Zone Alarm ForceField User Guide

February 14, 2008

Contents

Contents

Chapter 1

Introducing ZoneAlarm ForceField

ZoneAlarm ForceField is designed to provide you with the most up-to-date, comprehensive defense against rapidly growing Web threats. It helps you visit Web sites without worrying about harm to your PC or being watched, and perform financial transactions without fretting over possible fraud or theft. It also helps you to have maximum protection from identity theft, and provides as much Web surfing privacy as possible.

Topics:

A Quick Look at What ForceField Does

ForceField helps you use the Web without worrying about deception, theft, privacy invasions, and invisible harmful downloads. This section introduces ForceField protection, which incorporates a technology called virtualization.

Several Layers of Protection as You Surf

When you are on the Web with ForceField, it provides:

- Detection of fraudulent sites, spy sites, spyware in downloads, and site security.
- Blocking of stealth keystroke recording and screen picture grabs.
- Protection of your privacy, identity data, credit card numbers, and more.

Virtualization: A Defense Shield

ForceField incorporates ***virtualization*** technology, which does the following for you:

- Creates a temporary, isolated area in which uninvited Web attacks and junk can be safely trapped and deleted without harming or cluttering your PC. In other words, ForceField collects stealth downloads and installations in a virtual file system, which is deleted and is never saved to your real computer drive.
- Has the effect of making the inside of your PC invisible (by encryption) to intruders. This helps prevent your PC from being accessed, watched, or modified while you are using the Web.

When you ***choose*** to download something, it is allowed to pass the virtualization shield and be saved to your PC. For this reason, other ForceField features are designed to detect deceptive sites and block dangerous downloads.

Want to know more? See "Understanding the Threats and Your Protections" on page 12.

ForceField in Conjunction With Traditional Security

Traditional security products, such as ZoneAlarm firewalls, security suites, antivirus, and antispyware products, are made to fight PC-based threats. ZoneAlarm ForceField is made to fight the latest Web-based threats as they develop. Together, traditional security and ForceField provide two critical layers of protection.

In providing complex Web-threat protection, ForceField reduces the dangers that a traditional security suite has to fight, but cannot take its place. For example, ForceField checks for antivirus protection on your computer, but does not find and destroy viruses. And, it uses the latest defenses to detect spysites and prevent downloads of spyware, but if spyware somehow makes its way to your PC, you need a traditional security product eliminate it.

Feedback and Support

We like hearing from you

We want ForceField to be your loyal, easy, "tough-as-nails" security product for the Web. Tell us how to make it better for you! See http://www.zonealarm.com/ to be directed to product feedback links.

And, we want to offer the best possible online Help and User Guides. You can help us by sending your comments to cp_techpub_feedback@checkpoint.com.

Support

To access Customer Support, from the **ZoneAlarm ForceField menu** in the browser toolbar, choose **Settings**. Click **Contact Customer Support**.

You may also find answers you are looking for in one of these places:

- For known issues and workarounds, as well as system requirements, choose **Start** | **All Programs** | **ZoneAlarm ForceField** | **Readme**.
- Check the ForceField forum at http://forums.zonealarm.org/
- Check "Frequently Asked Questions" on page 35

Chapter 2

Understanding the Threats and Your Protections

You may want to know more about what's going on out there, and what ForceField is doing about it. Here, we start with an overview and then get into more detail.

Topics:

Overview of How Your Identity and Data are Protected

This table gives you a synopsis of how ForceField works to secure the safety of your credit card numbers, social security numbers, passwords, and personal information such as address and phone numbers.

ForceField Feature	How it Protects You From Theft	Enabling this feature in ForceField
Instant keylogger and screen grabber jamming	**Blocks programs that secretly record** your screen or your typing in order to collect your personal information. ForceField does not have to scan for and detect keyloggers and screen grabbers. Instead, it blocks the operating system calls that are used by keyloggers and screen grabbers, so there is never a need to worry about whether they will be detected in time.	On by default.
Virtualization and browsing data encryption	**Creates a virtual temporary file system to trap and stop uninvited programs** (known as ***drive-by downloads***) that attempt to track information about you. With encryption, helps make what you type on the Web unreadable to spying mechanisms inside and outside of your PC. See also "Virtualization: A Defense Shield," on page 8.	On by default.
Spy site detection	**Prevents spying mechanisms** from stealing your information. Prevents spyware on your computer from contacting Web sites to exchange information and give out your personal data.	On by default.
Download safety check	**Prevents spying mechanisms** from stealing your information by scanning downloads for spyware. **Prevents malicious software from harming your computer by warning you** if software you download is unsigned. If unsigned, it means the author of the software cannot be determined and there is no guarantee that the software has not been altered.	On by default.
Phishing site detection	**Prevents you from entering valuable data on a fraudulent site** that was designed to steal from you.	On by default.
Web site safety checking	**Warnings alert you** if you surf to a questionable or known dangerous site. Click the **Site Status** button in the ForceField toolbar for details about the security level of any site.	On by default.

