BP Internet Security™ User's Manual

Table of Contents

1 PART ONE

Before you use BP Internet Security™

Congratulations on your purchase of BP Internet Security™. Big Planet has partnered with the leading Internet security software companies to deliver to you the best possible solution to help you protect yourself, your family, and your computer.

Part One focuses on:

SECTION 1: Installing BP Internet Security™
SECTION 2: Getting to know BP Internet Security™

SECTION 1
Installing BP Internet Security™

You are about to begin installation of BP Internet Security™. To ensure you install BP Internet Security™ properly, please follow the instructions below.

NOTE BEFORE INSTALLATION: If you have installed a stand-alone version of ZoneAlarm™, you must uninstall it prior to installing BP Internet Security™. Also, be sure to shut down all other applications prior to installing BP Internet Security™. If you have any questions please call Technical Support at 1-800-487-1000 between 7 a.m. and 10 p.m. MST Monday through Friday, and between 8 a.m. and 8 p.m. MST Saturday and Sunday.

1.1 Get your License Key

1. Before you install BP Internet Security™ you must obtain a License Key by registering your product. You will need the following information:

- Proof of Purchase code, located on the inside cover of the CD storage case.
- Online customer account, if you do not already have one.
- Major credit card, to subscribe to the required (and very important) update service.

2. To get your License Key go to www.bigplanetusa.com/activatesecurity and follow the simple online instructions. Remember to print a copy of your License Key so you'll have it handy for the next steps.

1.2 Install BP Internet Security™

1. Insert your BP Internet Security™ CD into the CD-ROM drive of your computer. When the BP Internet Security™ setup screen launches, follow the simple prompts to begin installation. (If the Install program does not automatically start when you put the CD in your computer, open “My Computer,” select the “CD Drive,” and open “Setup.exe.”)

2. Accept the BP Internet Security™ License Agreement. Click **NEXT**.

3. Decide where you want BP Internet Security™ to be loaded. Click **NEXT**.

4. Follow the two important steps on this page:

a. Enter the product License Key you obtained and printed out into the space provided. If you don't have a license key, stop installation and complete STEP 1.1. ***Please note: your License Key is case sensitive. All lowercase entries are alphabetical letters; uppercase entries are numbers. Also note, the "0" entry is a zero and the "1" entry is the number one.***

b. Set up an administrative password. Using an administrative password will ensure that others will not change the security settings you select without your permission. If you wish, you may set up this password later using the BP Internet Security™ control panel. Big Planet strongly recommends you set up and use a password.

c. Click **NEXT** when finished.

5. Click **INSTALL** to begin BP Internet Security™ product installation. This may take several minutes to complete.

6. When done, click **FINISHED**.

7. Carefully review the ReadMe document that appears after the install has completed. You may want to print a copy of the ReadMe document for future reference. Close by clicking on the **[X]** button in the upper right-hand corner of the ReadMe.

8. You will be prompted to restart your computer in order for BP Internet Security™ to begin protecting your computer.

1.3 Set up BP Internet Security™ to work on your computer

Upon restarting your computer, the following will happen:

1. The BP Internet Security™ Tutorial will appear. Please take a few minutes to review this brief tutorial in order to familiarize you with BP Internet Security™. Click **FINISH** when done.

2. If your computer is already connected to an Internet or network connection, you will be prompted to configure your connection using the NETWORK CONFIGURATION WIZARD. If the NETWORK CONFIGURATION WIZARD does not appear immediately, you will be asked to configure your network once BP Internet Security™ detects a live Internet or network connection. You may see this prompt each time your computer recognizes a new high-speed, dial-up, or wireless connection. Follow the prompts through this simple process by clicking **NEXT**.

3. If you set up an administrative password previously, you will be prompted for it.

4. You are now ready to use BP Internet Security™.

SECTION 2
Getting to know BP Internet Security™

2.1 What's included in BP Internet Security™?

Before you begin using BP Internet Security™, it is important to understand the levels of protection associated with it, as well as the design and functionality of the product control panel. BP Internet Security™ protects you with the follow components:

• **Anti-spyware** is software that detects, isolates, and eliminates spyware loaded onto your computer without your knowledge.

• **Web filtering** is software that allows computer users to determine which Web content they will allow onto your computer through their browser.
• **A firewall** is software that sets up a defense barrier around your computer so that hackers and online criminals cannot access your computer's information.
• **Email protection** helps eliminate unsolicited and annoying email—known as "spam"—and protects you from identity theft caused by fraudulent email.

