE Premium operates when your computer runs under certain power conditions in order to conserve battery power. See configuring power save options.
- **Firewall**: You can configure and manage your firewall settings. See configuring firewall settings.

The Settings dialog box contains tabs with each tab allowing you to configure the main settings in VIPRE Premium.

Buttons on the Settings screens are the same for each tab and include the following:

- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.

- **Apply**: Click to apply the changes made and continue working in the dialog box.
- **Help**: Click to open the Help System specific to where you are in the VIPRE Premium interface.

Getting Definition and Software Updates

To manually get updates:

From the **Overview** screen, click the **Update Now** link. VIPRE Premium checks for updates and if there are any updates available, VIPRE Premium will download and apply them. The VIPRE Premium Update Progress dialog box displays the status of the update.

Note: VIPRE Premium uses a large definitions file on your computer. The updates it gets are applied to this file. If necessary, you can completely replace this file.

To set automatic updates:

Automatic Updates will automatically update both definitions and software, if available.

1. From the **Updates** area on the **Overview** screen, click **Edit Settings**. The Updates tab in the Settings dialog box displays.
2. Ensure that the **Allow Automatic Internet Access** check box is selected. If deselected, VIPRE Premium will not be able to connect to the Internet.
3. Optionally, if you connect via a proxy, click Proxy Settings to configure the proxy.
4. Select the **Automatically check for updates** check box.
5. Click the **hours** drop-down arrow and select how frequently you want VIPRE Premium to check for updates.

   Note: It is recommended to set this to 4 hours, which is the default.

6. Click **OK** to accept changes and close the dialog box.

During the scheduled update, VIPRE Premium will apply definition updates automatically as they become available. If a software update is available, you will be prompted to install the software update.

About ThreatNet

ThreatNet™ is a worldwide network of thousands of CounterSpy, VIPRE Antivirus, and VIPRE Antivirus Premium users sharing and identifying potentially dangerous program files (both through manual submissions and automatically), resulting in the blocking of new malware almost as quickly as it is released into the wild. ThreatNet also enables Sunbelt Software to track new outbreaks and compile statistical information.

How does ThreatNet work?

When an unknown potential security risk is detected by Active Protection, you are notified with a popup in the lower-right corner of your computer screen. With ThreatNet enabled, information about that risk is then automatically sent to SunbeltLabs™. This helps to identify new security risks as soon as they occur. This information is placed into definition updates, so that it can be made available to protect users from new malware.

ThreatNet Privacy Policy

All information sent to and from ThreatNet is transmitted securely and privately. The data sent in each user's report is completely anonymous. A report only includes simple security risk signatures and the file(s) that are determined to be risks. These files will be further analyzed by SunbeltLabs™ to further improve the security risk database so that the definitions are as up to date as possible.

Note: Personal information that can associate you or your computer will NEVER be included with any sent data. For more information, see Sunbelt Software's privacy policy at sunbeltsoftware.com.

ThreatNet and your firewall

If you are running Sunbelt's SPF or VIPRE Premium Firewall:

By default, port 80 is open allowing standard HTTP web-based traffic to flow. ThreatNet and auto updates are already configured to operate through Sunbelt's Firewall.

You can access SunbeltLabs, by going to http://research.sunbeltsoftware.com.

Enabling ThreatNet

ThreatNet™ is a worldwide network of thousands of CounterSpy, VIPRE Antivirus, and VIPRE Antivirus Premium users sharing and identifying potentially dangerous program files (both through manual submissions and automatically), resulting in the blocking of new malware almost as quickly as it is released into the wild. ThreatNet also enables Sunbelt Software to track new outbreaks and compile statistical information. In addition, you can allow ThreatNet to send copies of the actual risk file for evaluation.

To enable ThreatNet:

1. From the **Updates** area on the **Overview** screen, click **Edit Settings**. The Updates tab in the Settings dialog box displays.
2. In the **ThreatNet Community** area, select the following:

   - **Enable ThreatNet so I can anonymously help identify new security risks (recommended)**: Select to enable ThreatNet and join a community of users sharing information with Sunbelt Software about potential risks.
   - **Allow ThreatNet to send risk files to Sunbelt (recommended)**: With this option selected and when VIPRE Premium discovers an unknown potential risk, this file will be automatically sent to SunbeltLabs™ for analysis. With this option not selected, risk files will not be sent.

Configuring Active Protection

Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system.

Conceptually, AP has three detection layers of defense:

- **Signature detection** is when an exact match is detected against a known good or bad (malware) file. Bad files are immediately blocked to ensure that your computer is not infected; good files are allowed.
- **Heuristic detection** is characteristic detection. Heuristics look for known bad patterns inside a file. For example, let's say that a new variation of an existing malware program is released. VIPRE already knows characteristics of the existing file. So, it can use that information to catch the new variation.
- **Behavior detection** looks at how a program actually behaves. For example, many malware programs do predictable things to your computer system, such as change your homepage on your browser or insert certain information on your computer.

To set and configure Active Protection:

Warning: When using Active Protection, ensure that there is no other real-time protection software running. This includes other antivirus applications. If there is another real-time software running, the two programs running together may cause a noticeable decrease in system performance. You will notice an improvement in system performance by running VIPRE Premium in place of other antimalware programs.

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Active Protection** tab.
3. To enable AP, select the **Enable Active Protection** check box.
   -or-
   To disable AP, unselect the **Enable Active Protection** check box. Known risks will not be stopped in real-time; instead, they will be detected during scans. Skip to step 6.
4. In the **Handling of Known Bad Programs** area, select or unselect the following:

   - **Notify me when known risks are blocked and quarantined**: select this check box to see VIPRE working as it detects, blocks, and quarantines known risks. You can work with quarantined items at a later time. Unselect this check box to not be bothered by notifications; known risks will continue to be automatically quarantined. You can view AP history periodically to view a log of what AP has detected.
   - **Check files when they are opened or copied**: This option is for a higher state of protection and should be used primarily during a malware outbreak. Select this check box for AP to automatically scan a file when it is accessed. This option applies to preset files, including EXE, INI, HLP, BAT, and others. Once checked, the Extensions button becomes active allowing you to customize the extension, if desired for advanced users. Depending on your computer system's specifications and the number of programs that run on start-up, you may experience longer start-up times.

Caution: It is highly recommended to uncheck this setting under any of the following conditions to avoid a noticeable decrease in system performance: running backups; copying or moving large amounts and/or sizes of files (i.e. music collection, videos, photo collection, etc.); defragging a drive; or, running programs that do a lot of logging.

- **Extensions**: (advanced) Once the **Check files when they are opened or copied** option is selected, this button is enabled. Click to open the AP File Extensions dialog box, which allows you to set file extensions that will be checked by AP.

5. (advanced) In the **Handling of Unknown Programs** area, click **Advanced** to open the **Active Protection Unknown Programs Settings** dialog box where you can modify the advanced AP settings.
6. Click **OK**. Your AP settings are now applied.

Disabling Active Protection

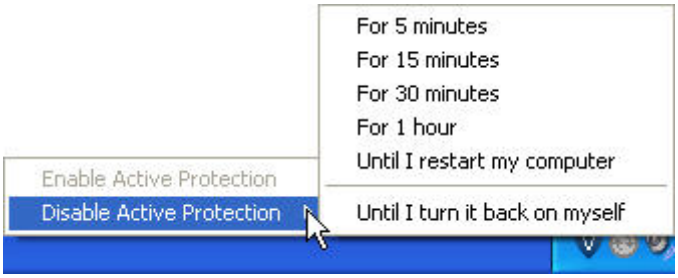
You can turn off Active Protection (AP) from the settings dialog box or from the system tray. Turning AP off from the dialog box requires you to manually turn it back on yourself when you want it on again. Turning AP off from the system tray allows you to turn it off for a designated period.

To disable Active Protection from the Settings: Active Protection tab:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Active Protection** tab.
3. To disable AP, unselect the **Enable Active Protection** check box. All of the fields in the screen will be grayed out.
4. Click **OK**. AP is now disabled.

To disable Active Protection from the system tray:

1. Right-click on the VIPRE Premium icon in the system tray and select **Active Protection**, and then **Disable Active Protection**.



2. Choose from any of the following options below for a set period of time, after which AP will be turned back on:

   - For 5 minutes
   - For 15 minutes
   - For 30 minutes

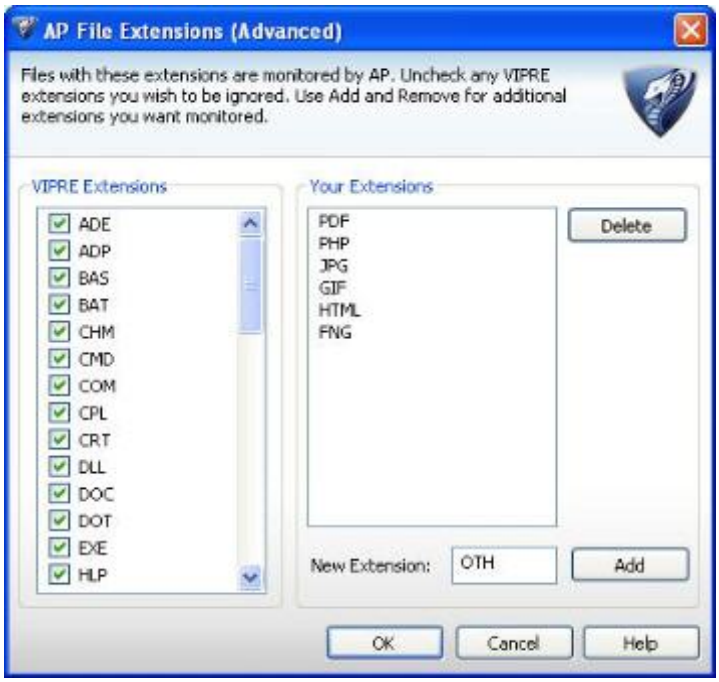
- For 1 hour
- Until I restart my computer
- Until I turn it back on myself

Note: At any time during the selected time above, you can turn AP back on.

AP File Extensions (Advanced) Dialog Box

The **AP File Extensions** dialog box is an advanced tool allowing you to that will be checked by AP. In addition to everything else that AP monitors, AP will monitor files with these extensions when they are opened, closed, or dragged/dropped onto any of your computer's drives.

This dialog box is accessible from **File>Settings>Active Protection** tab>click **Enable Active Protection**>click **Check files when they are opened or copied**>click **Extensions...** button.



This dialog box contains the following items:

- **VIPRE Extensions**: Displays the list of extensions that VIPRE will automatically check on access. Select or deselect any of the listed extensions and click **OK**.
- **Your Extensions**: Displays the list of user-added extensions that VIPRE will automatically check on access.
- **New Extension**: Enter a file extension limited to 10 characters and NO periods. It is not case-sensitive. The extension will then appear in the Your Extensions list. Wildcards are not supported.
- **Delete**: Select an extension from the **Your Extensions** list area and click **Delete**.
- **Add**: After entering the file extension, click **Add**. The extension will be displayed in Your Extensions list area.

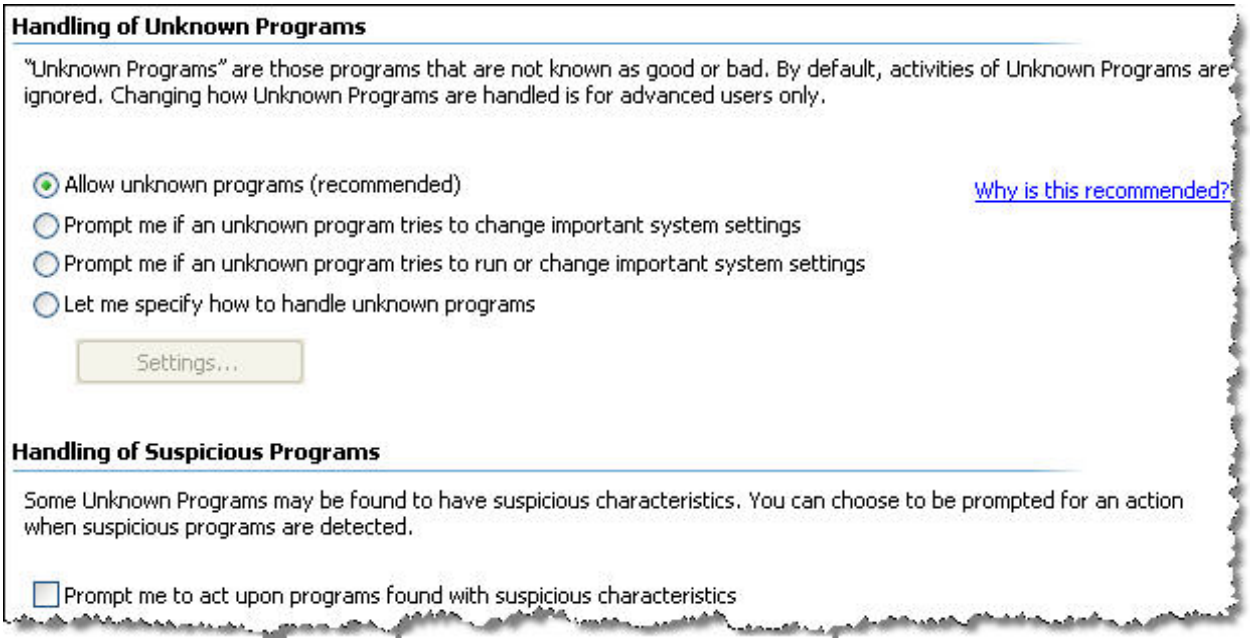
- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.

Active Protection Unknown Programs Settings Dialog Box

The **Active Protection Unknown Programs Settings** dialog box contains advanced AP settings allowing you to fine tune how AP handles unknown and suspicious programs. This dialog box is intended to be used only under extreme security conditions, such as a virus outbreak AND under careful use.

Warning: Modifying the handling of unknown programs can be risky. You may receive prompts that require you to act on certain operating system files (not easily identifiable), that if blocked can harm your computer.

This dialog box is accessible from **File>Settings>Active Protection** tab>**Advanced** button.



This dialog box contains the following items:

Handling of Unknown Programs

- **Allow unknown programs (recommended)**: This option is recommended for typical everyday computer use.
- **Prompt me if an unknown program tries to change important system settings**: Select this option only under extreme security conditions, such as a virus outbreak AND under careful use. When a computer is infected with malware, the malware will likely attempt to change system settings; however, Windows updates may do this as well.
- **Prompt me if an unknown program tries to run or change important system settings**: This is an increase in protection compared to the above option, where by you will be prompted whenever an unknown program tries to run. Select this option only under extreme security conditions, such as a virus outbreak AND under careful use.

- **Let me specify how to handle unknown programs**: Select to enable the Settings button below this selection. This option should be used by ONLY advanced users.
  - **Settings**: Click to open the Configure Active Protection dialog box.

Handling of Suspicious Programs

- **Prompt me to act upon programs found with suspicious characteristics**: Select this option only under extreme security conditions, such as a virus outbreak AND under careful use. A program may have some, but not all, characteristics typical of malware, such as how the file is compressed or where it writes information to the Windows registry. New updates that are not digitally signed or real malware can act "suspiciously." If this option is selected, you need to determine if "suspicious" files are good or bad.

Settings buttons

- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.

Configure Active Protection (advanced)

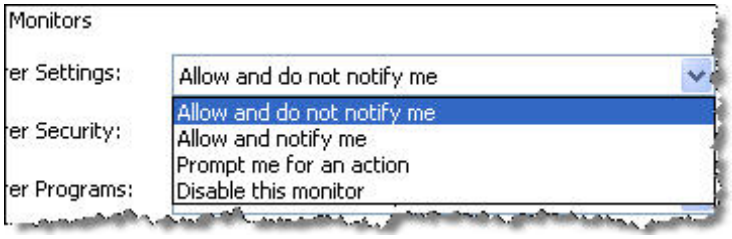
The **Configure Active Protection (AP)** dialog box allows you to set how a specific AP monitor will act when encountering an unknown program that is potentially harmful. Individual AP monitors are divided into the following areas: Internet Explorer, Windows Registry, and Windows System. You can set each one from its corresponding drop-down list option.