ForceField Feature	How it Protects You From Theft	Enabling this feature in ForceField
Privacy Browser mode	**Prevents anyone who uses the same computer from seeing personal information** you typed in online forms and fields.	If others use the computer you are using, you may want to click **Private Browser** in the toolbar ***before*** you bank, shop, or fill out online forms.

Understanding Phishing, Drive-bys, and Other Threats

Web threats are evolving and growing, but with software like ZoneAlarm ForceField you can stay ahead of them.

Protection from Zero Day Threats

A zero day is an attack that takes advantage of security holes for which no solution is yet available. This could be any kind of malicious software (malware) that loads itself onto your computer through hidden code on a Web site, or through email attachments. Zero day threats are typically still unknown and unrecognizable and therefore even antivirus and antispyware scans cannot yet detect them. This is why the ForceField virtualization technology is particularly important. It can shield you from such surprise attacks because it does not need to know the threat in order to stop it. Instead, it automatically catches and deletes stealth Web browser downloads in a safe, virtual data space that acts as your computer's stunt double.

Understanding Phishing, Spy Sites, and Spyware

When ForceField is on, it detects and warns you about known phishing and spy sites.

Phishing sites are fraudulent versions of legitimate sites, and are created to acquire your personal information, such as credit card numbers, for purposes of theft. Phishing is accomplished by sending email or instant messages that masquerade as being from trustworthy sources, such as your bank. These messages have a link to the phishing Web site, which looks just like a Web site you trust. You are instructed to enter your personal information at the phishing site, and this is how your information is stolen.

Spy sites are sites that trick you into downloading software that includes spyware. ***Spyware*** is software that is installed secretly to spy on, or even take partial control over, your computer. The typical motive is theft, including identity theft. In addition to collecting personal information and sending it outside your computer, spyware can also interfere in other ways, such as installing additional programs or monitoring Web-browsing activity for marketing purposes, or redirecting your browser to advertising sites. Spyware can also (unintentionally) affect the performance and speed of your PC. Stability issues, such as application or

computer crashes, are common. Spyware that interferes with networking software commonly causes difficulty connecting to the Internet.

Understanding Drive-by Downloads and Botnets

A couple more growing, important threats ForceField is designed to prevent are drive-by downloads and botnets. The virtualization engine helps shields you from these threats.

Drive-by downloads include any Web-based download to your computer that occurs without your knowledge. This could be spyware, viruses, or other troublesome programs designed to automatically install themselves and steal from you or harm your computer. Drive-by downloads are able to silently get through to your computer by exploiting security holes in Web browsers or operating systems. Drive-by downloads can also happen when you click a Web window in the mistaken belief that it is a harmless message or other type of Web link. Essentially, you can be tricked into initiating the download. The ForceField virtualization technology and spyware scanning systems work to protect you from these unwelcome downloads.

Botnets are used for a variety of purposes, including theft of software serial numbers, login identities, and financial information such as credit card numbers, as well as intentional network performance inhibition (such as denial-of-service attacks) and spam. Botnets are collections of software robots (known as "bots") silently running on invaded computers owned by unsuspecting computer users. The bots can be instructed remotely by the botnet originator, though the bots are designed to act autonomously and propagate themselves using security vulnerabilities that they uncover. Email spammers can purchase access to botnets and send out spam messages via the invaded computers. Because one of the ways that botnets propagate themselves is through drive-by downloads, ForceField is again important for insulating you from this type of invasion.

Dangerous Site and Download Detection

Topics:

How Phishing, Spy Sites, and Spyware are Detected

ForceField detects and protects you from phishing sites in the following ways:

- ForceField tracks a constant "feed" of the most recently discovered phishing sites. If you go to a Web page that is listed as a phishing site, ForceField checks it against the current phishing database and is able to alert you immediately.