These tools complement your existing anti-virus solution to give you the most advanced security on the Internet.

2.2 Getting Started
Once installed, you can access BP Internet Security™ and its components by clicking on the BP icon in your Windows system tray.

2.3 The BP Internet Security™ Control Panel
The tabs along the left-hand side of the screen allow you to easily navigate through the Control Panel.

• **The Main Menu tab** allows you to quickly and easily review and manage your security settings.
• **The Parental Control tab** gives you control over Web content filtering settings, letting you decide what content enters your home and what is kept out.
• **The Reports tab** allows you to review the specific threats that BP Internet Security™ has protected you from recently.
• **The Information tab** lets you register your product, update your software, and reset your password.
• **The Options tab** lets you decide whether or not to block unwanted advertising and annoying pop-ups, and lets you restore your originally installed default product settings.

When you finish making changes to your security settings, you can hide the control panel by clicking on the "Hide" button in the lower right hand corner. To exit BPIS and stop protecting your computer, right-click the BP icon in your system tray and select **Exit.**

2.4 Where can I get help?
If you need help while using BP Internet Security™ you can click on the "**Help**" button in the upper right corner of the main menu. You can then view the tutorial by clicking on the **Tutorial** link. Additional help options available include the BP Internet Security™ FAQ, which is updated and posted on the Big Planet website.

You can also call Big Planet technical support at 800-487-1000, available between 7 a.m. and 10 p.m. MST Monday through Friday, and between 8 a.m. and 8 p.m. MST Saturday and Sunday.

A more detailed explanation of the functions of BP Internet Security™ and the control panel features will follow in subsequent sections of this User Guide.

2 PART TWO

Getting to know the BP Internet Security™ Control Panel

All of the functionality of BP Internet Security™ are easily managed from a single product control panel. It has been built so you can easily navigate your way through the product features using the tabs along the left-hand side of the screen. The five categories outlined on the control panel are:

- Main Menu
- Parental Control Menu
- Reports Menu
- Information Menu
- Options Menu

Instructions and hints on how to use these pages to maximize the benefits of BP Internet Security™ are outlined in the following sections:

SECTION 3: Using the Main Menu
SECTION 4: Using the Parental Control Menu
SECTION 5: Using the Reports Menu
SECTION 6: Using the Information Menu
SECTION 7: Using the Options Menu
SECTION 8: BP Internet Security™ Product Pre-configurations
SECTION 9: Using the advanced features of BP Internet Security™ ZoneAlarm™

SECTION 3
Using the Main Menu

The Main Menu allows you to manage the settings for protecting your privacy and the privacy of your computer. It is broken into two main sections:

- Protect My Computer
- Actions

3.1 Protect My Computer

The Protect My Computer section contains the following functions:

- Firewall and program monitoring
- Spyware defense
- Virus protection
- Email protection

1. Firewall and program monitoring: This function enables BP Internet Security™ to activate the firewall so that it hides your computer on the Internet. Hackers will not be able to see it. It also restricts

Internet access to your computer by unknown programs. The firewall has been preset to **ON** for you. Big Planet recommends that you leave this setting on. To turn this function off, simply click the **ON** button and it will switch to **OFF**.

2. Spyware defense: This function tells BP Internet Security™ to scan your computer weekly to find and remove any new spyware threats. Spyware defense has been preset to **ON** for you. Big Planet recommends that you leave this setting on. If you decide to turn this function off, simply click the **ON** button and it will turn **OFF**.

3. Virus protection: This function provides your computer with maximum protection from harmful, invasive programs called "viruses" that can be transmitted to your computer through your Internet connection or through email attachments. Virus protection has been preset to **ON** for you. Big Planet recommends that you leave this setting on. To turn this function off, simply click the **ON** button and it will switch to **OFF**.

4. Email protection: This function protects you from fraudulent email "phishing" attempts that can steal your identity, and helps filter and eliminate spam in your email account. Email protection has been preset to **ON** for you. Big Planet recommends that you leave this setting on. To turn this function off, simply click the **ON** button and it will switch to **OFF**.

3.2 Actions
The Actions section of the Main Menu lets you run scans for spyware and viruses at any time, as well as adjust your security settings for short periods of time. The Actions menu contains the following functions:

- Find and quarantine all spyware now
- Find and remove all viruses now
- Temporarily reduce security settings

1. Find and quarantine all spyware now: This function tells BP Internet Security™ to run a detailed scan of your entire computer in order to find and remove any spyware already loaded onto your computer. Big Planet recommends running this detailed scan of your system at least once a week.