Warning: Individual monitors should only be modified by advanced users.

This dialog box can be accessed by selecting **File** menu>**Settings**>**Active Protection tab**>select **Enable Active Protection**>click **Advanced...** button>select **Let me specify how to handle unknown programs**>click **Settings...** button.

Drop-down list options

Note: These options are the same for all **Unknown Risk Monitors**.



- **Allow and do not notify me**: Select this option for AP to allow detected unknowns with this monitor to automatically run without notifying you.
- **Allow and notify me**: Select this option for AP to allow detected unknowns with this monitor to automatically run and to notify you that a potential risk was detected and allowed to run.

- **Prompt me for an action**: Select this option for AP to prompt you to take action when AP detects an unknown program from attempting to run.

> **Note:** This selection can result in frequent prompts, but offers the most user-control of how VIPRE Premium responds to unknowns.

- **Disable this monitor**: Select this option to completely deactivate the monitor.
- **OK**: Click to accept all changes made and close the dialog box.

Internet Explorer Monitors

Internet Explorer Settings

This monitor watches for any changes that are made to Internet Explorer (IE), including its home page, default start page, search preferences, default error pages, and handling of URL prefixes (for example, `http://`, `ftp://`, etc.). These changes could redirect you to malicious web sites that pose as being something else. It also watches for changes to your desktop wallpaper.

Internet Explorer Security

This monitor watches for changes in Internet explorer settings that could compromise some of the more secure settings. This could allow a remote Web site to exploit your computer, possibly allowing ActiveX controls to be installed with a "drive-by download". Your browser security preference settings are your first line of defense in stopping the theft or unwanted viewing of confidential, personal information. The most popular browsers offer you the ability to receive an alert or notification when any of the following occurs:

- Changes between secure and insecure transmission modes.
- Invalid site certificates (this setting notifies you when a site's SSL certificate is invalid or has expired, and an invalid certificate will deactivate SSL).
- A transmission is sent over an "open" or unsecured connection.
- A forms submittal is redirected (this setting warns you if information being submitted on a Web-based form is being sent to a Web site other than the one that you are currently viewing).

> **Tip:** To improve security with IE, you can use IE's more advanced security options. To access these options in IE, select **Tools>Internet Options>Advanced** tab. Among other choices, the Advanced tab contains a Security section that includes several configuration options pertaining to encrypted communications. Although most of the default settings are acceptable, certain security levels disable the items by default. You should enable these items: Check for publisher's certificate revocation, Check for server certificate revocation (requires restart), Do not save encrypted pages to disk, and Empty Temporary Internet Files folder when browser is closed.

Internet Explorer Programs

This monitor watches for sites being added to or removed from security zones in IE. It also watches for changes to IE's security zone settings, digital certificate store, and trusted publishers list. Changes to any of these locations could compromise the security of IE, prevent a user from accessing legitimate web sites, or redirect a user to malicious web sites. This monitor watches for changes that are initiated by unknown programs only, not users.

Windows Registry Monitors

System Startup Programs

This monitor watches for changes to system startup locations on the disk and in the Registry. System startup changes could allow a program or one of its components to start automatically with Windows.

System Policies

This monitor watches for Registry changes to system policy settings that could compromise computer security or restrict your control of Windows, IE, and your computer. Some system policy settings include the Windows task manager, anonymous user access, and Windows update.

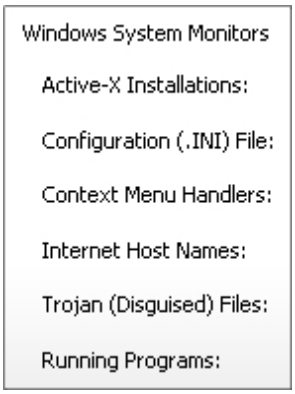
Shell Options

This monitor watches for changes in the Registry that affect how Windows handles certain file types. These changes could allow a program or one of its components to automatically open certain types of files on your computer or automatically associate it to a file type.

Windows Logon Security

This monitor watches for Registry changes to the Windows logon process. These changes could allow a new program or one of its components to start automatically with Windows and compromise the security of your computer.

Windows System Monitors



Active-X Installations

This monitor watches for ActiveX applications that are being downloaded with IE. ActiveX applications are programs that are downloaded from Web sites and stored on your computer. These programs are stored in `C:\windows\Downloaded Program Files`. They are also referenced in the registry by their CLSID, which is the long string of numbers between curly braces. IE regularly uses many legitimate ActiveX applications. You can delete most ActiveX applications from your computer without problem, because you can download them again.

Many of the current security vulnerabilities that exist in Microsoft's IE Web browser exist in the service called "active scripting". Active scripts are programs written in JavaScript, or sometimes Microsoft's VBScript and ActiveX. Active scripting can install malware on your computer. It is a method known as "drive-by downloading". While it is possible to disable active scripting completely, there are legitimate sites for which you want active scripting enabled.

For example, `http://windowsupdate.microsoft.com` (Windows Update Service) uses active scripting, as do many other legitimate Web sites. There may be Webmail sites that use active scripting. Some sites with high amounts of contents such as CNN's news site can also make heavy use of scripts. Online commerce sites such as CDW and PC Connection also use scripts in their sites. Fortunately, IE has in its design, a way to identify "trusted sites". That is, it is possible to disable active scripting on a general basis, but enable it for sites that you routinely visit, such as your Webmail or online commerce sites.

Configuration (.INI) File

This monitor watches for changes to key Windows .INI files and their equivalent Registry storage locations. Changes to an .INI file or its equivalent Registry location could allow a new program or one of its components to start automatically with Windows.

Context Menu Handlers

This monitor watches for changes to the commands or options that appear on the right-click context menus for certain files and other items in Windows.

Internet Host Names

This monitor watches for changes to the Windows HOSTS file (`C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS`), which translates Internet host names (for example, `www.example.com`) to the IP addresses (for example, `64.236.16.116`) that Internet programs actually use to access sites online. Changes to the HOSTS file could prevent you from reaching legitimate web sites or redirect you to malicious web sites.

Trojan (Disguised) Files

This monitor watches for the presence of Trojans that attempt to disguise themselves as legitimate Windows system files or that replace legitimate Windows system files with illegitimate versions.

Running Programs (Use with caution!)

This monitor watches for unknown processes or programs that are attempting to run on your computer. For typical computer use, it's best to have this set to **Allow and do not notify me**. If you want to aggressively monitor everything that runs on your computer, set this to **Prompt me for an action**. But, you could receive many prompts frequently depending on what programs are installed on your computer.

About Email Protection

What is VIPRE Premium's Email Protection and how does it work?

Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything. When an infected email attachment is detected, VIPRE Premium will attempt to clean it, ridding the attachment of its infection. If the infection is so severe that it cannot be cleaned, the entire attachment is quarantined. VIPRE Premium notifies you of detections and any actions that may be required by you.

In addition, archive files (e.g. RAR or ZIP) are also scanned in every email. If a RAR file is found to contain an infected item, the RAR file itself will be quarantined. If a ZIP file is found to contain an infected item, the infected item is removed from the ZIP file and quarantined; that infected file is then replaced by a TXT file notifying you that it was infected and that it has been quarantined.

What email programs/clients are supported by VIPRE Premium's Email Protection?

VIPRE Premium supports the following email programs: MS Outlook 2000+, Outlook Express 6.0+, and Windows Mail on Vista. Any POP3/SMTP client is also supported. When using a POP3/SMTP client, you must verify that the port settings of your email provider match VIPRE Premium's port settings. Please refer to your email provider's documentation for correct port settings. VIPRE Premium does not support the Internet Message Access Protocol (IMAP) for non-Microsoft email programs. IMAP is only supported for the Microsoft programs.

Note: If you use an Internet browser such as Internet Explorer (IE) or Firefox to access email, VIPRE Premium's Email Protection does not apply; in this case, your computer would be protected through Active Protection (AP).

How can I see what VIPRE Premium's Email Protection finds?

VIPRE Premium maintains a history of all of its detections in the View Email History screen (**MANAGE** tab>**View history** link>**EMAIL** tab). You can also view the items put in quarantine from the Quarantine screen (**MANAGE>View quarantine** link).

Enabling VIPRE Premium's Email Protection

To enable Email Protection:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Email Protection** tab.
3. Select the **Enable email protection** check box for VIPRE Premium to scan all incoming and outgoing emails.
4. Select the email program(s) that you use:

   - **I use Microsoft Outlook**: Select this option if you use this program to check your email.
   - **I use Microsoft Outlook Express or Windows Mail**: Select this option if you use either of these programs to check your email.
   - **I use another email program (Thunderbird, etc.)**: Select this option if you use a program other than a Microsoft program to check your email. Once selected, the Advanced button becomes enabled.

5. If you only selected a Microsoft option, skip to the next step.
   -or-
   If you selected "I use another email program" AND your email program requires you to change your email port settings from the default, configure the email port settings:

   - Click **Advanced**. The AV Email Settings dialog box displays.
   - Enter Email Port Settings:

     - **Inbound (POP3)**: Set this number to match both the POP3 number that your email provider uses AND what is set for your email application, as applicable. The default POP3 port is 110.
     - **Outbound (SMTP)**: Set this number to match both the SMTP number that your email provider uses AND what is set for your email application, as applicable. The default SMTP port is 25.

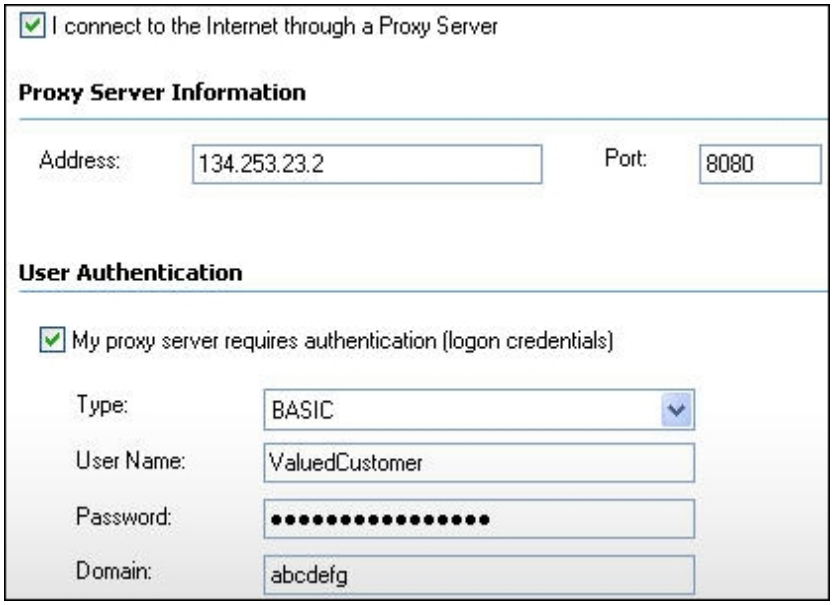
   - Click **OK**. Your port settings are saved and you are returned to the Settings dialog box.
6. Configure Anti-Phishing:

   - **Enable Anti-Phishing**: Select to enable anti-phishing. When enabled and you receive a phishing email, VIPRE strips the known bad URL link from the email, protecting you from the phishing scam.
   - **Do you want to quarantine a copy of the original email?**: Select to save an original copy of the email to the quarantine folder.

7. Click **OK**. Your Email Protection settings are saved.

Setting up a Proxy Server

If you use a proxy to connect to the Internet, enter the information here. For most home users, this procedure won't apply because a Proxy is generally used in corporate networks. If you think you may need to use a proxy and do not know how to acquire the necessary information, you can consult your Internet Service Provider (ISP) or network administrator to obtain proxy information.



To set up a proxy server:

1. From the **File** menu, select **Settings**. The Settings dialog box displays the default **Updates** tab.
2. Click **Proxy Settings**. The Proxy Settings dialog box.
3. Select the **I connect to the Internet through a Proxy Server** check box.
4. Enter the **Proxy Server Information**:

   - **Address**: Enter the IP Address (i.e. `10.3.120.3`) of a server that you are connected or the server name (i.e. OurServer).
   - **Port**: Enter the port number (i.e. `8080`) of the server that is used to connect to the Internet.

5. If the server to which you are connecting for Internet access requires logon credentials, select the **My proxy server requires authentication** check box.
6. Enter the **User Authentication** information provided by your Internet Service Provider or Network Administrator.
7. Click **OK**. Your proxy settings are enabled, allowing VIPRE Premium to establish an Internet connection.

Configuring Power Save Options

To set VIPRE Premium's behavior when your computer is asleep:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. From the **Settings** dialog box, click the **Power** tab.
3. To wake your computer when it is in sleep mode to run a scheduled scan, select **Wake from sleep on scheduled scans**. This is the recommended setting.

   -or-

   To NOT wake your computer when it is in sleep mode to run a scheduled scan, un-select **Wake from sleep on scheduled scans**.

   Warning: When you use Windows sleep mode and unselect this option, your computer may be at risk of missing important system scans, especially during periods of inactivity. To ensure that your computer is protected, you can run a scan manually or schedule a scan at a time that your computer is not asleep.

4. Click **OK** to accept changes and close the dialog box.

To set VIPRE Premium to conserve your laptop's battery:

Note: This does not apply to desktop PCs. This only applies to laptop computers.

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. From the **Settings** dialog box, click the **Power** tab.
3. Select **Power Save mode (laptops only)**.
4. Click **OK** to accept changes and close the dialog box.

Now, when your laptop is running on battery power, VIPRE Premium will not check for updates or run scheduled scans.

Chapter 3: Finding Malware

This Chapter covers all of the ways that VIPRE Premium can scan your computer in protecting it from malware, including various scans, the command line scanner, the boot time scanner/cleaner, and managing scan results.

About Scans

Generally, a scan consists of VIPRE Premium reading your computer's drive(s), determining what is a threat, and then either removing or quarantining that threat. The scope of a scan can be customized to target specific areas or files on your computer and can be triggered various ways, including manually and automatically at scheduled times.

Scopes of a scan:

Quick scan

A **Quick scan** will scan commonly affected areas of your computer. This scan is usually shorter in duration than the Deep System Scan.

Deep System scan

A **Deep System scan** will perform a thorough scan of all areas of your computer. Depending on how full your hard drive is, this could take longer.

Custom scan

A **Custom scan** is a targeted scan for very specific areas and/or types of items that you want looked at during a scan. that you to scan specific areas of your computer only, including running processes, registry files, cookies, and particular drives and folders

How a scan can be triggered:

Manual scans

A **Manual scan** is a scan that you perform on a as needed basis. If you feel you your computer may be infected or just want to insure that it isn't, running a manual scan will allow you to protect your computer.

See Scanning your computer for more information.

Automatic (Scheduled) scans

An **automatic scan** can be either quick or deep that you schedule to run at a time of your choosing. By default, VIPRE Premium is set to run a scheduled scan at 1:00 am. If your computer is not on during that time, you will want to change that time to one more suitable. You can add as many scheduled scans as you want.

See Scheduling Scans and Configuring Power Save Options for more information.

Email scanning

Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything. When an infected email attachment is detected, VIPRE Premium will attempt to clean it, ridding the attachment of its infection. If the infection is so severe that it cannot be cleaned, the entire attachment is quarantined. VIPRE Premium notifies you of detections and any actions that may be required by you.

See About Email Protection for more information.

Command Line Scanner

The Command Line Scanner is a helpful tool for the extreme occurrence that your computer becomes so infected from malware that it could become quite difficult to open any program, including VIPRE Premium.

See Running the Command Line Scanner for more information.

Scanning for Malware

You can perform three different types of scans - Quick, Deep System, and Custom - to detect and remove malware from your computer. You can run a scan using the default settings, configure quick and deep system scan options, or configure custom scan options.