- ForceField also uses advanced ***heuristics*** (which look for certain known characteristics of fraudulent sites) to detect phishing sites that were created even seconds before you encountered them.

ForceField detects and protects you from spy sites and spyware in the following ways:

- ForceField receives a constant feed of discovered spy sites, tracked 24 hours a day at our labs. If you go to a Web page that has been reported as a spy site, ForceField alerts you immediately. Your browsing is interrupted by a warning so that you can leave before anything bad happens.
- Similarly, ForceField receives constant updates about known spyware. If you choose to download an executable file harboring known spyware, the antispyware scanner detects it by scanning it against the latest spyware signature database. In addition, ForceField regularly scans your PC memory for spyware.
- The ForceField virtualization technology can trap and delete programs that are silently downloaded to your PC without your permission. These are trapped in a virtual file system so that they are not saved to your real computer hard disk.
- Virtualization also creates an encryption shield around your Web browsing activity, so that if any undiscovered spyware is still lurking on your PC, it will not be able to infiltrate your Web browsing session and see what you are doing and typing.

Unsigned Download Detection

In addition to scanning software downloads for spyware, ForceField also determines whether a software download is digitally signed. Digital signing confirms the software author and that the code has not been altered or corrupted since it was created.

If an executable that you are downloading from the Web is unsigned, ForceField warns you so you can delete it before causes any damage. Note that you do have the option of running an unsigned executable, but this is only recommended if you know and trust the source of the file.

The Web Site Safety Check

As you surf, ForceField checks the credentials each site, along with other details that typically determine how safe a site is. This includes:

- The strength of the site's SSL certificate, and how long the site has been around. Web sites use SSL certificates to secure information you send to the site. Without an SSL certificate, any information you provide could be intercepted and viewed for theft purposes.
- Whether it is a known spyware distributing site.
- Whether it is a known phishing site.

If any of the above information reveals a danger, ForceField alerts you, as described in "Warnings You See at a Risky Site" on page 21.

You can see a security status summary of a Web site you are visiting by clicking the **Site Status** button in the ForceField toolbar.

Note: Some Web sites may have certain pages secured by SSL certificates while other pages on the same site are not secured. As long as the pages you enter your info on are secure, your data is secured. For example, a shopping site home page may not have an SSL certificate, but when you get to the ordering page, **Site Status** reports that the ordering page ***does*** have an SSL certificate. In this case, entering info on the ordering page is considered secure.

How Stealth Actions are Blocked

Some Web sites and Web downloads silently put programs on your computer that record what you type or take pictures of your screen for theft purposes. Some make changes to your computer registry files, and some just download uninvited junk that takes up space.

ForceField blocks the following types of actions:

- ***Keyloggers:*** Keyloggers are invisible Web-based programs that record your keyboard input, and have been used to steal data.Note that keyloggers are sometimes employed for useful tools like language translation or volume control at Web sites. For this reason, if you prefer to have keyloggers blocked only when you type passwords, you can set this in the **Settings** panel. See "ForceField Settings Panel" on page 28.
- ***Screen grabbers:*** ForceField blocks screen grabbers. A ***screen grabber*** is another type of program designed to steal information from you. It silently takes pictures of your screen and retrieves them via the Internet. If you are entering personal data in online Web forms, that information could be captured in the pictures and used for identity theft or other theft.
- ***Uninvited "drive-by" downloads:*** ForceField catches invisible, drive-by downloads and traps them in a virtual file system where they cannot touch your real computer disk. They are deleted when you exit your browser.This provides a strong layer of insulation from malicious programs and junk that attempt to get onto your computer through trickery and security holes.

Chapter 3

ForceField Basics

As soon as you install ForceField and open a new Web browser window, your Web protections are in place.

Topics:

What You See When ForceField is On

ForceField performs much of its work behind the scenes, until it needs to warn you about a danger or let you know the results of a download safety scan.

You know that ForceField is protecting you when you see:

- The ZoneAlarm ForceField standard, short, or privacy toolbar in your Web browser (standard toolbar shown here).

- A brushed white edge around your Web browser (not visible when window is maximized to full screen).
- A ForceField icon in your desktop system tray.

Want to Know More?

For more about the private and default toolbar, see "The Toolbar" on page 27.

To find out about warnings you may see, see "Warnings You See at a Risky Site" on page 21.

Turning ForceField On and Off

Once you have installed ForceField, it's on and protecting you every time you surf the Web, by default.