To run a detailed scan of your system, follow these steps:

a. Click the **SCAN NOW** button. The BP Internet Security™ ZoneAlarm™ page will open and ZoneAlarm™ will automatically begin an in-depth scan of your computer. Depending upon your operating system, your computer's speed, and the number of files BP Internet Security™ has to inspect, this scan could take several minutes to complete. BP Internet Security™ will begin the scan by reviewing files on your computer.

b. As BP Internet Security™ locates potentially dangerous software, the number of dangerous spyware software will be counted and reported to you in the **SPYWARE FOUND** field.

c. BP Internet Security will automatically remove the spyware from your computer.

d. When BP Internet Security™ finishes scanning your computer, the **Scan Results** page will appear, displaying the name of the spyware, the risk it poses to your computer, and what BP Internet Security™ has done with it.

2. Find and remove all viruses now: This function tells BP Internet Security™ to run a detailed scan of your computer to find and remove any viruses that have infected it.

To run a detailed virus scan of your computer, follow these steps:

a. Click the **SCAN NOW** button. The BP Internet Security™ ZoneAlarm™ page will open and ZoneAlarm™ will automatically begin an in-depth scan of your computer. Depending upon your operating system, your computer's speed, and the number of files BP Internet Security™ has to inspect, this scan could take several minutes to complete. BP Internet Security™ will begin the scan by reviewing files on your computer.

b. As BP Internet Security™ locates viruses, the number of viruses will be counted and reported to you in the **INFECTIONS FOUND** field.

c. BP Internet Security will automatically quarantine, disable, or remove the viruses from your computer.

d. When BP Internet Security™ finishes scanning your computer, the **Scan Results** page will appear, displaying the name of the virus, the risk it poses to your computer, and what BP Internet Security™ has done with it.

3. Temporarily reduce security settings: This function allows you to temporarily reduce your security settings if you are having trouble accessing a desired website. When you click **REDUCE,** BP Internet Security™ will turn off for 30 minutes. At the end of 30 minutes, BP Internet Security™ will automatically turn back on and resume protecting your computer.

SECTION 4
Using the Parental Control Menu

The Parental Control Menu, accessible from the BP Internet Security™ control panel, lets you decide what Web content is allowed onto your computer, and what will be blocked.

4.1 Protect My Access

The Protect My Access section contains the following two functions:

- Web content filtering
- Decide which web content to block

1. Web content filtering: This function enables BP Internet Security™ to block objectionable websites based on your personal preferences. Web content filtering has been preset to **ON** for you. Big Planet recommends that you leave this setting on. To turn this function off, simply click the **ON** button and it will switch to **OFF**.

2. Decide which web content to block: This function takes you to a detailed listing of potentially objectionable Web content that you can decide to block. Big Planet recommends that you review this list shortly after installing BP Internet Security™. Follow these steps to set your Web content filtering:

a. To access the detailed listing so you can make your selections, click on the **SET** button.

b. You will be asked whether or not you want to continue on to the advanced Web-filtering settings. Click **YES**. If you click **NO** you will be returned to the BP Internet Security™ Main Menu.

c. After clicking **YES,** the Web filtering preferences page will appear.

d. Scroll down the list and check all of the categories you wish to restrict your computer from accessing. You may select (block all) by clicking **CHECK ALL**, or deselect (unblock all) by clicking **CLEAR ALL**. Before the Web filtering tools accept your selections, you will be prompted for your administrative password.

e. After making your selections, click on the **X** button on the upper right-hand corner of the page.

f. A window will appear with instructions on how to shut down the ZoneAlarm Security Suite. Simply click **OK** in this window. Your Web-filtering selections will go into effect immediately.

SECTION 5
Using the Reports Menu

The Reports Menu provides a dynamic security report that will inform you of the Internet threats BP Internet Security™ is monitoring and blocking. The information listed on the Reports page includes:

- **Unauthorized intrusions blocked:** A count of all outside intruders the firewall has successfully denied access to your computer.
- **Dangerous intrusions blocked:** A count of all hostile attempts by others to access your computer, but were denied access by the firewall.
- **Programs approved for Internet access:** A count of all programs on your PC that have been given permission to access the Internet. Big Planet has pre-configured over 20 common programs for permission to access the Internet. If a program has not been approved to access the Internet, a pop-up window may appear to ask if you do or do not wish to grant a specific program permission to access the Internet.
- **Dangerous email attachments quarantined:** A count of all suspicious email attachments that have been quarantined by BP Internet Security™ for further inspection. If an email attachment begins performing virus-like activity, this feature stops the attached program from taking action and quarantines it.
- **Email spam quarantined:** A count of all spam emails quarantined by BP Internet Security™.
- **Fraudulent emails blocked:** A count of emails suspected of being fraudulent and/or dangerous and quarantined by BP Internet Security™.
- **Cookies blocked:** A count of all cookies that were quarantined during the last scan of your system.
- **Spies treated:** A count of all spyware programs that were removed or disabled during the last scan of your system.
- **Date of last spyware scan:** The date when your computer was last scanned for viruses.
- **Viruses treated:** A count of all viruses that were removed or disabled.
- **Date of Last Virus Scan:** The date when your computer was last scanned for viruses.

SECTION 6
Using the Information Menu

The Information menu allows you to manage the important functionality of BP Internet Security™ to ensure you are getting the most out of software. It is broken into three sections:

- Register
- Update
- Password

6.1 Register

The Register section contains the following selection:

1. View your license key: You may be asked by Big Planet support to find your license key. Your license key is used to ensure that you continue to receive product upgrades.

a. To view your license key, click on the green **GO** button.

b. When you have finished, click **OK**. You may cancel this process and return to the Information menu by clicking **CANCEL**.

6.2 Update
The Update section contains the following selection:

1. Check now for program updates: BP Internet Security™ will alert you when updates are available. You can also check for updates anytime yourself using the **UPDATE** utility.

a. To check for software updates click on the green **GO** button.

b. BP Internet Security™ will check for software updates for you and automatically load any updates that it locates. It will alert you when it has completed this process. Click **OK** when finished.

c. BP Internet Security™ will also alert you if your software is currently up-to-date. Click **OK** when finished.

6.3 Password
To avoid unauthorized changes to your security settings, **BIG PLANET HIGHLY RECOMMENDS THAT YOU PASSWORD PROTECT YOUR SECURITY SETTINGS FROM UNWANTED CHANGES**. If you did not create a password during installation, you can create one at any time here. A password will allow you to lock your current settings in your control panel. This password will allow you to maintain and adjust appropriate security settings. When this feature is off, a password will not be required to change your security settings. **DO NOT LOSE YOUR PASSWORD!** Once you set your password, all changes to your BP Internet Security settings will require you to use this password.

1. Password protection: If you established an administrative password for BP Internet Security™ during installation then the green **ON** button will appear. If you did not set up a password at that time or if you have already turned this protection off, a red **OFF** button will appear.

If you already have a password, but your password protection is turned off, click the red **OFF** button. It will change to a green **ON** button.

If you do not have an administrative password and would like to set one up, follow these steps:

a. Click the red **OFF** button.

b. You will be prompted to enter a new password in the field provided.

c. Verify your new password by retyping it in the **Verify Password** field.

d. Click **SET** to establish your new password. You will be alerted that your new password has been created.

e. You may click **CANCEL** to stop the password creation process and return to the Information menu.

f. After setting up your new password, click the red **OFF** button to turn password protection **ON**.

2. Create or Change Password: Use this button if you would like to change your existing password. NOTE: If you did not create a password during installation, follow the instructions listed above.

To change your password, follow these steps:

a. Click on the green **GO** button.

b. A new window will appear that will prompt you for your old password.

c. It will also ask you for a new password. Retype the new password in the **Verify Password** field.

d. Click the green **SET** button to complete this process. You may click on **CANCEL** at any time prior to clicking **SET**.

e. You will be notified that your password has been updated. Click **OK** to return to the Information Menu.

SECTION 7
Using the Options Menu

The Options Menu allows you to adjust the protection levels pre-configured for you BP Internet Security™ to ensure that you are getting the protection you need. The Options Menu is divided into two sections:

- Don't Bug Me
- Settings

7.1 Don't Bug Me

This feature allows you to block unwanted banner ads and annoying pop-up advertisements from appearing on your computer while you are browsing the Internet. NOTE: Don't Bug Me is administrator password protected. In order to make changes to settings in this section, you will be prompted for your password if you have not already logged on as the administrator.

The Don't Bug Me section contains the following features:

1. Advertisement blocking: Advertisement blocking prevents banner advertisements normally shown on Web pages you visit from being displayed. This feature has been preset to be off. Big Planet recommends turning this feature on. To turn advertising blocking on, click on the red **OFF** button. It will switch to **ON**.