Note: You can continue to use other VIPRE Premium features while running a scan.

To run a simple scan:

1. Click the **Scan** tab. The Scan screen displays.
2. Select one of the following:

   - **Quick Scan**: Select to scan commonly affected areas of your computer. This scan is usually shorter in duration than the Deep System Scan. You can configure additional options in the Scan Options tab on the Settings dialog box.
   - **Deep System Scan**: Select to perform a thorough scan of all areas of your computer. Depending on how full your hard drive is, this could take longer. You can configure additional options in the Scan Options tab on the Settings dialog box.

3. Optionally, select **Shutdown computer after scan** to have VIPRE Premium automatically shutdown your computer after the scan completes.
4. Click **Scan Now**. Your selected scan begins to run, displaying the Scan Progress screen allowing you to view the progress of the scan, pause the scan, or cancel it.

   Once the scan completes and has found risks, the **Scan Results** screen displays the detected risks with the recommended clean action listed under the **Clean Action** column. If the scan reveals no risks, skip to step 5.

5. Click **Clean**. VIPRE Premium cleans the risks based on the recommended clean action listed in the Clean Action column.

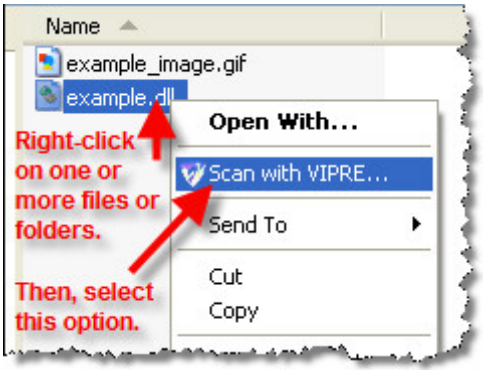
   Once the risks are cleaned, the Clean Results screen displays the details and summary of the scan.

   Note: For more information on cleaning risks, see Managing Scan Results.

6. Click **Done**. The Clean Results screen changes to the Scan screen. Your computer is now clean of viruses and malware.

Note: After the cleaning is finished, you may be prompted to reboot your machine and run VIPRE Premium's Boot Time Cleaner in order to completely remove a "hard to remove" risk.

You can right-click on one or more files or folders from Windows Explorer to run a scan.



To configure Quick and Deep System scan options:

You can select and deselect settings for all three scan types.

1. Click the **Scan** tab. The Scan screen displays.
2. Click the **Scan Options** link at the bottom of the screen. The Settings dialog box displays the Scan Options tab.
3. In the **Settings for all scans** area, select what each of the three scan types will include during a scan. Select a check box under the scan type(s) for the corresponding row, listed below:

- **Enable rootkit detection**: Select to include rootkits (software tools intended to conceal running processes, files or system data from the operating system).
- **Scan inside of archives**: Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined. See Working with Quarantined Items for more information.
- **Scan at a lower priority**: Select for VIPRE Premium to operate at a lower priority, allowing you to continue working with other programs without decreased performance. It's good to select this option for scheduled scans that occur during times of regular use of the computer.
- **Exclude removable drives**: Select to exclude external or temporary drives, such as flash and USB drives or external hard drives. It's best to keep this selected all times, except when you are intentionally scanning those external drives. By default, Quick and Custom scans will automatically exclude these drives.
- **Scan cookies**: Select to include all cookies on your system. This only applies to Internet Explorer (IE).
- **Scan registry**: Select for the scan to include your system's registry.
- **Scan running processes**: Select for the scan to include any program that is currently running. For example, if you have an Internet browser and an email program open, your scan will

include these running programs. If unselected, VIPRE Premium will not scan running programs.

- **Include low-risk programs**: Select to include low-risk programs. This option applies to all scan types and Active Protection.

Note: You can click **Restore Defaults** to revert back to factory settings.

4. Click **Apply** to save your settings.
5. Click **OK** to close the dialog box, returning you to the **Scan** screen.

To perform a Custom scan:

Configuring the Custom scan options is for running a scan on specific areas of your computer, outside of the options for Quick and Deep System scans.

1. Click the **Scan** tab. The Scan screen displays.
2. Select the **Custom Scan** option. The custom scan options are enabled.

3. Select one or more of the following options:

- **Scan running processes**: Select for the scan to include any program that is currently running. For example, if you have an Internet browser and an email program open, your scan will include these running programs. If unselected, VIPRE Premium will not scan running programs.
- **Scan registry**: Select for the scan to include your system's registry.
- **Scan cookies**: Select to include all cookies on your system. This only applies to Internet Explorer (IE).
- **Specify drives and folders to scan**: Select and then click **Browse** to perform a custom scan that includes a focus on specific drives, folders, and/or specific files. .

4. Optionally, select **Shutdown computer after scan** to have VIPRE Premium automatically shutdown your computer after the scan completes.
5. Click **Scan Now**. Your selected scan begins to run. The Scan Progress screen displays allowing you to view the progress of the scan, pause the scan, or cancel it.

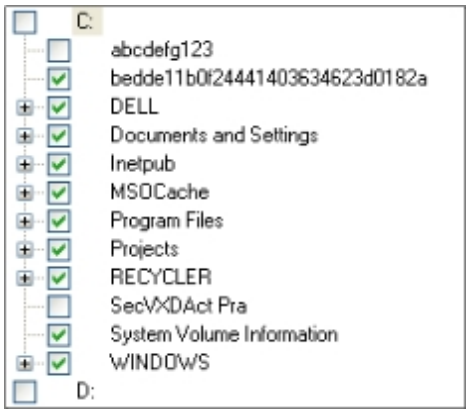
Specifying Drives and Folders to Scan

You can **Specify drives and folders to scan**: Select and then click **Browse** to perform a custom scan that includes a focus on specific drives, folders, and/or specific files. .

To specify drives and folders to scan:

1. On the **Scan screen**, select **Custom Scan**. The custom scan options become enabled.

2. Select the **Specify drives and folders to scan** check box and click **Browse**. The Select Folders to Scan dialog box displays.



3. Optionally, click the **Show Files** check box at the bottom to display files as well.
4. Check the drives you wish to scan to expand its folder list. Drill down and select the folders and/or files you wish to scan and click **OK**. The dialog box closes, and your selections display in the **Specify drives and folders to scan** list box.

Running the Command Line Scanner (advanced)

VIPRE Premium offers you the ability to run a scan from the command line scanner.

Note: Using VIPRE Premium's command line scanner is an advanced feature and should only be used by knowledgeable computer users.

The following parameters are available for the command line scanner with the syntax: `sbamcommandlinescanner.exe [parameter]:`

Parameter	Description
`/displaylocaldefversion`	gets current version number of definitions
`/displayvipreversion`	gets current VIPRE Premium software version number
`/displaysdkversion`	gets current SDK version number
`/scannowquick`	starts a Quick scan
`/scannowdeep`	starts a Deep System scan
`/updatedefs`	starts update definition
`/enableap`	enables active protection
`/applydefs [path to definitions]`	applies definitions file from a saved location

Running VIPRE Premium from the command line scanner (advanced):

1. Access the Windows Command Prompt. This can usually be opened by clicking the **Start** button and then selecting **All Programs>Accessories>Command Prompt**.
2. Verify that you are on the drive that VIPRE Premium is installed.

   The default drive is `c:`.

3. Navigate to the VIPRE Premium program folder.

   For example, `cd Program Files\Sunbelt Software\VIPRE`.

4. To display the valid syntax parameters, type `sbamcommandlinescanner`. The USAGE information is displayed, just as is displayed in the table above.
5. To run a parameter, type `sbamcommandlinescanner.exe [parameter]`.

   For example, if you want to view the current version of VIPRE Premium, type `sbamcommandlinescanner.exe/displayvipreversion`.

Warning: Once you start a scan, do NOT manually attempt to terminate it. The scan MUST be allowed to complete to avoid config errors. You will receive a notification that the scan is running. Once the scan completes, you will receive the message "`DONE:Cleaning Complete`."

Note: Scans are run based on the default settings in the VIPRE Premium interface. For example, if the Quick scan settings are set to: Include low-risk programs, Enable rootkit detection, and Scan cookies, then this is what the command line scanner will scan for when entering the `/scannowquick` command.

About FirstScan Boot Time Cleaner

VIPRE Premium's FirstScan™ is a cleaner that runs at boot time (when your computer is booting up/turning on). This proprietary technology bypasses the Windows operating system to remove malicious hidden processes, threats, modules, services, files, Alternate Data Streams (ADS), rootkits, and registry keys on your computer. FirstScan does not run every time you start your computer; instead, it is only triggered by a locked malware file during the cleaning after a scan.

Managing Scan Results

Once a scan completes, VIPRE Premium displays the **Scan Results** screen where you need to assign a clean action and clean the found risks. VIPRE Premium will automatically recommend a clean action, listed under the Clean Action column in the Scan Results table.

View the details of a risk:

1. Select a row in the table and click **Risk Details**. The Risk Details dialog box displays the details of the risk.
2. To view even more details, click **Learn More**. Your default web browser opens the SunbeltLabs™ website with more information on the risk.

Set a clean action and clean the risks:

1. Click **Select All** to set an action to all listed risks.
   -or-
   Select one or more risks.
2. To use the recommended action, click **Set Recommended Action**.
   -or-
   Click the **Set Recommended Action** down arrow  to pick from one of the following options:

   - **Recommended Action**: Allows VIPRE Premium to determine the clean action for the selected risk based on the latest definitions that are installed on your computer.
   - **Quarantine/Disinfect**: Sets the Clean Action for the selected risk to **Quarantine**. VIPRE Premium will first attempt to clean the infection in the file. If the file cannot be disinfected, VIPRE Premium will place the infected file into Quarantine. It will stay in quarantine for a default of 15 days. On the 16th day, it will be automatically deleted. You can change the amount of time it stays in Quarantine from the Quarantine dialog box. The Quarantine gives you the opportunity to further evaluate this file before removing it from your computer permanently.
   - **Remove**: Sets the Clean Action for the selected risk to **Remove**. This setting removes the selected risk permanently from your computer, and is not the recommended action. It is better to **Quarantine** a risk first, giving you the opportunity to later restore it to your computer if it turns out to not be a risk to you.
   - **Allow**: Sets the Clean Action for the selected risk to **Allow**. This setting allows the selected risk to remain on your system. It will only be allowed just this one time. It may be detected

again in future scans. If you believe this file to be acceptable to run on your computer, select **Allow Always**.

- **Allow Always**: Sets the Clean Action for the selected risk to **Allow Always**. This setting allows the selected risk to always remain on your system and VIPRE Premium will ignore it in future scans.

3. To set a restore point for system files that may have been detected as being infected, select **Create system restore point**.

   It is not uncommon for system files to become infected. Selecting this check box will enable the operating system to specify a system restore point prior to cleaning risks and deleting files. A System Restore is a Windows feature that allows you to undo harmful changes to your computer and restore it back to its original state just before the changes were made. For more information and accessing this Windows feature, go to **Start>Help and Support>**and locate **System Restore**. This restore point will be listed as "VIPRE Premium clean action." **It is a good practice to always keep this selected**.

   Note: This feature only restores system related files. It does not restore files and applications such as Hotbar. Also, Windows 2000 does not support restore points.

4. Click **Clean >**. The Clean Progress screen displays followed quickly by the Clean Results screen.

   If necessary, you can click **Cancel** to cancel the clean action and clean the risks at a later time.

   Note: After the cleaning is finished, you may be prompted to reboot your machine and run VIPRE Premium's Boot Time Cleaner in order to completely remove a "hard to remove" risk.

Chapter 4: Managing Malware

Once a scan is complete, you can use the **Manage VIPRE Premium** screen to manage the malware found during scans, email detection, and Active Protection (AP). You can also schedule scans to run automatically.

The following options are available:

- The **History** screen allows you to work with VIPRE Premium history, including scan, AP, email, and system.
- The **Quarantine** screen allows you to work with quarantine items. The Quarantine is a safe place on your computer that VIPRE Premium uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review the details of a risk and research it further and remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove the risks from Quarantine.
- The **Always Blocked** screen allows you to work with always blocked items, including reviewing all items blocked by Active Protection, view more specific details of a selected item, moving selected risks from the **Always Blocked** list to the **Always Allowed** list, or removing selected items from the list and return them to your system.
- The **Always Allowed** screen lists items that will always be ignored by both Active Protection and during a scan and allows you to work with always allowed items including adding items to this list, viewing the details of a listed item, and removing it from the list.
- The **Schedule Scans** screen allows you to schedule scans on your computer to occur automatically. Performing a Deep System Scan once a day is sufficient for most users; however, you may want to perform Quick Scans more frequently. For example, you can schedule a Deep System scan to run nightly and a Quick Scan to run once a day at a specified day of the week and time.

History Events

Any action that occurs in VIPRE Premium is recorded as a history, which includes scan, Active Protection (AP), Email, Firewall, and System. You can view and delete the history. By default, the history is stored for 15 days. On the 16th day, the history is automatically deleted. You can change the number of days that VIPRE Premium will keep the history and manually delete them.

Tip: Instead of deleting items in your history after a period of time, you can keep your scan history indefinitely and use this history to monitor your scans over long periods of time for comparisons.

To display the **View History** screen, select **Manage tab>History**.

To view history details:

1. Select either the **Scan**, **Active Protection**, **Email**, or **System** tab.
2. Select the history (row) you wish to review.
3. Click **Details**. The dialog box for the corresponding history displays.

To automatically delete VIPRE Premium history:

Performing this procedure will affect the history under Active Protection (AP), email, and system—all at once.

1. Click the **Change** link. The History Options dialog box displays.
2. Ensure the **Delete history older than** option is selected.
3. Click the up or down arrows to set the number of days you wish to keep histories and click **OK**.
   -or-
   Click inside the combo-box and enter the number of days you wish to keep histories and click **OK**.

Note: Selecting the **Keep all of my history** option disables the auto-delete function. All histories will be kept until you manually delete them.

To manually delete a history item:

From either the Scan, Active Protection, or Email tabs, select the item (row) you wish to delete and click **Delete**.

From either the Scan or Active Protection tabs, select the item (row) you wish to delete and click **Delete**.

Note: You can click **Select All** and then click **Delete** to clear the whole list for that tab only. The System tab allows you to remove all of its items by clicking **Clear All**.

Quarantined Items

The Quarantine is a safe place on your computer that VIPRE Premium uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review the details of a risk and research it further and remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove the risks from Quarantine.

To work with **Quarantine** items, select **Manage tab>Quarantine** and continue with any of the following procedures:

To view the details of a risk:

1. Select a risk from the list and click **Risk Details**. The **Risk Details** dialog box displays.
   -or-
   Double-click on a risk to display the **Risk Details** dialog box.
2. Optionally, click **Learn More** to go to SunbeltLabs™ for additional information.

To restore a risk from the quarantine list:

Select the risk(s) to restore and click **Restore from Quarantine**. The Unquarantine dialog box displays.

To delete a quarantined item from your computer:

Select the risk you wish to delete and click **Delete from Computer**. The item is permanently removed from your computer.

Note: You can click **Select All** and then click **Delete from Computer** to delete all items in Quarantine from your computer.

To set the auto delete function:

1. Click the **Change** link. The **Quarantine** dialog box displays.
2. Ensure the **Delete quarantined items older than** option is selected.
3. Click the up or down arrows to set the number of days you wish to keep quarantined items and click **OK**.
   -or-
   Click inside the box and manually enter the number of days you wish to keep quarantined items and click **OK**.

Note: Selecting the **Never automatically delete quarantined items** option disables the auto-delete function. All quarantined items will be kept until you manually delete them.

Sending Files to Sunbelt for Analysis

If VIPRE Premium quarantines a file that you believe should not be quarantined (i.e. potential false positive), you can send it to Sunbelt Software for analysis to help us improve our security risk database. You can send multiple files from the Quarantine screen or a single file from the Help menu.