To turn ForceField off:

- Right-click the ForceField system tray icon, and choose **Exit**.

To turn ForceField back on:

- From the **Start** menu, choose **All Programs** | **ZoneAlarm ForceField**

  The next time you open a Web browser, the ForceField toolbar and browser border appear.

When you need ForceField to be off by default, you can deselect the **Load on Startup** option in the **ForceField menu** | **Settings** | **Preferences** panel. (However, for maximum protection and convenience, it's recommend that you keep the load on startup option enabled so that ForceField is always on.)

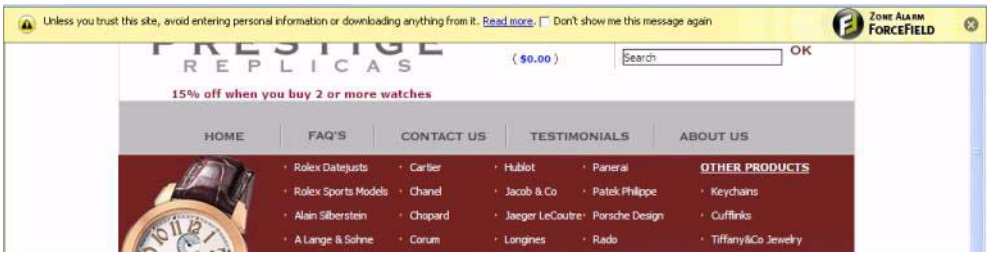
Warnings You See at a Risky Site

If a site is known to be dangerous (a fraudulent site or spyware distributor), the ForceField toolbar turns red and a warning interrupts your browsing. For sites that are questionable and not yet ***known*** to be dangerous, you see a caution message strip under the toolbar.

Yellow Cautions

If you reach a Web site that does not have adequate security credentials, a **Caution** message strip appears under the toolbar.

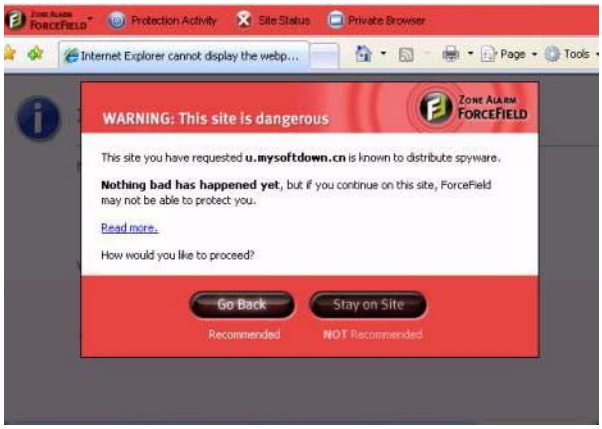
A yellow caution site may not be intentionally malicious. It may be that it is new, or has limited funding, and therefore has not yet obtained a strong security certification (SSL certificate). Nevertheless, the lack of security at the site means that data could be intercepted and used for theft or identity fraud, so avoid entering personal data such as name, address, social security number, or credit card number.



Risk level of Web site	MEDIUM for entering data or downloading files from this site.
Recommendation	With ForceField active, viewing the site should be safe, but **do not enter any personal information or download files at this site.**
Why is the site questionable?	To get more information the site, click the **Site Status** button in the ForceField toolbar.

Red Alerts

If you surf to a site that is known to be dangerous, your surfing is interrupted by a message box that warns you about the site. The ForceField toolbar also turns red.



Risk level of Web site	VERY HIGH
Recommendation	**If this is a phishing site, leave this site** in order to protect your computer, your identity, and your finances. **If this is a spyware distributor site,** ForceField protects you as long as you **do not enter any data or download anything from here**. Click the **Go Back** button in the message to get out safely.
For more about the site	Click the **Site Status** button in the ForceField toolbar.

Want to Know More?

In "Understanding the Threats and Your Protections" on page 12, you can learn more about threats like phishing sites and spyware, and about how ForceField is detecting and blocking behind the scenes.

Protection Activity Statistics

Many threats that ForceField catches are counted and you can view the count by clicking the **Protection Activity** button in the ForceField toolbar. Note that some threats are not counted because nature in which they are blocked precludes the ability to count them.