2. Pop-up window ad blocking: Popup blocking prevents advertiser's unsolicited pop-up advertisements from being displayed. This feature has been preset to be off. Big Planet recommends turning this feature on. To turn pop-up window ad blocking on, click on the red **OFF** button. It will switch to **ON**. NOTE: The BP Toolbar will also perform this function.

3. Windows Messenger pop-up blocking: Online advertisers take advantage of the Windows Messenger service to deliver unsolicited pop-up ads, even when the computer is not browsing the Internet. Big Planet recommends keeping this feature on. To turn Windows Messenger pop-up blocking off, click the green **ON** button. It will switch to **OFF**.

7.2 Settings

1. Restore Original Security Settings

This allows you to restore all of the security settings in BP Internet Security™ back to the recommended default settings that your product was shipped with. This feature can be especially helpful if you have recently changed some of your security settings and you can no longer access certain web pages or programs.

a. Restore original computer settings: Restores all of your BP Internet Security™ settings to the original factory recommended settings.

1. To restore your computer to the original factory shipped security settings, click on the green **GO** button.

2. BP Internet Security™ will ask you if you want to reset to the default settings and erase all changes since installation. If you want to do this, click **YES.** If you do not want to do this, click **NO** and you will be returned to the Information Menu.

3. After clicking **YES** you will be prompted for your password.

4. After inputting your password, click the green **OK** to proceed. You can click on the red **CANCEL** button to return to the Information Menu without making any changes to your settings.

5. After clicking **OK**, you will be notified that all of your security settings have been reset to the original system defaults.

b. **Harmful cookie defense:** This will enable BP Internet Security™ to block only potentially harmful cookies that Web sites store on your computer to keep track of you. This function has been preset to **ON** for you. Big Planet recommends keeping this feature on. To turn the Harmful cookie defense off, click on the green **ON** button. It will switch to **OFF**.

SECTION 8
BP Internet Security™ Product Pre-Configurations

Big Planet has pre-configured your security settings for your home computer. There is no need to change your Internet security settings after installing BP Internet Security™. Big Planet has worked with security experts at our technology partners (Zone Labs and Cerberian) to ensure that once installed, BP Internet Security™ is properly configured to immediately start protecting you against the very latest online security threats. Pre-configurations are set as follows:

8.1 Firewall Pre-configurations

- Internet Zone Security—High
- Trusted Zone Security—Medium
- Program Control—Medium
- Alert Events shown—OFF
- Event Logging—ON
- Program Logging—High

8.2 Web-Filtering Pre-configurations

- Cookie Control—Medium
- Ad Blocking—OFF
- Mobile Code Control—OFF
- Clean Cache Automatically—OFF
- Inbound Mailsafe protection—ON
- Outbound Mailsafe protection—ON
- Web filtering—ON
- Smart filtering—ON

Basic pre-configurations can be changed from the BP Internet Security™ Control Panel, while the advanced pre-configurations must be adjusted from within the user interfaces for the ZoneAlarm™ firewall and Web-filtering control panel. To access these control panels click on the icons loaded in the Windows™ system tray. To better understand the advanced functionality of the ZoneAlarm™ firewall with Web-filtering, please consult the ZoneAlarm™ product manual listed in the next section.

SECTION 9
Using the advanced features of BP Internet Security™ ZoneAlarm Pro™

9.1 The BP Internet Security™ ZoneAlarm™ firewall with Web-filtering Product Manual
The BP Internet Security™ ZoneAlarm™ firewall with Web-filtering product manual can be accessed through the following Internet link:
http://download.zonelabs.com/bin/media/pdf/zaclient60_user_manual.pdf

3 PART THREE

BP Internet Security™ Help

The chapters in Section Three focus on:

SECTION 10: Advanced Technical Troubleshooting

SECTION 10
Advanced Technical Troubleshooting

This section provides guidance for troubleshooting issues you may encounter while using BP Internet Security™ ZoneAlarm™ software.

10.1 VPN

If you are having difficulty using VPN software with BP Internet Security™ ZoneAlarm™ software, refer to the table for troubleshooting tips provided in this section.

1. Configuring BP Internet Security™ ZoneAlarm™ software for VPN traffic

If you cannot connect to your VPN, you may need to configure BP Internet Security™ ZoneAlarm™ software to accept traffic coming from your VPN.