Note: Personal information that can associate you or your computer will NEVER be included with any sent data. For more information, see Sunbelt Software's privacy policy at sunbeltsoftware.com.

To send a file for analysis:

...when you are restoring a file from quarantine (multiple files)

1. Open the **Quarantine** screen (click the **MANAGE** tab and then click **View quarantine**). The Quarantine screen displays a table of quarantined risks.
2. In the table of quarantined risks, locate and select the quarantined item(s) that you want to send to Sunbelt.
3. Click **Restore from Quarantine**. The Unquarantine dialog box displays.
4. Select **Send files to Sunbelt for analysis**.
5. Click **OK**. The "Files sent to Sunbelt" dialog box displays a confirmation of the sent file(s).
6. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
7. Click **OK**.

...from the quarantine risk area (multiple files)

1. Open the **Quarantine** screen (click the **MANAGE** tab and then click **View quarantine**). The Quarantine screen displays a table of quarantined risks.

2. In the table of quarantined risks, locate and select the quarantined item(s) that you want to send to Sunbelt.
3. Right-click and select **Send to Sunbelt**. The "Files sent to Sunbelt" dialog box displays a confirmation of the sent file(s).
4. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
5. Click **OK**.

...from a saved location (only one file)

1. From the **Help** menu, select **Send file for analysis**. The "Browse to a file to send to Sunbelt" dialog box displays.
2. Click **Browse** and navigate to the file that you want to send for analysis. Click **Open**. The file is displayed in the "Browse to a file to send to Sunbelt" dialog box.
3. Click **OK**. The "Browse to a file to send to Sunbelt" dialog box closes and the "Files sent to Sunbelt" dialog box displays a confirmation of the sent file(s).
4. Optionally, click **Copy to Clipboard** to copy the file that was sent for pasting into an email or any other location.
5. Click **OK**.

Always Blocked Items

Blocked Items apply ONLY to Active Protection (AP). When AP prompts you after detecting an unknown program, and you determine it to be bad, click **Block**. From then on, VIPRE Premium will always block this program from running—adding it to the Always Blocked list. You can later decide to remove it from this list. If that program is actually a program that you want to run on your computer, you can move it to the Always Allowed list.

An "unknown" is a potential risk that has yet to be established as a "known" risk by Sunbelt Software's security risk database. An unknown could be safe to *your* computer; it just has yet to be determined safe or unsafe.

A "known" risk is based on Sunbelt Software's definitions in the security risk database and has been determined as being harmful based on analysis and history of reported cases. Much of this information comes from users like you who have ThreatNet enabled. You may, however, consider a "known" to NOT be a risk to you (i.e. Hotbar). Some programs use adware that *you* may want to run on your computer. In this case, you will want to always allow it to run.

To always block a program from running on my computer:

1. Configure Active Protection, selecting either High or Medium. This will cause the VIPRE Premium Warning dialog box to display, prompting you to take action.

   Note: The Low level for AP is the "off" setting for unknown programs—AP will not prompt you when detecting an unknown program.

2. When prompted, click **Block**. The blocked item is sent to the Always Blocked list.

To view the Always Blocked screen list:

Select **Manage tab>Always Blocked**.

To view the details of a blocked item:

1. Open the **Always Blocked** screen.
2. Select on a risk and click **Risk Details**.
   -or-
   Double-click on a risk to display its details in a popup.

To move a risk from the Always Blocked list to the Always Allowed list:

1. Open the **Always Blocked** screen.
2. Select the risks you wish to move and click **Move to Always Allow**. The item will no longer be blocked the next time it is detected; instead, it will be always allowed and listed on the Always Allowed screen.

Note: To move all items in the list, click **Select All** and then click **Move to Always Allow**.

To remove a blocked item from the Always Blocked list:

1. Open the **Always Blocked** screen.
2. Select the risk you wish to remove and click **Remove From List**. The item will no longer be blocked the next time it is detected.

Note: To remove all items in the list, click **Select All** and then click **Remove From List**.

Always Allowed Items

There may be times when VIPRE Premium's Active Protection (AP) detects an unknown risk, which you determine to be safe. To avoid being prompted again, you can add this "unknown" program to the Always Allowed list. VIPRE Premium will then treat it as a "known" so that it will stop coming up in scan results and in AP prompts. You can also remove it from this list later.

To always allow a program to run on your computer:

VIPRE Premium offers you three ways to allow a program to always run on your computer without it coming up in scans or AP:

...from the VIPRE Premium Warning dialog box:

With AP enabled to a Medium or High setting, VIPRE Premium will display a Warning dialog box whenever it encounters an unknown risk.

1. Configure Active Protection, selecting either High or Medium. This will cause the VIPRE Premium Warning dialog box to display, prompting you to take action.

   Note: If you select Low, AP will not prompt you to take action when detecting an unknown risk.

2. When prompted, click **Allow**. The allowed item is sent to the Always Allowed list.

...after a scan:

1. Run a scan on your computer.
2. From the Scan Results screen, select the item you want to always be allowed.
3. Click **Set Recommended Action drop-down arrow**  and select **Always Allow**.
4. Click **Clean**. The selected item will be placed in the **Always Allowed** list and will no longer be identified as a risk during future scans.

   At any time, you can remove it from the list.

...manually from the Always Allowed screen:

1. Click **Add**. The Add to always allow dialog box displays.
2. Select one of the following:

   - **Allow an entire folder**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. For example, `C:\Example\`. All files under this directory will be allowed. If any of the files or folder(s) exists elsewhere on your system, it will not apply to this always allowed selection.
   - **Allow file by full path (wildcards ok)**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. For example, `C:\Example\example file.txt`. Only the file with this path will be allowed. If the file exists elsewhere on your system, it will not apply to this always allowed selection. The supported wildcards are "`*`" and "`?`".

- **Allow by file name (wildcards ok) only**: Select this option and click **Browse** to locate your entry. The entry will be displayed in the text box. Use this field if AP or a scan is detecting a specific file frequently. For example `Firefox.exe`. Any file with this name will be allowed no matter where it exists on your system.
- **Allow a file by its signature**: Select this option and click **Browse**. VIPRE Premium looks for the file's unique identifier (MD5 or CRC8) so that if the filename is changed or the file is moved elsewhere on your system, it will still be allowed.

3. Click **OK**. The item is added to the Always Allowed list.

To view details of an Always Allowed item:

1. Open the **Always Allowed** screen by selecting **Manage** tab>**Always Allowed**.
2. Select on an item and click **Details**. The **Always Allowed Details** dialog box displays.
   -or-
   Double-click on a risk to display the **Always Allowed Details** dialog box.

To remove an allowed item from the Always Allowed list:

1. Open the **Always Allowed** screen by selecting **Manage** tab>**Always Allowed**.
2. Select the item you wish to remove and click **Remove From List**. The item is removed from the Always Allowed list and will show up during future scans or when it's run with AP is enabled.

Note: You can click **Select All** and then click **Remove From List** to remove all items from the **Always Allowed** list.

Scheduling Scans

It is important that VIPRE Premium scans on your computer periodically for best results. Scheduling a scan to run automatically is the best way to ensure that your computer is free from malware on a regular basis. You can schedule as many scans as you wish, and later edit, delete, or enable/disable them as necessary. Also, if a scheduled scan is missed, you can set VIPRE Premium to automatically make up the missed scan.

Note: Schedule scans according to how often your computer is used. If you use it every day, you should at least run a **Quick Scan** every day. We recommend that you schedule a **Deep System** scan to run in the middle of the night, provided your computer is turned on.

To schedule a scan:

1. Open the **Schedule Scans** screen (**Manage>Schedule Scans**)
2. Click **Add New**. The **Schedule a Scan** dialog box displays. The **Enable this scheduled scan** option is checked by default.
3. Select one of the following:

- **Quick Scan**: Select to scan commonly affected areas of your computer. This scan is usually shorter in duration than the Deep System Scan. You can configure additional options in the Scan Options tab on the Settings dialog box.

- **Deep System Scan**: Select to perform a thorough scan of all areas of your computer. Depending on how full your hard drive is, this could take longer. You can configure additional options in the Scan Options tab on the Settings dialog box.

4. Select a time for the scan to run. You can select the hours, minutes, or AM/PM and click the up or down arrows to choose your desired time.

Warning: When adding a new scheduled scan, make sure that you remain mindful of whether or not you turn off the "Wake from sleep on scheduled scans" in the power settings. This can greatly impact whether or not an automatic scan takes place.

5. Select the days on which you wish to run the scan. You can select one or more days to be scanned. Deselect a day's box to remove it from the schedule.
6. Click **OK**. The dialog box closes and the scheduled scan displays on the Schedule Scans screen.
7. If desired, set the cleaning action.
8. To schedule another scan, repeat steps 2 - 6.

To edit an existing scheduled scan:

From the Schedule Scans screen you can enable or disable, or delete selected scans. You can also edit the type, time, and frequency of a scan.

Select the scan you wish to edit by clicking on it in the **Schedule scans** list box.

- Click **Enable/Disable** to enable or disable the selected scan.
- Click **Delete** to delete the selected scan.
- Click **Edit** to open the **Schedule a Scan** dialog box. Make any necessary changes and click **OK**.

Note: You can also click **Select All** to perform a group action on all scheduled scans, such as deleting or enabling/disabling all scans. Clicking **Select All** disables the **Edit** function.

To set the cleaning action:

You can set the cleaning action that VIPRE Premium takes after running a scheduled scan.

1. Click the **Scan Options** link at the bottom of the **Schedule Scans** screen. The Settings: Scan Options screen displays.
2. In the **Settings for scheduled scans only** area, select one of the following:

- **Automatically take the recommended cleaning action**: After a scheduled scan completes, VIPRE Premium automatically cleans the risks based on the recommendation of Sunbelt Software's research team, and will display the Clean Results screen for you to review the results. Select this option for the most carefree way of ridding your computer of malware. For more information, visit SunbeltLabs.
- **Show me the results and let me decide**: After a scheduled scan completes, VIPRE Premium displays the Scan Results screen for you to take corrective action on the detected risks. Select this option for the most control over your computer.

3. Click **OK** to apply and save your settings. The dialog box closes and you are returned to the Schedule Scans screen.

To make up a missed scheduled scan:

You can miss a scheduled scan if your computer is turned off while a scan is scheduled to run. Perform the steps below to automatically make up a missed scan:

1. Click the **Scan Options** link at the bottom of the **Schedule Scans** screen. The Settings: Scan Options screen displays.
2. In the Missed Scheduled Scans area, select the following:

   - **Make up missed scans with a quick scan**: When selected, VIPRE Premium will automatically make up a missed scheduled scan. This means, for example, that if you scheduled a scan for 1:00 AM and the computer was turned off for the night, once your computer is turned on VIPRE Premium will automatically begin a Quick scan after the delay.

     Note: Even if the missed scheduled scan was a Deep System scan, this make up scan will only be a Quick scan.

   - **Delay scan by**: Select a number of minutes for VIPRE Premium to wait before starting an automatic Quick scan. The default is 5 minutes.

3. Click **OK** to apply and save your settings. The dialog box closes and you are returned to the Schedule Scans screen.

Chapter 5: Configuring the Firewall

About the VIPRE Premium Firewall

The VIPRE Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. It can be run in either "Simple" or "Learning" modes. You can create customized rules while in either mode.

Firewall Modes

Simple Mode:

Simple Mode is suited for most users who simply want basic firewall protection and not have to do anything more to manage it. All you need to do is keep the firewall enabled in the default Simple Mode. While in this mode, you can make changes and create rules, as needed. Feel free to contact the Sunbelt Technical Support for FREE to help you in changing your firewall settings.

Simple Mode starts with default settings that are suited for the average user and will block all inbound activity.

Learning Mode:

Learning Mode, better suited for more experienced users, will frequently prompt you to essentially teach the VIPRE Firewall how to act. You will be prompted to take action on activity by applications and for certain Operating System actions. Your actions to the prompts can be remembered and applied to this activity in the future, by creating or modifying a rule.

Example 1: Applications

For example, if you are running a gaming application ("Generic Game") and you click "Allow" when prompted and checking "Add a rule...", the Firewall creates an Application rule for the "Generic Game" application. If desired, you can further customize this generated Application rule from the Application Exceptions screen.

Example 2: Code Injections

For example, with Host Intrusion Prevention System (HIPS) enabled and an application attempts to inject code, clicking "Allow" when prompted will create a Code Injection rule for the application. If desired, you can further customize this generated Code Injection rule from the Host Intrusion Protection System Exceptions screen.

Firewall Screens

Firewall Settings:

Firewall Settings allows you to manage the Firewall, Web Filtering, and Process Protection settings.

Statistics:

The **Statistics** screen lists all firewall statistics including network activity, intrusions blocked by the Intrusion Detection Systems (IDS), actions blocked by process protection, items blocked by rules, and items blocked by web filtering.

Connections:

The **Connections** screen allows you to view your computer's Network connections and the applications that are actively involved in network communication.

Firewall History:

The **Firewall History** screen allows you to view the event history of VIPRE Antivirus Premium's firewall components, which are grouped into tabs. Each tab contains a table that lists all relevant information for that firewall component. You can view details for any selected item in a table and clear its history.

Enabling or Disabling the Firewall

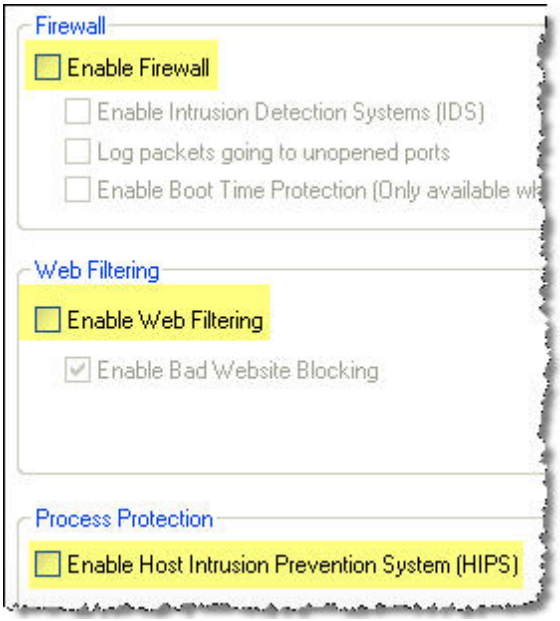
The **Firewall** protects your computer from both incoming and outgoing traffic. Enabling the Firewall will restrict network activity based on your Firewall settings.

To completely TURN OFF the Firewall:

Note: The Firewall has three components that all need to be turned off separately from the Firewall Settings screen; the system tray only turns off the top "Firewall" area.

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Firewall** tab.
3. Unselect the following:

   - **Enable Firewall**
   - **Enable Web Filtering**
   - **Enable Host Intrusion Prevention System (HIPS)**



4. Click **OK** to save your settings. Your Firewall is now completely turned off.

To enable/disable the Firewall from the System Tray Icons:

Note: Disabling the firewall from the system tray does not turn off the Firewall completely.

1. Right-click the **VIPRE Premium icon** in the System Tray.

2. Select **Firewall**.
3. Select one of the following:

- **Enable Firewall**: turns *on* the "Firewall" functions on the Firewall Settings dialog box. This does not include Web Filtering or Process Protection.
- **Disable Firewall**: turns *off* the "Firewall" functions on the Firewall Settings dialog box. This does not include Web Filtering or Process Protection.
- **Stop All Traffic**: stops all incoming and outgoing traffic.
- **Resume All Traffic**: resumes filtering of incoming and outgoing traffic based on the VIPRE Firewall settings.

Resetting to Firewall Defaults

Reset to the VIPRE Firewall defaults if you suspect that something that you changed in the Firewall is causing problems and don't know what specifically to fix.

You can reset the VIPRE Firewall to the default settings of either of the two modes: Simple or Learning. While resetting, you can switch from one mode to the other. Resetting applies to all VIPRE Firewall settings (Firewall, Web Filtering, and Process Protection).