Included in the Protection Activity window counts

The following are counted:

- phishing sites blocked
- spy sites blocked
- suspicious sites detected
- Web downloads scanned
- spyware found in Web downloads

Not included in the Protection Activity window counts

Certain threats are instantly captured by the virtualization engine or otherwise blocked in a manner than cannot be counted. For this reason, the count you see here does ***not*** include unrequested downloads blocked, keystroke recorders (keyloggers) blocked, and screen picture grabbers blocked.

Want to Know More?

In "Understanding the Threats and Your Protections" on page 12, you can learn more about threats like phishing sites and spyware, and more about how ForceField is detecting and blocking behind the scenes.

Chapter 4

Using Private Browser: Leaving No Trace

Whether you are shopping for gifts for someone that shares your PC, browsing adult sites, or researching private medical concerns, there may be many occasions for keeping your Web activity private. The Private Browser button on the ForceField toolbar opens a special mode of ForceField that prevents others who may use your computer from seeing where you have been and what you have typed.

Topics:

What Happens in Private Browser?

The ForceField Private Browser:

- Erases your tracks, thus preventing anyone that uses your computer from seeing where you have surfed and what you have typed.
- Continues to provide all of the ForceField protections you receive in the default ForceField mode.

See "Which Records are Erased," on page 25 for more information.

Why not use Private Browser all the time?

Convenience is the reason you may not want to use Private Browser all the time. You may prefer the convenience of having Web sites you trust remember you and your shopping cart information (through the use of cookies), or you might appreciate the convenience of auto-completion and auto-fill finishing your typing for you. You may also like to use your History list to get back to a site you were visiting at an earlier time.

Using Private Browser

When you want to keep your Web activity to yourself:

1. Click the **Private Browser** button ***before*** you begin your private surfing.

   A new browser window opens, and the toolbar looks like this:

2. When are done with private browsing and want to return to the default ForceField, just exit the browser.

   The next time you open the browser, it will be in default ForceField mode.

Which Records are Erased

The Private Browser is designed to make sure that any automatic, involuntary records of where you have been are erased, but it preserves a couple records that you may create yourself. This table outlines what is kept and what is erased when you use Private Browser.

Overview of How Private Browser is Different

Normally, whether you are using ForceField or not, browser records of where you have been, such as a history list of sites you visited, are preserved. In Private Browser mode, such records of where you have been are erased.

What is erased from Private Browser session	What remains after Private Browser session
Where you have been: Web browser History list, cookies, Web page caches	Any file or program you chose to download (unless you delete it)

What is erased from Private Browser session	What remains after Private Browser session
Records of what you have downloaded	
What you have typed: auto-complete, auto-fill	

The items listed in the table above are explained in more detail below.

Records of Where You Have Been

The following tracks are erased when you exit Private Browser:

- Lists of sites you visited in Private Browser. Sites you have visited are typically available through a menu item called ***History***. T
- Any ***cookies*** your browser picks up in a Private Browser session. Web sites you visit often install cookies into your browser, and you can see a list of these cookies (which usually includes site names) in your Web browser settings. Cookies are used by sites to recognize you or track what you do on a site. For example, this is how sites save your "shopping cart" contents and account information.
- The ***browser cache*** of your Private Browsing sessions. The browser cache is a temporary storage area of content copied from pages you have visited, which is preserved so that the pages can load quickly the next time you visit.

Records of What You Have Downloaded

Web browsers keep a list of what you have downloaded, which usually pops up each time you download from the Web. What you download while using Private Browser is not recorded in this list.

Records of What You Have Typed

To prevent other users from seeing what you type, auto-completion and auto-fill are turned off when you are in Private Browser mode. ***Auto-completion*** is where your Web browser remembers what you have typed in Search fields and online forms, and completes words when you (or someone else) begin typing the same letters. For example, the person you want to surprise with a ring uses your computer to search for "english translation," and they see "engagement ring" appear as auto-completion of their typing. ***Auto-fill*** is when information you commonly enter in online forms, such as names, passwords, and addresses, is saved by the browser and filled in automatically when you fill out an online form.

Chapter 5

Guide to the ForceField Controls

Topics:

The Toolbar

The ForceField toolbar appears in the top of your Web browser window.

The Default ForceField Toolbar

The Private Browser ForceField Toolbar

The Short Toolbar option

A compact version of the ForceField toolbar is available. To use it, from the **ForceField** menu, choose **Switch to short toolbar**.

You can return to standard toolbar by choosing **Switch to large toolbar** from the ForceField menu.