To configure BP Internet Security™ ZoneAlarm™ software to allow VPN traffic:

a. Add VPN-related network resources to the Trusted Zone. See "Adding to the Trusted Zone" on page 49 of the ZoneAlarm™ User Guide.

b. Grant access permission to the VPN client and any other VPN-related programs on your computer. See "Setting permissions for specific programs" on page 78 of the ZoneAlarm™ User Guide.

c. Allow VPN protocols. See "Adding a VPN gateway and other resources to the Trusted Zone" on page 39 of the ZoneAlarm™ User Guide.

2. VPN auto-configuration and expert rules

If you have created expert firewall rules that block VPN protocols, BP Internet Security™ ZoneAlarm™ software will not be able to automatically detect your VPN when you initiate a connection. To configure your VPN connection, you will need to make sure that your VPN client and VPN-related components are in the Trusted Zone, and that they have permission to access the Internet. See "Configuring your VPN connection" on page 37 of the ZoneAlarm™ User Guide.

3. Automatic VPN detection delay

BP Internet Security™ ZoneAlarm™ software periodically polls your computer to determine if supported VPN protocols are engaged. Upon detection, BP Internet Security™ ZoneAlarm™ software prompts you to configure your connection automatically. If you have recently installed a VPN client and have tried to connect BP Internet Security™ ZoneAlarm™ software may not have detected your VPN configuration. If

you prefer BP Internet Security™ ZoneAlarm™ software to configure your connection automatically, you can wait ten minutes, and then try connecting again. If you prefer to connect right away, you can configure your connection manually. See "Configuring your VPN connection" on page 37 of the ZoneAlarm™ User Guide.

10.2 Networking

1. Making your computer visible on your local network
If you can't see the other computers on your local network, or if they can't see your computer, it is possible that BP Internet Security™ ZoneAlarm™ software is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible on the local network:

a. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone," on page 49 of the ZoneAlarm™ User Guide.

b. Set the Trusted Zone security level to Medium, and the Internet Zone security level to High. This allows trusted computers to access your shared files, but blocks all other machines from accessing them. See "Setting advanced security options" on page 44 of the ZoneAlarm™ User Guide.

2. Sharing files and printers across a local network
BP Internet Security™ ZoneAlarm™ software enables you to quickly and easily share your computer so that the trusted computers you're networked with can access your shared resources, but Internet intruders can't use your shared resources to compromise your system. BP Internet Security™ ZoneAlarm™ software will detect your network automatically and display the New Network alert. You can use the alert to add your network subnet to the Trusted Zone. For more information, see "New Network alert" on page 230 of the ZoneAlarm™ User Guide.

To configure BP Internet Security™ ZoneAlarm™ software for secure sharing:

a. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone" on page 49 of the ZoneAlarm™ User Guide.

b. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files. See "Choosing security levels" on page 43 of the ZoneAlarm™ User Guide.

c. Set the Internet Zone security level to High. This makes your computer invisible to non-trusted computers. See "Setting the security level for a Zone" on page 43 of the ZoneAlarm™ User Guide.

3. Resolving a slow start up
If BP Internet Security™ ZoneAlarm™ software is configured to load at startup, some users connected to the LAN may find that it takes several minutes for the startup process to finish. In most cases, this is because your computer needs access to your network's Domain Controller to complete its startup and login process, and BP Internet Security™ ZoneAlarm™ software is blocking access because the Domain Controller has not been added to the Trusted Zone. To solve this problem, add the host name or IP address of your network's Domain Controller to the Trusted Zone.

10.3 Internet Connection

1. Connecting to the Internet fails after installing BP Internet Security™ ZoneAlarm™ software
If you are unable to connect to the Internet after installing BP Internet Security™ ZoneAlarm™ software, the first troubleshooting step is to determine whether BP Internet Security™ ZoneAlarm™ software is the cause. If you are unable to follow any of the steps below, contact Big Planet technical support.

To determine if BP Internet Security™ ZoneAlarm™ software is the cause of connection problems:

a. Select Overview/Preferences.

b. In the General area, clear the checkbox labeled "Load BP Internet Security™ ZoneAlarm™ software at startup." A warning dialog labeled Zone Labs TrueVector Service opens.

c. Click **YES** in this dialog box.

d. Restart your computer, then try to connect to the Internet.

e. If you can connect: Your BP Internet Security™ ZoneAlarm™ software settings may be the cause of your connection problems. Make sure that your browser has access permission.

f. If you cannot connect—your BP Internet Security™ ZoneAlarm™ software settings are not the cause of your connection problems.