When resetting or switching modes, you can also choose to keep or delete user-defined firewall rules (See Step 4 below for more detail.).

To reset the VIPRE Firewall to the default settings:

1. From the **File** menu, select **Settings**. The Settings dialog box displays.
2. Click the **Firewall** tab, and then click **Reset to Defaults**. The Reset Firewall Defaults dialog box displays.
3. Select one of the following:

- **Reset to Simple Mode**: Resets to the VIPRE Firewall "Simple Mode" default settings. This is resetting any change that you may have made to the Firewall Settings tab.

- **Reset to Learning Mode**: Resets to the VIPRE Firewall "Learning Mode" default settings. Learning mode will prompt you whenever there is an attempt made for a network connection.

4. Optionally, select **Delete all user defined firewall rules** if you suspect that one of the user-defined rules you created is causing problems and don't know which one to fix. A "user-defined" rule can include rules created when answering a prompt or manually through the VIPRE Firewall Settings screen. Any user-defined rule created by any of the following areas apply: Applications, Ports, Advanced, Zones, Web Filtering, and Code Injection.

Note: If there are settings that you know are good and want to keep, make note of those settings for re-entering after resetting.

5. Click **OK** on the Reset Firewall Defaults dialog box.
6. Click **OK** on the Firewall Settings screen. Your Firewall settings are now applied.

Managing the VIPRE Firewall

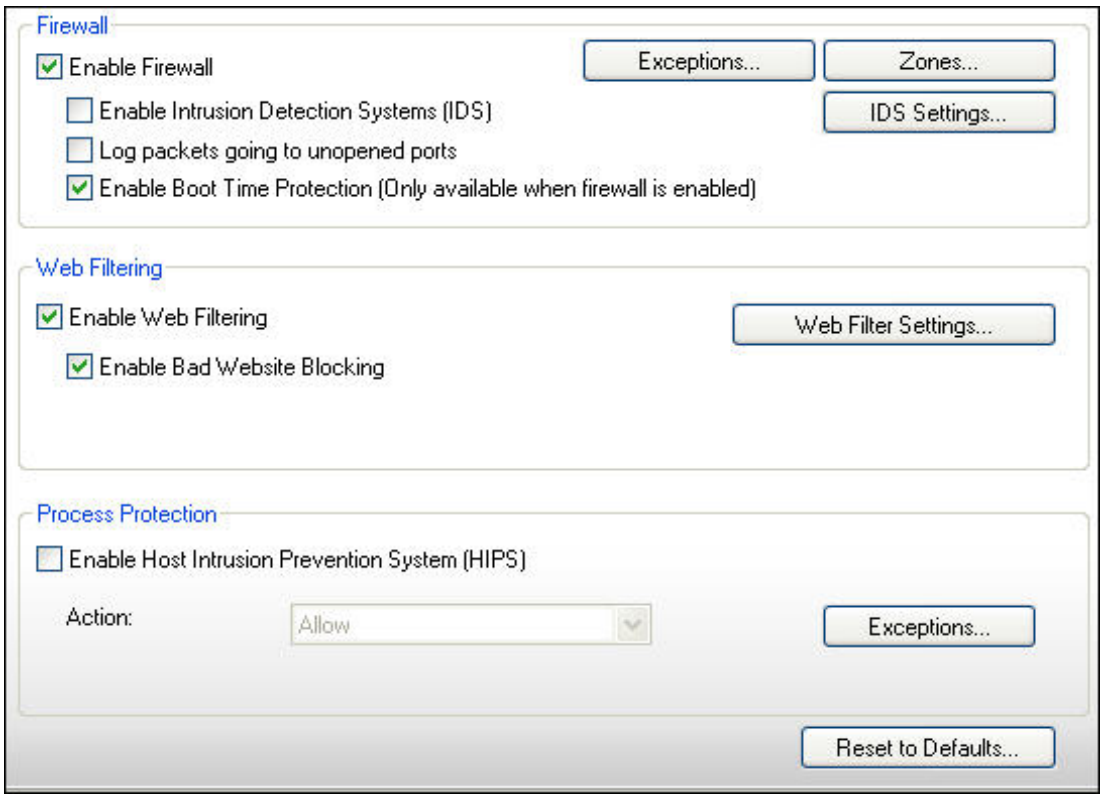
Settings: Firewall

Firewall Settings allows you to manage the Firewall, Web Filtering, and Process Protection settings. You can turn off your firewall completely by disabling the Firewall, Web Filtering, and Process Protection.

You can access the Firewall Settings any of the following ways:

- From the **File** menu, select **Settings** and then click the **Firewall** tab.
- From the **Overview** screen, under "Firewall" click **Edit Settings**.
- From the **Firewall** screen, under "Settings" click **View Settings**.

Caution: Modify your firewall settings with care, especially when creating exceptions. But, at anytime you feel you set something wrong and don't know how to fix it, you can Reset to Firewall Defaults.



This screen contains the following items:

Firewall

- **Enable Firewall**: The firewall is enabled by default. The "firewall" includes Exceptions, Zones, IDS, and packet logging. Web Filtering and HIPS are NOT controlled by this check box. It is recommended to have the firewall enabled at all times.
  - **Enable Intrusion Detection Systems (IDS)**: Select to activate the IDS rules engine. Click **IDS Settings** to enable/disable and modify actions of the IDS rules.

  - **Log packets going to unopened ports**: Packet logging is logged in the PUP screen of the Firewall History. The log refreshes around every 30 seconds. Only the last 100 items are kept in the log.

- **Enable Boot Time Protection**: Boot time protection protects your computer when it starts, blocking traffic from occurring before Windows has a chance to open. The "Enable Firewall" check box must be selected for boot time protection to be enabled. This option is enabled by default. Disabling it is useful for testing and troubleshooting (i.e. to solve problems with remote host administration). For security reasons, it is recommended that you do not disable this option unless necessary.
- **Exceptions**: Click to open the Firewall Exceptions dialog box where you can manage Applications, Ports, and Network exceptions.
- **Zones**: Click to open the Networks and Zones dialog box where you can manage Trusted Networks & Zones, and Untrusted Networks.
- **IDS Settings**: Click to open the Intrusion Detection Systems dialog box where you can modify an Action to intrusions based on priority, and enable/disable specific IDS rules.

Web Filtering

Web filtering acts like a proxy by receiving all Internet traffic before seamlessly displaying it in your web browser. Web filtering can protect you from malicious websites, scripts, and ActiveX controls.

Note: If after modifying the web filtering you cannot access desired web content (if something is not displaying), you may have set the filtering too high and may need to adjust it accordingly.

- **Enable Web Filtering**: This is selected/enabled by default. Enables the default web filtering settings and any user-modified web filtering setting. When unselected, the default web filtering and user-modified web filtering settings will be disabled.
- **Enable Bad Website Blocking**: Select to prevent from accidentally becoming infected by drive-by downloads and other exploits, ensuring the web pages you visit are safe *before* clicking a link, and not after the fact. This is selected/enabled by default.
- **Web Filter Settings**: Click to open the Web Filter Settings dialog box where you can set specific web filtering for customized protection.

Process Protection

- **Enable Host Intrusion Prevention System (HIPS)**: Select to activate HIPS and any code injection exceptions that you may have added.
- **Action**: Select an action from the drop-down list and then click **Apply**.
- **Exceptions**: Click to open the Host Intrusion Protection System Exceptions dialog box where you can manage the code injection exceptions. You can add exceptions for applications that you want to be allowed to code inject. Some non-malicious programs use this technique.

- **Reset to Defaults**: Click to reset to the VIPRE Firewall defaults if you suspect that something that you changed in the Firewall is causing problems. For more information, see Resetting to Firewall Defaults.

- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.
- **Apply**: Click to apply the changes made and continue working in the dialog box.
- **Help**: Click to open the Help System specific to where you are in the VIPRE Premium interface.

Managing Firewall Exceptions (rules)

Managing Application Exceptions

VIPRE Antivirus Premium comes with default application exceptions. You can add new application exceptions, edit exceptions, and delete user-added exceptions. These application exceptions (rules), tell the Firewall what action to take for network activity to/from the application.

To add, edit, or delete an application exceptions:

1. Navigate to the **Applications** screen. (**File>Settings>Firewall** tab>**Exceptions** button>**Applications** tab)
2. To add a new application exception, click **Add**. The Add an Application Rule dialog box displays.
   -or-
   To edit an existing application exception, select a row in the table and click **Edit**. The Modify an Application Rule dialog box displays. Skip to Step 4.
   -or-
   To delete an existing application exception, select a row of a user-added rule in the table and click **Delete**. Skip to Step 5.

   Note: You can only delete user-added exceptions.

3. Click **Browse** to locate the application or manually enter the **Path** to the application.
4. Select an action (Allow, Allow with Notify, Block, Block with Notify, or Prompt) for the following conditions:
   - **Trusted Inbound**: applies only to an inbound connection for your trusted network(s).
   - **Trusted Outbound**: applies only to an outbound connection for your trusted network(s).
   - **Not-trusted Inbound**: applies only to an inbound connection for any network that is not trusted.
   - **Not-trusted Outbound**: applies only to an outbound connection for any network that is not trusted.
5. Click **OK** to accept changes.

Managing Port Exceptions

You can add, edit, or delete port exceptions. These port exceptions (rules), tell the Firewall what action to take for network activity that matches the port rule.

Note: Adding a port exception by using this procedure will be for a specific application and protocol. If you want to create a general port exception that is not specific to an application or one that is more advanced, you need to add an advanced exception.

To add, edit, or delete a port exception:

1. Navigate to the **Ports** screen. (**File>Settings>Firewall** tab>**Exceptions** button>**Ports** tab)
2. To add a port exception, click **Add**. The Add a Port Rule dialog box displays.
   -or-
   To edit an existing port exception, select a port exception in the table and click **Edit**. The Modify a Port Rule dialog box displays. Skip to Step 4.

   Note: The table will list both Port and Advanced exceptions, as specified in the "Type" column. If you want to edit an Advanced exception, go to managing advanced exceptions.

   -or-
   To delete an existing port exception, select a port exception in the table and click **Delete**. Skip to Step 8.
3. Enter a **Name** for the port exception.
4. Click **Browse** to locate the application or manually enter the **Path** to the application.
5. Select a **Port Number** from the drop-down or enter it manually.
6. Select a **Protocol** from the drop-down.
7. Select an action (Allow, Allow with Notify, or Block with Notify) for the exception from the drop-down.
8. Select a direction (Both, In, or Out) for the exception from the drop-down.
9. Click **OK** to accept changes.

Managing Advanced Exceptions

Advanced exceptions can apply to a specific application and include one or a combination of protocol, local and remote ports, and direction of traffic. These advanced exceptions (rules), tell the Firewall what action to take for network activity that matches the advanced rule. You can add, edit, or delete an advanced exception.

To add, edit, or delete an advanced exception:

1. Navigate to the **Ports** screen. (**File>Settings>Firewall** tab>**Exceptions** button>**Ports** tab)
2. To add an advanced exception, click **Add Advanced**. The Add an Advanced Rule dialog box displays.
   -or-
   To edit an existing advanced exception, select an advanced exception in the table, as indicated in the "Type" column, and click **Edit**. The Modify an Advanced Rule dialog box displays.

-or-
To delete an existing advanced exception, select an advanced exception in the table, as indicated in the "Type" column, and click **Delete**. Skip to Step 11.

3. Enter a **Rule Name** for the advanced exception.
4. Optionally, enter a **Description** for the exception.
5. Optionally, assign an application to the advanced exception:

   Click **Browse** to locate an application or manually enter the file path to the application.

6. Select an **Action** from the drop-down: Allow, Allow with Notify, Block, Block with Notify, or Prompt. This is the resulting action this rule will take if triggered.
7. Select a **Direction** from the drop-down: Both, In, or Out. This rule will apply only to this selected direction.
8. Optionally, select a **Protocol**: ICMP, IGMP, TCP, or UDP.
9. Optionally, enter one or more **Local or Remote Ports**:
   - Under "Fore these local ports" or "For these remote ports," click **Add**. The Add a Port dialog box displays, allowing you to enter a single port (Beginning Port) or a port range.
   - Under the "Beginning Port" area, select a port from the drop-down. The port number displays in the Port Number field and its description displays in the Description field.

   You can also manually enter the port.

   - To enter a port range, under the "Ending Port" area, select a port from the drop-down. The port number displays in the Port Number field and its description displays in the Description field.

     This port range will be, with an allowed action, will be allowed past the Firewall.

   - Click **OK**. The Add a Port dialog box closes after saving your changes. You are returned to the Modify an Advanced Rule dialog box, where the port or port range is displayed.
10. Click **OK**. The Add an Advanced Rule dialog box closes after creating your advanced exception. The newly created advanced exception displays in the table on the Ports dialog box.
11. Click **OK** on the Ports tab of the Firewall Exceptions dialog box.

Modifying Network Exceptions

You can edit existing VIPRE network exceptions. These network exceptions, tell the Firewall what action to take for network activity that matches the network rule. Network exceptions filter packets of information that are transmitted in and out of your computer.

To edit a network exception:

1. Navigate to the **Network** screen. (**File>Settings>Firewall** tab>**Exceptions** button>**Network** tab)
2. Select a network exception in the table and click **Edit**. The Modify a Network Rule dialog box displays.
3. Select an action (Allow, Allow with Notify, Block, Block with Notify, or Prompt) for the following:
   - **Trusted Inbound Action**: applies only to an inbound connection for your trusted network(s).
   - **Trusted Outbound Action**: applies only to an outbound connection for your trusted network(s).
   - **Not-trusted Inbound Action**: applies only to an inbound connection for any network that is not trusted.
   - **Not-trusted Outbound Action**: applies only to an outbound connection for any network that is not trusted.
4. Click **OK** to accept changes. The Modify a Network Rule dialog box closes, returning you to the Network tab on the Firewall Exceptions dialog box.
5. Click **OK** to save changes. The Network exception is now modified.

Managing Networks and Zones

Managing Trusted Networks & Zones

The **Trusted Networks & Zones** tab allows you to add or edit a trusted network or zone. You can also delete a user-added network or zone. A trusted zone is typically a home or work network or a specific computer.

A trusted network or zone can be added when you respond to a VIPRE prompt telling you that a network was detected.

Note: A user-added trusted network can be moved to the Untrusted Networks list by clicking **Move to Untrusted**. This option is only available for added networks; this is unavailable for IP addresses or an address range.

To add, edit, or delete a trusted network or zone:

1. Navigate to the **Trusted Networks & Zones** screen. (**File>Settings>Firewall** tab>**Zones** button)
2. To add a trusted network or zone, click **Add**. The Add a Trusted Zone dialog box displays.
   -or-
   To edit a trusted network or zone, select a row in the table and click **Edit**. The Modify a Trusted Zone dialog box displays.
   -or-

To delete a user-added trusted network or zone, select a row in the table and click **Delete**. Skip to Step 6.

3. Enter a detailed **Description** for the trusted network or zone.
4. Select an **Adapter**.

   VIPRE Antivirus Premium automatically scans your network adapters and displays them in this drop-down. In addition to the listed network adapters, "Any" can be selected, which will apply to any adapter your computer encounters.

5. Under **Address Type**, select one of the following:

   - **IP address**: Enter the IP address.
   - **Address range**: Enter an IP range in the First IP address and Last IP address fields.
   - **Network**: Enter an IP address and Mask.

6. Click **OK**. Your changes are saved. If adding a new network or zone, it displays in the Trusted Networks & Zones table.

Managing Untrusted Networks

The **Untrusted Networks** tab allows you to add, edit, or delete an untrusted network.

An untrusted network can be added when you respond to a VIPRE prompt telling you that a network was detected.

Note: An added untrusted network can be moved to the Trusted Networks & Zones list by clicking **Move to Trusted**.