For more details about these features, see:

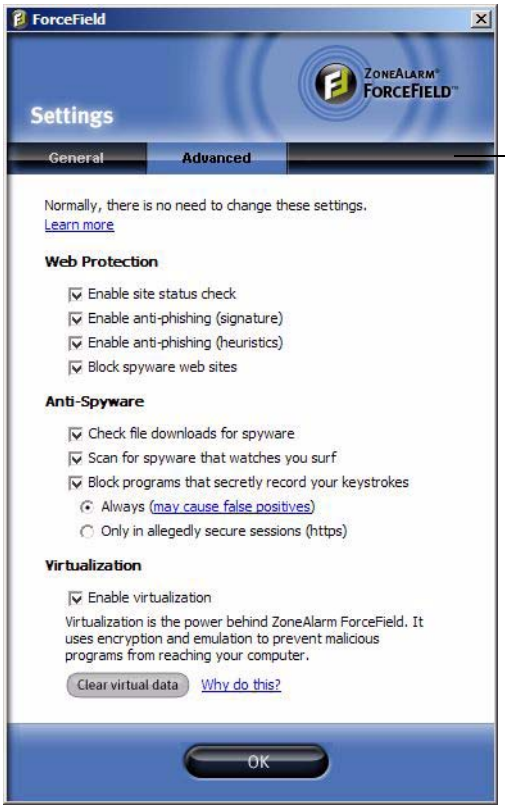
- "Using Private Browser: Leaving No Trace" on page 24
- "Protection Activity Statistics" on page 23
- "The Web Site Safety Check" on page 16

ForceField Settings Panel

The Settings panel lets you control, enable, and disable several ForceField features. You can use the details provided here as a reference in considering the Settings options.

To open the Settings panel, choose **ForceField menu** | **Settings**.

- "General Settings" on page 28
- "Advanced Settings" on page 29



Click buttons to go to General or Advanced settings.

General Settings

Use the following information for considering options in the General Settings tab of the Settings panel.

Updates	Keep this option selected so that your installation of ForceField continues to be automatically (silently) updated with the latest protections and protection technology. The update components include: ■ ***Anti-spyware Scanner:*** This component scans executables you choose to download from a Web page (including from browser-based email) to check for spyware. ■ ***Trust Checker:*** This is the technology that reviews data that determines the trustworthiness of Web sites you visit. ■ ***LTA:*** Lightweight Trust Agent. Checks status of antivirus software. ■ ***ZoneAlarm ForceField Core:*** This component keeps ForceField's core technology up to date. ■ ***Spyware Sites Database:*** This is the component makes sure that ForceField is aware of every spyware site discovered and reported to Internet monitoring services.
Confirmation Messages	To go back to being warned about all questionable or known dangerous sites, click the "**Reset**" link to restore all messages. (If you went to any sites that displayed a **yellow caution** or **red alert**, and then clicked a link to indicate that you trust the site, ForceField remembers that you consider the site safe and no longer warns you about it.)
Startup	Select this option if you want ForceField to be running every time you startup your computer. If you prefer to have ForceField off by default, then deselect this option.
Support	Click the link to find out how to contact product support.

Advanced Settings

For helpful information about when you might want to disable a setting on this panel, see "Settings for Troubleshooting" on page 32.

Web Protection Settings

Enable site status check	Checks security-related information about each site you visit.
Enable anti-phishing (signature)	At each site you visit, ForceField checks an online anti-phishing signature database to see if the site has been reported as a phishing site.
Enable anti-phishing (heuristics)	ForceField analyzes each site you visit for phishing characteristics.
Block spyware web sites	Protects you from sites that distribute spyware to your computer, either silently or by embedding spyware in downloads that appear to be trustworthy.

Anti-Spyware Settings

Check downloaded files for spyware	Executable downloads (programs) are thoroughly checked for spyware. If you have another form of download checking that includes the latest spyware detection, you might simplify downloads by unchecking these options or by disabling the other download detection.
Scan for spyware that watches you surf	Scans your computer's memory space for spyware when ForceField is running.
Block programs that secretly record your keystrokes	For maximum protection of data you enter online, choose **Always**. However, this setting may block the occasional safe program that uses keylogging, such as language translation sites, Web-based volume control, online conferencing, or child monitoring programs. If you have conflicts using any of those programs, use **Only in alledgedly secure sessions (https).** This way you will still be protected when entering important data on secure sites.