2. Allowing ISP Heartbeat messages

Internet Service Providers (ISPs) periodically send heartbeat messages to their connected dial-up customers to make sure they are still there. If the ISP cannot determine that the customer is there, it might disconnect the customer so that the user's IP address can be given to someone else. By default, BP Internet Security™ ZoneAlarm™ software blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet. To prevent this from happening, you can identify the server sending the messages and add it to your Trusted Zone or you can configure the Internet Zone to allow ping messages.

a. Identifying the source of the heartbeat messages—This is the preferred solution because it will work whether your ISP uses NetBIOS or ICMP (Internet Control Messaging Protocol) to check your connection, and it allows you to maintain high security for the Internet Zone.

To identify the server your ISP uses to check your connection:

1. When your ISP disconnects you, click Alerts & Logs/Log Viewer.

2. In the alerts list, find the alert that occurred at the time you were disconnected.

3. In the Entry Detail area, note the Source DNS detected. If you're not able to identify the server this way, contact your ISP to determine which servers need access permission.

4. After you have identified the server, add it to the Trusted Zone. See "Adding to the Trusted Zone," on page 49 of in the ZoneAlarm™ User Guide.

b. Configuring BP Internet Security™ ZoneAlarm™ software to allow ping messages—If your ISP uses ICMP echo (or ping) messages for connectivity checks, configure Zone Labs security software to allow ping messages from the Internet Zone.

To configure BP Internet Security™ ZoneAlarm™ software to allow ping messages:

1. Select **Firewall/Main**.

2. In the Internet Zone area, click **Custom**.

3. Select check box labeled **Allow incoming ping (ICMP echo).**

4. Click **OK**.

5. Set the security level for the Internet Zone to Medium. See “Choosing security levels” on page 43 of in the ZoneAlarm™ User Guide.

3. Connecting through an ICS client

If you are using the Windows Internet Connection Sharing (ICS) option or a third-party connection-sharing program, and you are unable to connect to the Internet, make sure that BP Internet Security™ ZoneAlarm™ software is properly configured for the client and gateway machines. See “Enabling Internet Connection Sharing” on page 36 of in the ZoneAlarm™ User Guide. Do not configure BP Internet Security™ ZoneAlarm™ software for Internet Connection Sharing if you use hardware such as a server or router, rather than a host PC.

4. Connecting through a proxy server

If you connect to the Internet through a proxy server and you are unable to connect to the Internet, make sure that the IP address of your proxy server is in your Trusted Zone. See “Adding to the Trusted Zone” on page 49 of the ZoneAlarm™ User Guide.

APPENDIX A: Glossary of Internet Security Terms

Ad Blocking—Zone Labs security software feature that enables you to block banner, popup and other types of advertisements.
Adware—A form of spyware. Displays the "pop-up" ads you've seen on your computer. Advertisers use it to generate online revenue and exposure. Adware installs components that gather personal information without informing you that it's doing so.
Animated ad—An advertisement that incorporates moving images.
Anti-spyware—Software that detects, isolates, and eliminates spyware that has been loaded onto your computer without your knowledge.
Banner ad—An ad that appears in a horizontal banner across a Web page.
Broadband—High-speed Internet connection typically offered by cable and phone companies. Without adequate Internet security, broadband users are always at risk of online security threats because their computers are always connected to the Internet.
Cerberian—Cerberian is a software development and application services company that filters, monitors and reports on Internet use and activity. The Web filtering utility in BP Internet Security™ uses Cerberian content categories to determine whether access to websites you visit will be allowed or blocked.
Component—A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.
Cookies—Bits of information secretly stored on your computer allowing others to monitor your Internet activities. This spyware is often used to gather information on your Web-surfing habits to help companies create better marketing strategies. However, many send information to online criminals who would use it to harm you.
Definitions—A definition is the set of fingerprints that characterize a piece of spyware.
Dial-up connection—Connection to the Internet using a modem and an analog telephone line. The modem connects to the Internet by dialing a telephone number at the Internet Service Provider's site. This is in distinction to other connection methods, such as Digital Subscriber Lines, that do not use analog modems and do not dial telephone numbers.
Fingerprints—Fingerprints are the unique patterns of files, cookies, and registry entries that spyware installs.
Firewall—Software that sets up a defense barrier around your computer so that hackers and online criminals cannot access the information on your computer.
Hackers—Individuals with computer and Internet skill levels sufficient enough to break security settings on personal computers and servers over the Internet. Some hackers do it for recreation, others for malicious intent.
Identity theft—Occurs when a criminal obtains and uses another individual's personal information (social security numbers, financial account information, etc.) to take over that individual's identity. The criminal then conducts fraudulent activities in the victim's name.
IP address—The number that identifies your computer on the Internet, as a telephone number identifies your phone on a telephone network. It is a numeric address, usually displayed as four numbers between 0 and 255, separated by periods. For example, 172.16.100.100 could be an IP address. Your IP address may always be the same. However, your Internet Service Provider (ISP) may use Dynamic Host Configuration Protocol (DHCP) to assign your computer a different IP address each time you connect to the Internet.
ISP—Internet Service Provider. An organization that offers Internet access to customers.
Mail Server—The remote computer from which the email program on your computer retrieves email messages sent to you.
Packet—A single unit of network traffic. On "packet-switched" networks like the Internet, outgoing messages are divided into small units, sent and routed to their destinations, then reassembled on the other end. Each packet includes the IP address of the sender, and the destination IP address and port number.
Pass-lock—When the Internet Lock is engaged, programs given pass-lock permission can continue accessing the Internet. Access permission and server permission for all other programs is revoked until the lock is opened.