To add, edit, or delete an untrusted network:

1. Navigate to the **Untrusted Networks** screen. (**File**>**Settings**>**Firewall** tab>**Zones** button>**Untrusted Networks** tab)
2. To add an untrusted network, click **Add**. The Add an Untrusted Zone dialog box displays.
   -or-
   To edit an untrusted network, select a row in the table and click **Edit**. The Modify an Untrusted Zone dialog box displays.
   -or-
   To delete an untrusted network, select a row in the table and click **Delete**. Skip to Step 6.
3. Enter a detailed **Description** for the trusted network or zone.
4. Select an **Adapter**.

   VIPRE Antivirus Premium automatically scans your network adapters and displays them in this drop-down. In addition to the listed network adapters, "Any" can be selected, which will apply to any adapter your computer encounters.

5. Enter an **IP address** and **Mask** for the network.

6. Click **OK**. Your changes are saved. If adding a new network or zone, it displays in the Untrusted Networks table.

Managing Intrusion Detection Systems Settings

Intrusion Detection Systems (IDS) settings allows you to manage activity based on advanced filtering rules provided by Sunbelt Software. The IDS rules are grouped by priority: low, medium, and high. You can set how intrusions under these priority levels are acted upon. You can also enable/disable a rule under each priority level, and log port scans.

Once IDS is enabled, you can view the intrusions blocked by IDS on the Firewall Statistics screen.

To enable/disable IDS:

1. Navigate to the **Firewall Settings** screen. (**File>Settings>Firewall** tab)
2. Under the **Firewall** area, select the **Enable Intrusion Detection Systems (IDS)** checkbox to enable, and unselect to disable.
3. Click **OK** to save changes.

To modify an action for intrusions:

1. Navigate to the **Intrusion Detection Systems** screen. (**File>Settings>Firewall** tab>**IDS Settings** button)
2. Under a priority level that you want to modify, click its drop-down and select one of the following: Allow, Allow with Notify, Block, or Block with Notify.
3. Click **OK**. The Intrusion Detection Systems dialog box closes.
4. On the **Firewall Settings** screen, select the **Enable Intrusion Detection Systems (IDS)** check box.
5. Click **OK** to save changes.

To enable/disable an IDS rule:

1. Navigate to the **Intrusion Detection Systems** screen. (**File>Settings>Firewall** tab>**IDS Settings** button)
2. Under a priority level that you want to modify, click its associated **Details** button. The Advanced Protection Rules (Intrusion Detection System) dialog box displays.
3. Locate the rule you want to change and select to Enable, or un-select to Disable.
4. Click **OK**. The Advanced Protection Rules dialog box closes, returning you to the Intrusion Detection Systems dialog box.
5. On the **Intrusion Detection Systems** dialog box, Click **OK** to save changes and close.
6. On the **Firewall Settings** screen, select the **Enable Intrusion Detection Systems (IDS)** check box and click **OK** to save changes.

To log port scans and view them:

1. Navigate to the **Intrusion Detection Systems** screen. (**File>Settings>Firewall** tab>**IDS Settings** button)

2. Under the **Ports Scans** area, select the **Log port scans** check box.
3. Click **OK**. The Intrusion Detection Systems dialog box closes.
4. On the **Firewall Settings** screen, click **OK** to save changes.
5. To view history for logged port scans:
   - Click the **FIREWALL** tab from the main console.
   - Click **View Firewall History**. The Firewall History screen displays.
   - Click the **IDS** tab. If port scans are attempted on your computer, they will be displayed here and listed under the "Category" column.
6. To view a summary of the intrusions blocked by IDS on the Firewall Statistics screen:
   - Click the **FIREWALL** tab from the main console.
   - Click **View Statistics**. The Firewall Statistics screen displays.
   - The number of **Port scans** displays under **Intrusions Blocked by IDS**.

Web Filtering Settings

The **Web Filtering Settings** tab allows you to block certain types of data from websites.

This screen contains the following items:

- **Advertisements**
  - **Block 3rd party advertisements**: Select to block 3rd party advertisements, which may be malicious.
  - **Change** button: Click to open the Advertisement blocking by URL dialog box where you can manage advertisement blocking. You can view, modify, and add your own URL/Web Page to what is blocked.
- **Web Page Content Filtering**
  - **Block JavaScripts**: Select to block JavaScripts from running in your web browser.
  - **Block VBScripts**: Select to block VBScripts from running in your web browser.
  - **Block ActiveX**: Select to block ActiveX from running in your web browser.

Note: Blocking JavaScripts, VBScripts, and/or ActiveX may cause some problems displaying some Web pages. If so, you can add an allowed website for such a page.

- **Privacy Settings**
  - **Filter persistent cookies**: Select to filter cookies that send information each time a web site is visited.
  - **Filter session cookies**: Select to filter temporary cookies that are only used when opening a particular page.
  - **Filter foreign cookies**: Select to filter cookies from third-party servers.
  - **When a website directs me to another website, do not include the first website's address**: Select to keep your browsing private when you are redirected to other websites. This setting applies to "Referer logging," which is used to allow websites and web servers to identify where people are visiting them from, typically for promotional or security purposes. A referer is popularly used to defend against cross-site request forgery and for statistical

purposes. When unselected, the details of a link request are stripped from the referring website so that the target website cannot identify the page of which the page request originated from.

- **Log Webfilter blocked events**
  - **Log when connections are blocked**: Select to log whenever any of the Web Filtering settings block something. You can view the log from the WEBFILTER tab on the Firewall History screen.
- **OK**: Click to accept all changes made and close the dialog box.
- **Cancel**: Click to close the dialog box without retaining any changes.

Managing Advertisement Blocking

VIPRE Premium's Advertisement Blocking uses a list of malicious ad sites and text strings contained in the site addresses compiled by SunbeltLabs. You can add, edit, or delete a user-defined Domain/URL, and block/unblock an advertisement Domain/URL.

Domain/URLs that are unblocked (disabled) will essentially override the "Block 3rd party advertisements" setting.

To add, edit, or delete a user-defined Domain/URL:

1. Navigate to the **Web Filter Settings** screen. (**File>Settings>Firewall** tab>**Web Filter Settings** button)
2. Select the **Block 3rd party advertisements** check box, and then click **Change**. The Advertisement blocking by URL dialog box displays.
3. To add an advertisement filter, click **Add**. The Add an Advertisement filter dialog box displays.
   -or-
   To edit a user-defined advertisement filter, select a row in the table and click **Edit**. The Modify an Advertisement filter dialog box displays.
   -or-
   To delete a user-defined advertisement filter, select a row in the table and click **Delete**. The item is removed immediately. Click **OK** to close.
4. Select one of the following options:

   - **Sub-string**: Looks for a match of the string you enter anywhere within a URL (i.e. `adserver009`).
   - **Wild card**: Allows for "?" and "*" to match any character in the URL (i.e. `*.sunbeltsoftware.com`).
   - **Regular expression**: This is to be used by experts who are familiar with the regular expression syntax (i.e. `adtrack\d*\`).

5. Enter a **URL or Web page** expression that reflects the selection you made in Step 4.
6. Click **OK** to add the URL or Web page to the Advertisement blocking by URL dialog box.
7. On the **Firewall Settings** screen, verify that **Enable Web Filtering** is selected.

To block/unblock an advertisement Domain/URL:

1. Navigate to the **Web Filter Settings** screen. (**File>Settings>Firewall** tab>**Web Filter Settings** button)
2. Select the **Block 3rd party advertisements** check box, and then click **Change**. The Advertisement blocking by URL dialog box displays.
3. Navigate to a desired item in the list, and then **select** to Enable or **unselect** to Disable.
4. Click **OK** to save changes and close the dialog box.
5. On the **Firewall Settings** screen, verify that **Enable Web Filtering** is selected.

Managing Allowed Web Sites

You can add an allowed website and filter specific types of content. You can also edit an existing allowed web site or remove one. Settings made on the Allowed Web Sites screen will over-ride the Web Filter Settings.

The VIPRE Firewall includes some default allowed web sites, such as sunbeltsoftware.com, sunbeltsecurity.com, and update.microsoft.com. These allow your computer to receive the necessary Windows updates and VIPRE definitions to keep your computer's security up to date and protected. These default sites can not be removed.

To add, edit, or remove an allowed web site:

1. Navigate to the **Allowed Web Sites** screen. (**File>Settings>Firewall** tab>**Web Filter Settings** button>**Allowed Web Sites** tab)
2. To add an allowed web site, click **Add**. The Add an Allowed Web Site dialog box displays.
   -or-
   To edit an existing allowed web site, select a row in the table and click **Edit**. The Modify an Allowed Web Site dialog box displays.
   -or-
   To remove an existing allowed web site, select a row in the table and click **Remove**. The item is removed immediately. Click **OK** to close.
3. Enter a Web site address in the box after "`http://www.`" For example, `sunbeltsoftware.com`.
4. Optionally, under **Web content**, select one or more options to block for this specific website.
5. Optionally, under **Cookies**, select one or more of the cookie options to block for this specific website.
6. Optionally, under the **Referer** section, select the option to keep your browsing private when you are redirected to other websites.
7. Click **OK**. Your allowed web site changes are saved and you are returned to the previous screen. The newly created allowed web site displays in the table on the Allowed Web Sites tab.
8. On the **Firewall Settings** screen, verify that **Enable Web Filtering** is selected.

Managing Process Protection

Process Protection is used to allow specific programs/applications to inject code into another program/application.

To add and configure an injection exception:

1. Navigate to the **Host Intrusion Protection System Exceptions** dialog box. (**File>Settings>Firewall** tab>**Process Protection Exceptions** button)
2. Click **Add**. The Add Code Injection Exception dialog box displays.
3. Click **Browse** to locate the application or manually enter the **Path** to the application.
4. Click **OK** to accept changes. The application is added to the list in the Host Intrusion Protection System Exceptions dialog box.
5. Click **OK** to return to the Firewall Settings screen.
6. Select the **Enable Host Intrusion Prevention System (HIPS)** check box.
7. Select an **Action** from the drop-down: Allow, Allow with Notify, Block, or Block with Notify.
8. Click **Apply** to save changes.

To delete a code injection exception:

1. Navigate to the **Host Intrusion Protection System Exceptions** dialog box. (**File>Settings>Firewall** tab>**Process Protection Exceptions** button)
2. Select an injection exception in the table and click **Delete**.
3. Click **OK** to accept changes.

Viewing Firewall Statistics

The **Statistics** screen lists all firewall statistics including network activity, intrusions blocked by the Intrusion Detection Systems (IDS), actions blocked by process protection, items blocked by rules, and items blocked by web filtering.

This screen is accessible from **Firewall>Statistics**.

This screen contains the following items:

Show statistics... drop-down box

Click the arrow to select how the firewall statistics data displays. Select by the last hour, day, week, or month. Items beyond a month are not included in the listed counts.

Reset all statistics

Click this button to reset ALL listed counts to zero, regardless whether you are listing by hour, day, week, or month.

Network Activity

Displays the traffic over your network in bytes.

- **Bytes in/out ARP**: Displays the number of bytes of information flowing in/out of the ARP (Address Resolution Protocol).
- **Bytes in/out ICMP**: Displays the number of bytes of information flowing in/out of the ICMP (Internet Control Message Protocol).

- **MB in/out UDP**: Displays the number of megabytes (MB) of information flowing in/out of the UDP (User Datagram Protocol).
- **Bytes in/out TCP**: Displays the number of bytes of information flowing in/out of the TCP (Transmission Control Protocol).

Intrusions Blocked by IDS

When you enable the Intrusion Detection Systems (IDS), the number of detected intrusions display:

- **High**: Critical attacks.
- **Medium**: Medium-level priority intrusions (e.g. service blocking).
- **Low**: Low-level priority intrusions (e.g. suspicious activities).
- **Port scans**: Displays the number "Port Scans" detected. You must enable Log port scans for VIPRE Premium to detect and display any.

Note: To view detailed history of the specific detected intrusions, view the firewall history.

Actions Blocked by Process Protection

Displays the number of blocked actions by the Process Protection. Host Intrusion Prevention System (HIPS) must be enabled.

- **Code injections blocked**: Number of code injection attempts. Only the number of detected user-defined code injection attempts to processes are displayed here
- **Process termination attempts blocked**: Number of attempted shutdowns of the system blocked.

Items Blocked by Rules

- **Ports/Advanced items blocked**: Number of ports and/or advanced items that were blocked. Only the number of detected user-defined port exceptions and advanced exceptions are displayed here.
- **Network items blocked**: Number of network items that were blocked. Only the number of detected network exceptions are displayed here.
- **Application items blocked**: Number of application items that were blocked. Only the number of detected application exceptions are displayed here.

Items Blocked by Web Filter

Displays the number of blocked Web items by Web Filtering. You must enable Web Filtering for these items to be detected.

- **JavaScripts**: Number of filtered JavaScript items.
- **VBScripts**: Number of filtered Visual Basic Script items.
- **ActiveX**: Number of filtered ActiveX components.
- **Advertisements**: Number of blocked ads and web pages components blocked by ad filtering rules.
- **Referers**: Number of Referred items filtered from the HTTP header.

- **Persistent**: Number of persistent cookies blocked. A persistent cookie remains on your computer's hard drive until you erase them or they expire. How long a cookie remains on your system depends on how long the visited website has programmed the cookie to last.
- **Session**: Number of session cookies blocked. A session cookie is a temporary cookie that is created while connected to a website and is erased when you close your browser at the end of your Internet browsing session. The next time you visit that particular website is considered a new "session," thus creating a new cookie.
- **Foreign**: Number of third-party cookies blocked. A foreign or third-party cookie either originates on or is sent to a website different from the one you are currently viewing.

Viewing Connections

The **Connections** screen allows you to view your computer's Network connections and the applications that are actively involved in network communication.

The following connection types can be listed in the table:

- **Connected in**: an incoming connection is established (red arrow, pointing left).
- **Connected out**: an outgoing connection is established (green arrow, pointing right).
- **Listening**: an application is listening for connections (cable symbol).

This screen is accessible from **Firewall>Connections**.

This screen contains the following items:

- **Local Point**: Local IP address (or a corresponding DNS name) and port (or service name).
- **Remote Point**: IP address (or DNS name) and port number (or service name) of a particular remote point. The same information for the local IP address and port is provided (see above).
- **Protocol**: Protocol used (TCP, UDP, or both).
- **Speed In, Speed Out**: Current speed of incoming and outgoing data of the connection in kilobytes per second (KB/s).
- **Bytes In, Bytes Out**: Amount of incoming and outgoing data within the connection.

A key at the bottom of the tab shows the number of active connections.

Viewing Firewall History

The **Firewall History** screen allows you to view the event history of VIPRE Antivirus Premium's firewall components, which are grouped into tabs. Each tab contains a table that lists all relevant information for that firewall component. You can view details for any selected item in a table and clear its history. The history refreshes around every 30 seconds. Displayed history items depend on your history settings, and for events that are generated often, only the last 100 items display.

This screen is accessible from **Firewall>Firewall History**.

This screen contains the following items:

APP RULES Tab

The **APP RULES** tab displays the application events that were generated based on the application exceptions (rules).

PORT RULES Tab

The **PORT RULES** tab displays the port events that were generated based on user-defined port exceptions (rules).

NETWORK RULES Tab

The **NETWORK RULES** tab displays the network events that were generated based on the network exceptions (rules).

ADV RULES Tab

The **ADV RULES** tab displays events that were generated based on user-defined advanced exceptions (rules).

WEBFILTER Tab

The **WEBFILTER** tab displays events that were generated based on the web filtering settings.

IDS Tab

The **IDS** tab displays the Intrusion Detection Systems events that were generated based on the IDS settings.

HIPS Tab

The **HIPS** tab displays the Host Intrusion Prevention System events that were generated based on the Process Protection settings.