Virtualization Settings

Virtualization	Keep virtualization enabled to maximize your protection with encryption and keep the safe, temporary "net" that catches drive-by downloads. For a description of virtualization, see "Virtualization: A Defense Shield" on page 8.
Clear virtual data	Deletes all unsolicited downloads caught in the ForceField protective virtual file system. Also deletes browser download history list, history list of sites visited, form and search history saved by browser, browser cache, cookies, and passwords saved by browser.

Chapter 6

Troubleshooting and Customizing

If you need to troubleshoot possible conflicts between ForceField and other applications, or want to adjust certain behavior, go to the ForceField Settings panel.

Topics:

Settings for Troubleshooting

For maximum protection, all options in the **Advanced Settings** panel of the **Settings** window are on by default. Choose **ForceField menu** | **Settings** from the ForceField toolbar.

Because some programs could conflict with the features associated with these settings, you may at times want to turn a setting off, as described below.

With ForceField on, if you have trouble with...	Try this
Child monitoring programs	In the **Advanced Settings** panel, make sure that **Anti-Spyware**	**Block programs that secretly record your keystrokes** is deselected while using child monitoring programs.
Failed installation of browser features, toolbars, or other downloaded programs Web browser add-on toolbars disappearing	Can occur because, in order to prevent drive-by downloads, ForceField blocks ActiveX installations that it does not yet recognize. In the **Advanced Settings** panel, disable **Virtualization**	**Enable Virtualization** before installing the feature or program. Be sure to turn virtualization back on after installation.

With ForceField on, if you have trouble with...	Try this
Online conference programs (e.g., Webex)	In the **Advanced Settings** panel, make sure that **Anti-Spyware**	**Block programs that secretly record your keystrokes** while using the online conferencing program.
Language translation sites	In the **Advanced Settings** panel, make sure that **Anti-Spyware**	**Block programs that secretly record your keystrokes** is deselected when you visit these sites.
Volume controls on Web sites	In the **Advanced Settings** panel, make sure that **Anti-Spyware**	**Block programs that secretly record your keystrokes** is deselected when using these volume controls.
Multiple different spyware scans appearing when you download files from a Web site.	In the **Advanced Settings** panel, deselect **Anti-Spyware**	**Check file downloads for spyware.** **Important:** Do this only if you are confident that you have another adequate spyware scanner running on all Web sites. Many Web email programs scan email downloads, but you may still need Web site downloads scanned by ForceField.

Did this solve your problem? If not:

- Check the Readme for known issues and workarounds in this release. Choose **Start** | **All Programs** | **ZoneAlarm ForceField** | **Readme**.
- Check "Frequently Asked Questions" on page 35.
- Check, or post to, the ForceField forum at http://forums.zonealarm.org/.
- To access Customer Support, from the **ZoneAlarm ForceField menu** in the browser toolbar, choose **Settings**. Click **Contact Customer Support**.

Customizing Settings

Examples of configurations you may want to alter in the **Settings** panel include:

- **General | Startup setting:** You can control whether ForceField starts automatically when you start up your computer. (By default, it starts automatically.)
- **General | Messages settings:** You can restore all warning and caution messages about sites you have visited. In case, for example, you or someone else who uses your computer may have accidentally indicated trust in a site you now prefer to be warned about.
- **Advanced Settings** to solve problems that may arise from software conflicts, as described in "Settings for Troubleshooting" on page 32.

To customize your ForceField settings:

1. Choose **ForceField menu** | **Settings** from the ForceField toolbar or system tray icon.
2. In the **Settings** panel that appears, select and deselect options according to your preferences.

   Refer to "ForceField Settings Panel" on page 28 for information about these settings.

Chapter 7

Frequently Asked Questions

Questions about interactions with other products

Other questions about ForceField

Have another question or problem?

- See also "Settings for Troubleshooting" on page 32, especially for help with possible conflicts between ForceField and third-party products.
- For known issues and workarounds, see the **Readme**, available from the ZoneAlarm ForceField start menu.
- Try checking, or posting to, the ForceField forum at http://forums.zonealarm.org/
- To access Customer Support, from the **ZoneAlarm ForceField menu** in the browser toolbar, choose **Settings**. Click **Contact Customer Support**.

Questions about interaction with other products

- "What happens when I use IM or email within my Web browser?" on page 36
- "Does ForceField let me install a browser plug-in or PDF reader?" on page 36

See also "Settings for Troubleshooting" on page 32 for help resolving conflicts between ForceField and third-party products.