Persistent cookie—A cookie put on your hard drive by a website you visit. These cookies can be retrieved by the website the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.
Phishing—A hoax where Internet criminals send out false emails in the name of a legitimate organization in order to trick victims into sending personal information back to be used in identity theft crimes.
Ping—A type of ICMP message (formally "ICMP echo") used to determine whether a specific computer is connected to the Internet. A small utility program sends a simple "echo request" message to the destination IP address, and then waits for a response. If a computer at that address receives the message, it sends an "echo" back. Some Internet providers regularly "ping" their customers to see if they are still connected.
Pop-under ad—An ad that appears in a new browser window that opens under the window you're looking at, so you don't see the ad until you close the original browser window.
Pop-up ad—An ad that appears in a new browser window that "pops up" in front of the window you're looking at.
Private network—A home or business Local Area Network (LAN). Private networks are placed in the Trusted Zone by default.
Quarantine—Zone Labs security software's MailSafe quarantines incoming email attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other mailware that hackers distribute as email attachments.
Session cookie—A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their short life span.
Skyscraper ad—An ad that appears in a vertical column along the side of a Web page.
Spam—Unsolicited promotional email.
Spyware—Dangerous software that collects information about your computer activities. It sends that information to others without your knowledge or permission. Once on your computer, spyware installs itself and starts working. It's difficult to detect, and often impossible for average users to remove. Types of spyware include tracking cookies, adware, Trojan Horses, and system monitors.
System monitors—Spyware that observes and captures keystrokes of virtually everything you do on your computer—including passwords, social security numbers, credit card numbers, emails, chat room dialog, websites you've visited, and programs you've run. They usually run unnoticed, storing the information on your computer in a secret file to be retrieved later.
Third party cookie—Persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other third party. These cookies are commonly used to deliver information about your Internet activity to that third party.
Tracking cookies—Tracking cookies are one type of spyware. These are pieces of information that are generated by a web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your web experience, and continue to serve useful purpose in enabling a personalized web experience. However, some websites now issue tracking cookies, which allow multiple websites to store and access cookies that may contain personal information (including surfing habits, user names and passwords, areas of interest, etc.), and then simultaneously share the information it contains with other websites. This sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms. Tracking cookies are almost always installed and accessed without your knowledge or consent.
Trojan horses—Spyware that is often disguised as harmless or even desirable programs, but is actually designed to cause loss or theft of computer data and to destroy your system. They usually arrive as email attachments or bundled with other software. Some give attackers unrestricted access to your computer anytime you're online, allowing file transfers, adding or deleting of files and programs, and taking control of your mouse and keyboard.
Virus—A software program written to disrupt computer systems and to destroy data. Viruses are the most well known Internet security threat.
Web bug—An image file, often 1x1 pixel, designed to monitor visits to the page (or HTML email) containing it. Web bugs are used to find out what advertisements and Web pages you have viewed.
Web filtering—A software tool that allows computer users to determine which Web content they will allow onto your computer through their browser.

Worms—Similar to viruses but much more dangerous. They spread rapidly by accessing your email address book and automatically forwarding themselves to every address it contains. Current anti-virus software can't find worms once they've been loaded onto your system.
Zone Labs—Manufacturer of the ZoneAlarm™ firewall program.