ADAPTER Tab

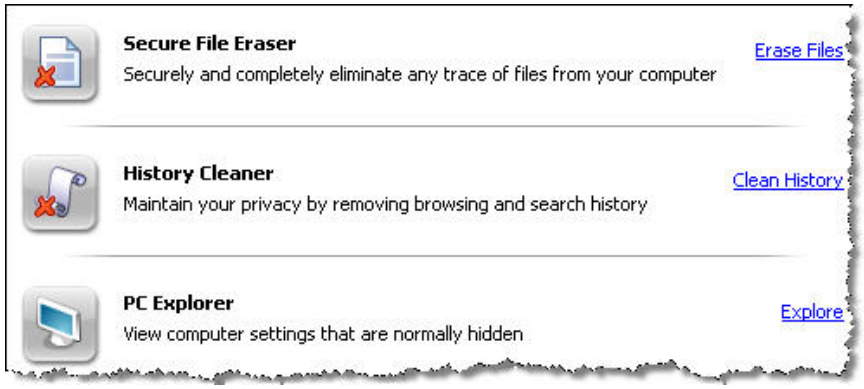
The **ADAPTER** tab displays the network adapter events that were generated based on the trusted and untrusted zones.

PUP Tab

The **PUP** tab displays the Packets to Unopened Ports. You must have the Log packets going to unopened ports enabled.

Chapter 5: Using System Tools

The **System Tools** screen provides you access to areas of your computer that you don't normally see.



- The **Secure File Eraser** allows you to completely eliminate all traces of a file. See Erasing Files Permanently.
- The **History Cleaner** is a privacy tool that allows you to remove your browsing and search histories, including the history stored by many popular applications. See Removing Browsing and Search Histories from your Computer.
- The **PC Explorer** is for informational purposes allowing you only to view settings on your computer that are normally hidden. You cannot take any action to what is viewable from this area. See Using PC Explorer.

Erasing Files Permanently

VIPRE Premium offers you a privacy tool to permanently remove files from a storage device. When a file is deleted, it is not really gone. While the file is no longer shown in Windows Explorer, the data still exists on the drive and can be retrieved with special utilities. The **Secure File Eraser** allows you to completely eliminate all traces of a file.

Warning: When you use the Secure File Eraser to erase a file, the file cannot be retrieved with special data recovery utilities. If you are attempting to remove a shortcut, the target file will be permanently erased, NOT the shortcut.

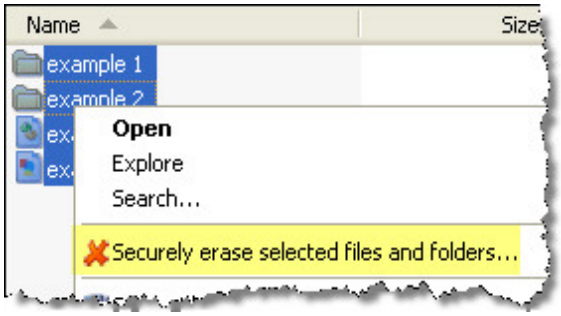
Note: You can permanently erase files from nearly any drive (storage device) connected to your computer. For example, floppy drives, flash drives, external and internal hard drives.

To permanently erase a file from a storage device:

1. Click on the **Tools** tab, and then click the **Secure File Eraser** icon. The Secure File Eraser screen displays.
2. Select the **Add the "Erase files..." option to your Windows Explorer right-click menu** check box. This option will be immediately added to the Window's Explorer menu, allowing you to use this feature.
3. Open **Windows Explorer**.

Tip: To open Windows Explorer on your computer, right-click on **Start** and select **Explore**.

4. In **Windows Explorer**, navigate to the desired drive, folder, and/or file and select one or more items to be permanently removed.
5. Right-click on the selected items. The options menu displays.



6. Select **Securely erase selected files and folders...** The confirmation window displays.
7. Click **Yes**. The selected items are permanently removed from the drive.

Note: Depending on the size and quantity of selected files, you may experience a short delay before you see them removed.

Removing Browsing and Search Histories from your Computer

You can remove browsing and search histories from your computer, including the history stored by many popular applications.

To permanently remove browsing and search history from your computer:

1. Click the **Tools** tab, and then click **History Cleaner**. The History Cleaner screen displays.
2. To display only programs installed on your machine, select **Show installed programs only**.
   -or-
   To view a listing of all programs that VIPRE Premium can clean, deselect **Show installed programs only**.
3. In the list, select the check boxes for the program that you want cleaned.
   -or-
   Click **Select All** to select all programs for cleaning.
   -or-
   Click **Unselect All** to deselect all programs from the list.
4. Click **Clean History**. VIPRE Premium cleans the histories of all select programs and displays a message when finished.
5. Click **OK**.

Using PC Explorers

VIPRE Premium's PC Explorers allows you to view settings on your computer that are normally hidden. Details on the PC Explorers can be found in Appendix II, Screens, PC Explorer screen.

To view the PC Explorers:

1. Select the **Tools** tab. The System Tools screen displays.
2. Click **PC Explorer**. The PC Explorer screen displays.
3. From the **My PC Explorers drop-down box**, select from one of the following:

   - **Downloaded ActiveX**: Displays all the downloaded and currently installed ActiveX programs for Internet Explorer.
   - **Internet Applications**: Displays a list of programs that are currently connected to a remote computer, or are listening for connections from a network or the Internet.
   - **Running Processes**: Displays a list of all the processes (programs) that are currently running on your computer.
   - **Startup Programs**: Displays a list of all the applications that can start up and run when you start your computer or log into Windows.
   - **Internet Explorer BHOs**: Also known as "Browser Helper Objects," this is an application that extends Internet Explorer and acts as a plug-in.
   - **Window's Host Files**: Displays a list of the current host files in your Windows Host file.
   - **Window's LSPs**: Also know as "Winsock Layered Service Providers," this shows all Layered Service Providers that are installed on your computer.
   - **Shell Execute Hooks**: Allows you to view any of your computer's Windows Shell Execute Hooks.

4. Select an item in the list and click **More Details** or double-click on the selected item. The PC Explorer Details dialog box displays with more information on the selected item.
5. Click **OK** to close the dialog.
6. To view more PC Explorer items, repeat steps 2-5.

Appendix I: Glossary: Main

See also: Glossary: Firewall

Adware
Adware, also known as advertising software, is often contextually or behaviorally based and tracks browsing habits in order to display third-party ads that are meant to be relevant to the user. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results.

Adware Bundler
An Adware Bundler is a downloadable program that is typically "freeware" because it is bundled with advertising software -- adware. The adware may function independently of the bundler program, but in some cases the bundler program will not function if the adware is removed, or will not install unless the adware is installed. Most Adware Bundlers install several adware applications from multiple adware vendors, each of which is governed by a separate End User License Agreement (EULA) and Privacy Policy. Some Adware Bundlers may not fully and properly disclose the presence of bundled advertising software during installation.

Adware Downloader
An Adware Downloader is a multi-dropper application that installs multiple advertising programs from a single adware vendor.

Adware Installer
An Adware Installer is a "freeware" program from an adware vendor that bundles advertising software (adware) from the adware vendor itself.

Adware, Low Risk
Low Risk Adware is advertising software that displays ads on the desktop but is installed with better notice, disclosure and user consent than the majority of adware programs. Nonetheless, some Low Risk Adware programs may still not fully disclose all potentially objectionable functionality during installation. Some Low Risk Adware programs display less intrusive forms of advertising, such as banner ads or text links embedded within the program itself. Low Risk Adware typically does not transmit personally identifiable information (PII) and is not considered a serious privacy risk.

Application
See program.

Anti-spyware Software
Software that protects a computer from spyware infection. Spyware protection software finds and removes spyware without system interruption.

Backdoor
A backdoor is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

Bot
See Zombie.

Botnet

Botnet is a collection of software robots (bots) that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software.

While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (zombies) running software, usually installed via worms, Trojans, or backdoors under a common command-and-control infrastructure.

Browser Hijacker or Overview Page Hijacker

A program that can change the settings in your Internet browser. Most often, this includes your search page URLs, in order to redirect all Internet searches to a specified pay-per-search site. Also targeted are your default home page settings, which can be diverted to another page, often a pornography site.

Browser Plug-in

A Browser Plug-in is a software module that is attached to the browser, usually Internet Explorer, and that works within the browser to provide additional functionality. Browser Plug-ins may be installed with adware and used to display advertising as well as redirect the browser to alternate sites and alternate search results. Many Browser Plug-ins also monitor user web surfing and search data to facilitate targeted, contextual advertising. A toolbar is one type of Browser Plug-in.

Cookies

Cookies are small text files that Web sites place on your computer to recognize users. On subsequent visits to the same site, the cookie records information about your activity on it. This is often used to gauge where on a site individual users tend to frequent in order to develop page content tailored to each user's preferences and to improve offerings on the site so that you will come back to visit again.

While cookies are not harmful to your computer, they can be an issue of privacy. Tracking cookies are greatest risk to your privacy. They track your location on the web - any site you visit.

Definitions

Definitions (often called threat definitions) are the basis that a antivirus or antispyware tool uses to compare against when protecting you from all sorts of malware, whether by scans, email protection, or real time protection.

Dialer (General)

A Dialer is a program that uses the computer's modem to dial telephone numbers, often without the user's knowledge and consent. A Dialer can connect to a toll number that adds long distance charges to the telephone bill without the user's knowledge or permission. Dialers may be downloaded through exploits and installed without notice and consent. A Dialer may be legitimate if downloaded and installed with full, meaningful, and informed user consent.

Drive-by download

When programs are downloaded without your knowledge or consent. This is most often accomplished when the user clicks to close or respond to a random advertisement or dialogue box.

E-Mail Flooder

An E-Mail Flooder is a program used to send mass e-mail to flood or disrupt a PC or network.

Exploit

An Exploit is software or code that targets security vulnerabilities, usually in the operating system or browser, but may also target vulnerabilities in other programs. Exploits are typically used to install malicious software on the victim's computer without the victim's knowledge or consent. An Exploit

may be used to install malware that gives the attacker complete access to and control of the affected computer from a remote location.

Firewall

A firewall is an electronic barrier on your computer where that all information coming in and going out must travel. A firewall prevents external computer systems from communicating directly with your computer. A firewall analyzes information passing between the two computers, and rejects it if it does not conform to pre-configured rules (or exceptions). See the Firewall Glossary for more related terms.

High Risks

High risks are typically installed without user interaction through security exploits, and can severely compromise system security. Such risks may open illicit network connections, use polymorphic tactics to self-mutate, disable security software, modify system files, and install additional malware. These risks may also collect and transmit personally identifiable information (PII) without your consent and severely degrade the performance and stability of your computer.

Hijacker

Hijackers are software programs that modify users' default browser home page, search settings, error page settings, or desktop wallpaper without adequate notice, disclosure, or user consent. When the default home page is hijacked, the browser opens to the web page set by the hijacker instead of the user's designated home page. In some cases, the hijacker may block users from restoring their desired home page. A search hijacker redirects search results to other pages and may transmit search and browsing data to unknown servers. An error page hijacker directs the browser to another page, usually an advertising page, instead of the usual error page when the requested URL is not found. A desktop hijacker replaces the desktop wallpaper with advertising for products and services on the desktop.

IRC bots

IRC (Internet Relay Chat) bots are sets of scripts or an independent program that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. It differs from a regular client in that instead of providing interactive access to IRC for a human user, it performs automated functions.

Joke Program

A Joke Program is software that is designed to mimic the actions of a virus but is not malicious and does not harm the machine.

Key Logger

A key logger is a program that captures and logs keystrokes on the computer without the user's knowledge and consent. The logged data may be encrypted and is typically sent to a remote attacker. The key logger is usually hidden from the user and may use cloaking (rootkit) technology to hide from other software in order to evade detection by anti-malware applications. Key loggers may be installed by trojans with other malicious software through exploits, and are often used by online criminal gangs to facilitate identity theft and bank fraud operations.

Known Risks (also known bads, known threats, or knowns)

A risk is described as being "known" based on Sunbelt Software's definitions in the security risk database and has been determined as being harmful based on analysis and history of reported cases. Much of this information comes from users like you who have ThreatNet enabled. You may, however, consider a "known" to NOT be a risk to you (i.e. Hotbar). Some programs use adware that *you* may want to run on your computer. In this case, you will want to always allow it to run.

Low Risk

Low Risk programs/software should not harm your machine or compromise your privacy and security unless it has been installed without your knowledge and consent. A Low Risk Software application may be a program that you knowingly and deliberately installed and that you wish to keep. Although some Low Risk Software programs may track online habits—as provided for in a privacy policy or End User License Agreement (EULA)—or display advertising within the applications themselves, these programs have only vague, minimal, or negligible effects on your privacy.

Malware

Malware, short for malicious software, is a general term with clearly hostile or harmful functionality or behavior that is used to compromise and endanger individual PCs as well as entire networks.

Operating System

The operating system is the underlying software that enables you to interact with your computer. The operating system controls the computer's storage, communications, and task management functions. Examples of common operating systems include Microsoft Windows, MS-DOS, MacOS, and Linux.

Opt-out

Options presented by spam email. These options are often fake. For example, if you respond to a request to remove something, you may well be subjecting yourself to more spam. By responding, the sender knows that your email account is active. A 2002 study performed by the FTC demonstrated that in 63% of the cases where spam offered a "remove me" option, the option either did nothing or resulted in more spam email.

Personally Identifiable Information (PII)

Information such as your name, address, phone number, credit card information, bank account information, or social security number.

Potentially Dangerous Tool

A Potentially Dangerous Tool is an application that is not necessarily harmful if properly installed by the user or administrator of the PC, but which could be harmful or disruptive to the user, PC, or network if deployed by unauthorized parties for potentially malicious purposes.

Potential Privacy Risk

Software designated Potential Privacy Risk includes programs that are not harmful to the user's system, but which may use inadequate privacy policies or poor disclosure of data collection and transmission practices, including personally identifiable information (PII) or non-personally identifying information, in the End User License Agreement (EULA).

Potentially Unwanted Program

Potentially Unwanted Programs include software that does not fit into another category (such as Low Risk Adware or Potential Privacy Risk) that users might want detected because the software includes some form of potentially objectionable functionality.

Privacy Policy

The responsibilities of an organization that is collecting personal information, as well as the rights of an individual who provides personal information. A legitimate organization should explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. Individuals should be able to obtain their own data and make corrections if necessary

P2P Program

A P2P (or Peer to Peer) Program is software that enables the user to participate in an online file sharing network and trade or share files with other users in the network. P2P Programs often bundle advertising software, but some P2P Programs are adware-free. P2P Programs are typically not harmful in and of themselves, but the user is at risk for infection with adware and/or malware though files downloaded from the file sharing network.

Program

A program or application is a set of instructions directing the computer to perform a task. This could be anything, from adding two numbers and outputting the result, to the complex instructions in the program of a computer game. A program can be safe or harmful.

Risk

See Known Risks.

Risk Definitions

See definitions.

Rogue Security Program

A rogue security program is software of unknown or questionable origin, or doubtful value. A rogue security program usually shows up on websites or SPAM emails as intrusive warnings that claim that your computer is infected and offer to scan and clean it. These should never be trusted. Reputable antivirus or antispyware companies will NEVER use this way of "notifying" you. A rogue security program may appear like an ordinary antivirus or antimalware program, but will instead attempt to dupe or badger you into purchasing the program. While some rogue security programs are the equivalent to "snake oil" salesman resulting in no good, others may actually result in harm by installing malware or even stealing the credit information that you enter and possibly resulting in identity theft. Further, you need to be cautious about closing or deleting these alerts, even when you know they're fake. Tips to protect yourself from fake antivirus programs.

Rootkit

A rootkit is software that cloaks the presence of files and data to evade detection, while allowing an attacker to take control of the machine without the user's knowledge. Rootkits are typically used by malware including viruses, spyware, trojans, and backdoors, to conceal themselves from the user and malware detection software such as anti-virus and anti-spyware applications. Rootkits are also used by some adware applications and DRM (Digital Rights Management) programs to thwart the removal of that unwanted software by users.