Do ForceField settings override ZoneAlarm or Web browser settings?

It depends on whether or not you are using Private Browser. In standard mode, ForceField is designed to allow previous browser or ZoneAlarm *customizations* you made to remain as configured. For example, if you have configured your browser to stop saving a site History list, ForceField does not change that setting.

Private Browser mode can override some settings. Regardless of any prior browser or ZoneAlarm settings, when you exit Private Browser, the following records of your browsing session are erased:

- Web browser History list, cookies, Web page caches
- Records of what you have downloaded (download list)
- auto-complete, auto-fill

What happens when I use IM or email within my Web browser?

Use instant messaging and email programs within your Web browser as you always have.

IM	All of your sent and received messages are preserved in the way they usually are preserved.
EMAIL	All of your sent and received messages are preserved in the way they usually are preserved. Anything you choose to download from email can be saved to your PC. ForceField performs a download safety check on the file, which alerts you if the file appears to contain spyware or is unsigned, at which time you can choose not to save it.

Does ForceField let me install a browser plug-in or PDF reader?

In the virtual file system, ForceField catches programs that attempt to install themselves in your Web browser without your permission. But, sometimes you may want to install a toolbar and it will install silently and thus appear to be uninvited. In this case, ForceField may treat it like a drive-by download and block it.

This can happen with an ActiveX program or a PDF reader. ForceField recognizes and allows many common ActiveX programs, such as most search engine toolbar installations, but is not aware of all safe ActiveX programs.

To install plug-ins such as special toolbars in your Web browser, turn ForceField off temporarily, and turn it back on after you install the plug-in. You can refer to "Turning ForceField On and Off," on page 20.

Other questions about ForceField

What does ForceField add to the protection of other ZoneAlarm products?

ForceField adds the following critical Web protections to ZoneAlarm security software:

- Only ForceField can stop "zero day" drive-by downloads, which are not yet discovered by antivirus and antispyware databases and have no known solution.
- Warns you when you go to sites that do not have adequate security credentials.
- Detects known and unknown phishing Web sites. Checks sites against up-to-date database of known phishing sites. Can detect unknown phishing sites created only seconds ago with heuristics (detecting characteristics of phishing).
- Uses encryption to make what you type on the Web unreadable to any spyware hiding on your system.
- Privacy Browser option lets you choose to leave no trace on your computer of what you've typed or where you've been.
- Blocks the system calls that keylogger and screen grabber programs use to secretly record your keystrokes or onscreen activity. This eliminates the risk of waiting for scan that might not find them.

See also "ForceField in Conjunction With Traditional Security" on page 9 for more about the important role of both types of security.

Does ForceField hide my IP address?

No, ForceField does not affect the visibility of your network IP address.

Does ForceField protect me from spyware and viruses?

In a nutshell: ForceField defends you against the latest ways that spyware and viruses are passed on the Web, and it detects spyware in downloads, but it does not destroy viruses and spyware. It is intended to be used in conjunction with antispyware-antivirus programs that destroy viruses and spyware.

Viruses: ForceField greatly reduces the amount of malicious software that can get onto your computer through Web sites and stealth downloads. But, if a virus does hit your computer, either through email or another route, a traditional antivirus program is needed because ForceField does not remove viruses.

Spyware: ForceField should be used with a traditional antispyware program, as it does not destroy spyware. ForceField provides many layers to help you avoid spyware, from spyware

scans to spy site detection, and is constantly updated by the latest spy site and spyware signature databases.

For more information about exactly how ForceField protects and detects, see “Dangerous Site and Download Detection” on page 15.

Does ForceField let me keep files I download?

Yes, anything you choose to download can be saved to your computer. You will be warned if ForceField detects known spyware in a program you download, or if it finds the executable is unsigned. The choice is entirely up to you. See “Unsigned Download Detection” on page 16 for more information.

The files that ForceField blocks are the drive-by ones that you did not initiate.

Does the Private Browser include the same protections as default ForceField?

Yes, the Private Browser does provide all of the Web protection provided by the default ForceField. It just adds privacy to those features.

Note that convenience is the reason you may not want to use Private Browser all the time. You may prefer the convenience of having Web sites you trust remember you and your shopping cart information (through the use of cookies), or you might appreciate the convenience of auto-completion and auto-fill finishing your typing for you. You may also like to use your History list to get back to a site you were visiting at an earlier time.

Index

T

U

V

W

Y

Z