Security Disabler

A Security Disabler is a program that compromises or terminates security applications running on the machine, including software firewalls, anti-virus programs, and anti-spyware programs. A Security Disabler may also delete anti-virus and anti-spyware definitions. Some sophisticated Security Disablers are capable of terminating security software while giving the appearance that it is still running.

Service (Windows Service)

A Service is an executable that performs specific functions and is designed not to require user intervention. A service usually starts when the Windows operating system is booted and runs in the background as long as Windows is running. If the VIPRE Premium service fails, you can manually start the service.

Shareware
Software that is distributed for evaluation without cost. Shareware usually requires payment to the author for full rights to the software.

Spam
Unsolicited commercial email. It is often sent in bulk, via "open-relays" to millions of computer email accounts. It takes a toll on an Internet users' time, their computer resources, and the resources of Internet Service Providers (ISP). Most recently, spammers have begun to send advertisements via text message to cell phones.

Spyware
Spyware is software that transmits information to a third party without notifying you. It is also referred to as trackware, hijackware, scumware, snoopware, and thiefware. Some privacy advocates even call legitimate access control, filtering, Internet monitoring, password recovery, security, and surveillance software "spyware" because those could be used without notifying you.

Surveillance
A Surveillance Tool is a program that monitors and captures data from a computer including screenshots, keystrokes, web cam and microphone data, instant messaging, email, websites visited, programs run and files accessed and files shared on a P2P (peer to peer) network. Many Surveillance Tools can run in stealth mode, hidden from the user, and have the ability to store captured data for later retrieval by or transmission to another computer.

System Snooper
A System Snooper is a program that is used to monitor and record data on the computer's usage. System Snoopers may track address bar URLs, browser cache, search history, file download history, recently used documents, recently run programs, cookies, and index.dat files. While System Snoopers may have legitimate uses, they may also be used to monitor other people's computer use without their knowledge and consent. Some System Snoopers are easily visible to the user, while others may be hidden.

Threat
See Known Risks.

Threat Definitions
See definitions.

Threats, Misc.
Miscellaneous threats include applications that do not fit into other categories or that fall into multiple categories. Miscellaneous threats typically include some form of potentially objectionable functionality that may pose privacy or security risks to users and their PCs.

Toolbar
A Toolbar is a type of browser plug-in that adds a third-party utility bar to the web browser, usually just below or next to the browser's address bar. A Toolbar typically has a search function and provides search results for paid advertisers. It often has buttons that are links to advertisers' web pages. An advertising toolbar may track browsing and search queries in order to display contextually relevant search results and ads.

Traces
A trace is the smallest unit of malware that is detected and can include files, folders, or Registry keys/values. A risk is made up of these smaller units.

Trojan

A trojan is installed under false or deceptive pretenses and often without the user's full knowledge and consent. In other words, what may appear to be completely harmless to a user is in fact harmful by containing malicious code. Most trojans exhibit some form of malicious, hostile, or harmful functionality or behavior.

Trojan FTP

A Trojan FTP program is a File Transmission Protocol tool that allows an attacker to download, upload and replace files on the affected machine, typically for malicious purposes. A Trojan FTP is usually installed through an exploit without the victim's knowledge and consent, and is often used to host potentially dangerous or illegal content (warez, child porn, etc.) on the compromised computer.

Unauthorized Program

An Unauthorized Program in an I.T. environment could be any software program installed by users on the network that is not compliant with the I.T. and security policies of the network owner or administrator.

Unknown

A potential risk that has yet to be established as a "known" risk by Sunbelt Software's security risk database. An unknown could be safe to *your* computer; it just has yet to be determined to be either safe nor unsafe.

Virus

A computer virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as CD-ROMs or flash drives. Viruses can also spread via email through infected attachments and files. Most viruses include a "payload" that can be anywhere from annoying and disruptive to harmful and damaging; viruses can cause system damage, loss of valuable data, or can be used to install other malware.

Worm

A worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike viruses, however, worms spread without attaching to or infecting other programs and files. A worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through email by sending copies of itself to everyone in the user's address book. A worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some worms may be used to compromise infected machines and download additional malicious software.

Zombie/Bot

Zombies and Bots are programs used to compromise a computer and allow it to be remotely exploited by an attacker for specific malicious tasks. A computer infected with a Zombie or Bot may be used by an attacker to send spam, participate in a Distributed Denial of Service (DDOS) attack against web sites or other computers, or install adware and spyware for monetary gain. The "zombied" or compromised computer becomes part of a Botnet—a large network of other compromised machines that are controlled and used for malicious purposes by the Bot master.

Appendix II: Glossary: Firewall Terms

See also: Main Glossary

Application protocol

Application protocols are transmitted in packets of TCP or UDP protocol. They are used for transmission of user (application) data. In addition to standard application protocols which are available (i.e. SMTP, POP3, HTTP, FTP, etc.), application programmers may use a custom (non-standard) method for communication.

ARP

Acronym for Address Resolution Protocol. ARP is an IP service that maps physical addresses to logical addresses.

Browser

A browser is a software application which enables a user to display and interact with text, images, videos, music, games, and other information typically located on a Web page at a website on the World Wide Web or a local area network. Some examples include Internet Explorer (IE), Firefox, Opera, Netscape, and Chrome.

Buffer

A region of memory reserved for use as an intermediate repository in which data is temporarily held while waiting to be transferred between two locations or devices. For instance, a buffer is used while transferring data from an application, such as a word processor, to an input/output device, such as a printer.

Cookies

Cookies are small text files that Web sites place on your computer to recognize users. On subsequent visits to the same site, the cookie records information about your activity on it. This is often used to gauge where on a site individual users tend to frequent in order to develop page content tailored to each user's preferences and to improve offerings on the site so that you will come back to visit again.

While cookies are not harmful to your computer, they can be an issue of privacy. Tracking cookies are greatest risk to your privacy. They track your location on the web - any site you visit.

DHCP

Acronym for Dynamic Host Configuration Protocol. A TCP/IP protocol that enables a network connected to the Internet to assign a temporary IP address to a host automatically when the host connects to the network. See also IP address, TCP/IP. Compare dynamic SLIP.

Direction

Direction refers to the flow of traffic in and out of your computer. Traffic direction can be either inbound or outbound.

DNS

Acronym for Domain Name System. The hierarchical system by which hosts on the Internet have both domain name addresses (i.e. home.example.com) and IP addresses (i.e. 152.156.2.6). The domain name address is used by human users and is automatically translated into the numerical IP address, which is used by the packet-routing software. DNS names consist of a top-level domain (i.e. .com, .org, and .net), a second-level domain (the site name of a business, an organization, or an individual), and possibly one or more subdomains (servers within a second-level domain).

Exception

An exception, as it applies to the network security of the firewall, can be a user-defined or default program, port, or protocol that is allowed to communicate through the firewall.

Firewall

A firewall is an electronic barrier on your computer where that all information coming in and going out must travel. A firewall prevents external computer systems from communicating directly with your computer. A firewall analyzes information passing between the two computers, and rejects it if it does not conform to pre-configured rules (or exceptions).

IDS

Acronym for Intrusion Detection System. A type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, both inside and outside the organization. An IDS can detect a wide range of hostile attack signatures, generate alarms, and, in some cases, cause routers to terminate communications from hostile sources.

ICMP

Acronym for Internet Control Message Protocol. A protocol used for transmission of control messages. Several types of such messages are available, such as a report that the destination is not available, redirection request or response request (used in the PING command). ICMP is an error-reporting mechanism to control the flow of traffic network over IP and UDP, ensuring that the data can be reliably delivered.

IGMP

Acronym for Internet Group Membership Protocol. A protocol used by IP hosts to report their host group memberships to any immediately neighboring multi-cast routers.

IP Address

Acronym for Internet Protocol. A protocol transmitting all Internet protocols in its data part. The header of this protocol provides essential routing information, such as source and destination IP address (which computer sent the message and to which computer the message should be delivered).

Packet

A packet is a segment of data sent from one computer or network device to another computer or network device over a network. Packets may contain such information as its source, destination, size and other useful information, helping the packet get to its destination.

Port

The most essential information in TCP and UDP packet is the source and destination port. The IP address identifies a computer in the Internet, whereas a port identifies an application running on the computer. Ports 1-1023 are reserved for standard services and the operating system, whereas ports 1024-65535 can be used by any application. In a typical client to server connection, usually the destination port is known (connection is established for this port or UDP datagram is sent to it). The source port is then assigned by the operating system automatically.

PPTP

Acronym for Point-to-Point Tunneling Protocol. An extension of the Point-to-Point Protocol used for communications on the Internet. PPTP was developed by Microsoft to support virtual private networks (VPNs), which allow individuals and organizations to use the Internet as a secure means of

communication. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. See also virtual network.

Protocol

A protocol is the set of rules governing the format and control of messages being sent around a network.

Proxy

A proxy is an intermediary where traffic is first directed. A firewall proxy directs traffic through the firewall application where it is filtered before passing it on to the viewing application, such as a web browser.

Rule

A rule, as it applies to the network security of the firewall, consists of one or more exceptions (e.g. applications, protocols, ports, and direction of traffic) that is user-defined.

Scope

Scope refers to the extent that a rule or exception is applied. For example, when adding a port as an exception to the Network Security, you can apply the scope to any device connected to your network, whether this be for all computers at your home or all devices connected to via a WiFi hotspot. You can also limit the scope to one or more computers by IP address, thus restricting the scope to just one or more machines.

TCP

Acronym for Transmission Control Protocol. It is used as a transmission protocol for most application protocols, such as SMTP, POP3, HTTP, FTP, Telnet, etc. TCP operates at a higher level (compared to IP, which operates on the lower level), concerned only with the two end systems—for example, a Web browser and a Web server. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Besides the Web, other common applications of TCP include e-mail and file transfer. Also, TCP controls segment size, the rate at which data are exchanged, and network traffic congestion.

TCP/IP

TCP/IP is a general term for protocols used in communication over the Internet. Data is divided into data items called packets within individual protocols. Each packet consists of a header and a data part. The header includes routing information (i.e. source and destination address) and the data part contains transmitted data.

The Internet protocol stack is divided into several levels. Packets of lower protocols encapsulate parts of higher-level protocols in their data parts (i.e. packets of TCP protocol are transmitted in IP packets).

UDP

Acronym for User Datagram Protocol. UDP is a connectionless protocol that uses a simple transmission model without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to using delayed packets. UDP protocol is used especially for transmission of DNS queries, audio files, video files, or other types of streaming media which promote speed over reliability.

VPN

Acronym for Virtual Private Network. Nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines.

WAN

A WAN (wide area network) formed of permanent virtual circuits (PVCs) on another network, especially a network using technologies such as ATM or frame relay.

Web browser

See browser.

WiFi

WiFi, Wireless Fidelity, is a radio frequency standard that is used to connect devices (e.g. laptops, WiFi phones, or other suitable portable devices) together using a wireless connection. Instead of computers being connected with network cables, signals are sent over radio frequencies using wireless network cards and hubs.

WiFi hotspot

A WiFi hotspot is a venue that offers WiFi access. The public can use a laptop, WiFi phone, or other suitable portable device to access the Internet.

Appendix III: Troubleshooting

Troubleshooting: Computer Performance Issues

Are you running another antivirus or antispyware product?

Running more than one antivirus, antispyware, or antimalware product (e.g. AVG, Kaspersky, McAfee, Norton, NOD32, Panda, Symantec, ZoneAlarm, etc.) with real-time protection turned on can cause serious degradation in your computer's performance. Only one should be active at a time. In addition, you can use several scan tools to perform manual scans, but do so one at a time for the best performance. Please refer to those products' documentation for specific advice.

Are you running another firewall product?

Also, running more than one firewall at the same time can make it seem that your computer is operating slower. It is recommended to uninstall or completely disable other firewall products.

Is VIPRE Premium currently scanning?

If VIPRE Premium is scanning and you are running other programs that require large amounts of memory, such as computer games and video/image editing, you may want to consider discontinuing the scan and running it later after you are finished doing what you are doing. You can do any of the following:

- To temporarily pause the scan, right-click on the green VIPRE Premium icon in your system tray (lower-right corner of your computer screen) and select **Scan>Pause Scan**. You can resume the scan later by selecting **Scan>Resume Scan**.
- To cancel the scan, right-click on the green VIPRE Premium icon in your system tray (lower-right corner of your computer screen) and select **Scan>Abort Scan**. You can run the scan again later by selecting **Scan>Quick** or **Deep**.

Tip: Schedule a scan to run during a time that your computer is most likely not being used and will be turned on. How?

Troubleshooting: VIPRE Premium Icon in the System Tray is Red

If the VIPRE Premium icon in your system tray (lower-right area of your computer screen) is red, you are being alerted that the VIPRE Premium service is disabled. You will need to restart the service.

To start the VIPRE Premium service:

1. Right-click on the red VIPRE Premium icon and then select **Start Anti-Malware Service** from the menu.

   The VIPRE Premium service starts and should be running normally. Also, the icon will change from red to blue or gray.

2. Please, contact Technical Support if you are still experiencing problems.

Getting Help with VIPRE Premium

VIPRE Premium offers you several ways to get help:

Help

The **Help** is your primary resource for answers to questions you may have while using VIPRE Premium. The Help contains overviews and procedural information about the tasks you can perform in the application, as well as descriptions of each screen and dialog box in the application with detailed information about each field they contain. Whenever you want to know about a screen or dialog box that you are in, you can press F1 on your keyboard or click the **Help button**. The applicable help topic will display for that screen.

Once in the Help, you can locate the information you need any of the following ways:

- **Contents:** Select **Help>Contents**. This opens the Help Contents pane. Navigate through the books and pages to find the information you need. When you click a topic page, it opens.
    - **Glossary:** Select **Help>Contents** tab**>Glossary** book**>Glossary** page. This opens the glossary topic with a linked alphabet at the top of the page. Click any of the linked letters in the glossary to see the definitions under that letter. You can also scroll down to the desired term.
- **Index:** Select **Help>Index** tab. This opens the Help Index pane. Navigate through the index to find keywords for the information you need. When you click a keyword in the index, the associated topic displays.
- **Search:** Select **Help>Search** tab. This opens the Help Search pane. Enter one or more keywords in the field and click **Search**. Links to topics containing those keywords are listed below. When you click a topic link, that topic displays.
- **Favorites:** When you are in a topic that you want to put in your "Favorites," select **Help>Favorites** tab and click **Add** at the bottom. The added topic is then listed in the "Topics" area for easy access the next time you need it.

Downloadable Manuals

- The **Quick Start Guide** covers the basic steps needed to get VIPRE Premium up and running right away.

Go to the product page and click on "User's Guide."

VIPRE Premium PC Rescue Program

The VIPRE Premium PC Rescue Program is a command-line utility that will scan and clean an infected computer that is so infected that programs cannot be easily run.

http://live.sunbeltsoftware.com/

Knowledge Base

You can browse the online Knowledge Base for articles covering the most common support issues.

Click http://support.sunbeltsoftware.com/, then select your product from the drop-down box and click "Search."

Sunbelt Support Forum

The Sunbelt Support Forum is a peer-to-peer support forum to get help and tips from fellow VIPRE Antivirus Premium users.

http://supportforums.sunbeltsoftware.com/

SunbeltLabs

SunbeltLabs offers you a central access to our research and tools for consumers, enterprises, and security researchers. We welcome your submissions and feedback to help make the Internet safer and our products more effective.

SunbeltLabs™

Contact Sunbelt Software Technical Support

You can contact the US-based Sunbelt Software Technical Support team and get answers to your specific support issues any of the following ways:

- Website: http://www.sunbeltsoftware.com/Support/
- Product Enhancement Request
- Email: support@sunbeltsoftware.com
- US/Canada Toll-free: 877-673-1153
- Worldwide: 1-727-562-0101
- Address:
  Sunbelt Software, Inc.
  33 North Garden Avenue, Suite 1200
  Clearwater, Florida 33755