ZoneAlarm ForceField User Guide

ZoneAlarm® ForceField™

April 11, 2008

Contents

Chapter 1 **Introducing ZoneAlarm ForceField**

A Quick Look at What ForceField Does 8
ForceField in Conjunction With Traditional Security 9
Feedback and Support 9

Chapter 2 **Understanding the Threats and Your Protections**

Overview of How Your Identity and Data are Protected 11
Understanding Phishing, Drive-bys, and Other Threats 13
Protection from Zero Day Threats 13
Understanding Phishing, Spy Sites, and Spyware 13
Understanding Drive-by Downloads and Botnets 13
Dangerous Site and Download Detection 14
How Phishing, Spy Sites, and Spyware are Detected 14
Unsigned Download Detection 15
The Web Site Safety Check 15
How Stealth Actions are Blocked 16

Chapter 3 **ForceField Basics**

What You See When ForceField is On 18
Turning ForceField On and Off 18
Warnings You See at a Risky Site 19
Yellow Caution Banner 19
Red “Might be Phishing” Warning 20
Red Warning Alerts 21
Protection Activity Statistics 22

Chapter 4 **Using Private Browser: Leaving No Trace**

What Happens in Private Browser? 23
Using Private Browser 24
Which Records are Erased 24

Chapter 5 **Guide to the ForceField Controls**

The Toolbar 26
ForceField Settings Panel 27
General Settings 27
Advanced Settings 28

Chapter 6 **Troubleshooting and Customizing**

Troubleshooting Interference with Other Programs 31

Customizing Settings 32

Chapter 7 **Frequently Asked Questions**

Questions about interaction with other products 35

Other questions about ForceField 36

Index 38

Chapter 1

Introducing ZoneAlarm ForceField

ZoneAlarm ForceField by CheckPoint 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 increases protection from identity theft, and provides as much Web surfing privacy as possible.

Topics:

- "A Quick Look at What ForceField Does" on page 8
- "ForceField in Conjunction With Traditional Security" on page 9
- "Feedback and Support" on page 9

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.

ForceField shields you on the Web by:

✓ **Detecting** dangerous sites and downloads.

✓ **Blocking** stealth keyboard recording and pictures of your screen.

✓ **Protecting** your privacy and valuable info.

Virtualization: A Defense Shield

ForceField incorporates ***virtualization*** technology, which creates a temporary, isolated area in which stealth attacks and junk are trapped and deleted without harming or cluttering your PC.

For example, ***drive-by download*** spyware can be automatically and silently downloaded to your PC. Even well-known Web sites have been mugged by drive-by download criminals. With its virtualization technology, ForceField catches and deletes these drive-bys so they never make it to your real PC.

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 more detail about ForceField protections?

- "Understanding the Threats and Your Protections" on page 11
- "What does ForceField add to the protection of other ZoneAlarm products?" on page 36
- "Using Private Browser: Leaving No Trace" on page 23.

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. 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.

See also “What does ForceField add to the protection of other ZoneAlarm products?” on page 36.

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/forcefield 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 Product 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 34

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" on page 11
- "Understanding Phishing, Drive-bys, and Other Threats" on page 13
- "Dangerous Site and Download Detection" on page 14
- "How Stealth Actions are Blocked" on page 16

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 no need to worry whether they will be detected in time.	On by default.
Virtualization	**Creates a virtual temporary file system to trap and stop uninvited programs** (known as ***drive-by downloads***) that attempt to track information about you. See "Understanding Drive-by Downloads and Botnets" on page 13. See also "Virtualization: A Defense Shield," on page 8.	On by default.
Spy site detection	**Prevents spying mechanisms** and sites that distribute spyware from stealing your information.	On by default.
Download safety check	**Prevents spying** by scanning downloads for spyware. **Prevents criminal 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.
Privacy Browser mode	**Prevents anyone who uses the same computer from seeing personal information** you typed in online forms and fields.	Click **Private Browser** in the toolbar ***before*** you start surfing.

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, created to acquire your personal data in order to steal from you. 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. Even well-known Web sites have been mugged by drive-by download criminals. Drive-by downloads get through to your computer by exploiting security holes in Web browsers or operating systems.They can also happen when you click somewhere 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. With the virtualization net, ForceField catches and deletes drive-bys so they never make it to your real PC.

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" on page 14
- "Unsigned Download Detection" on page 15
- "The Web Site Safety Check" on page 15

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.

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.

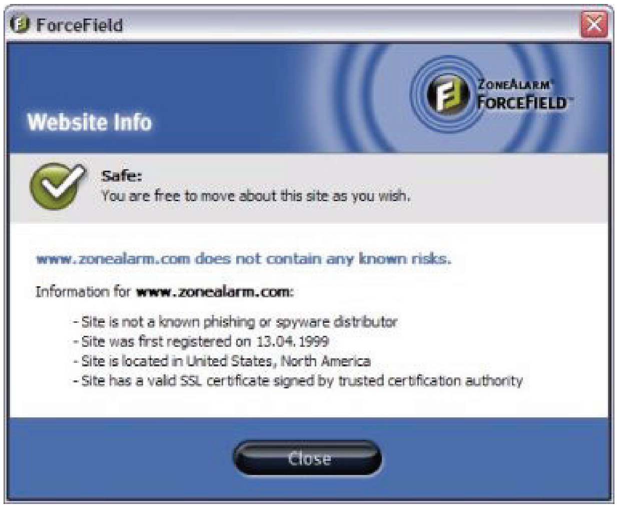
The Web Site Safety Check

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. 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.
- How long the site has been around.
- Whether it is a known spyware distributing site.
- Where the Web site is hosted.
- 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 19.

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



Safe:
You are free to move about this site as you wish.

www.zonealarm.com does not contain any known risks.

Information for **www.zonealarm.com**:

- Site is not a known phishing or spyware distributor
- Site was first registered on 13.04.1999
- Site is located in United States, North America
- Site has a valid SSL certificate signed by trusted certification authority

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 stealth actions by blocking the following:

- ***Keyloggers:*** ForceField blocks keyloggers by turning off the system calls that make keylogging possible. Keyloggers are silent 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 are completing a secure "https" Web transaction, such as at a secure banking or shopping site, you can set this in the **Settings** panel. See "ForceField Settings Panel" on page 27.
- ***Screen grabbers:*** ForceField turns off screen grabber system calls so that screen grabbers produce only blank screen shots. 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 neutralizes them in a virtual file system where they cannot touch your real computer disk. 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" on page 18
- "Turning ForceField On and Off" on page 18
- "Warnings You See at a Risky Site" on page 19
- "Protection Activity Statistics" on page 22

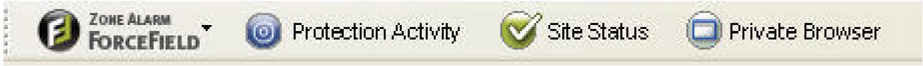
Want to know more about ForceField? See "A Quick Look at What ForceField Does" on page 8 and "Understanding the Threats and Your Protections" on page 11.

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 your Web browser when you see:

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



- A brushed white edge around your 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 26.

To find out about warnings you may see and what to do, see "Warnings You See at a Risky Site" on page 19.

Turning ForceField On and Off

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

Occasionally you may find a Web site that you trust seems to have a conflict with ForceField. The site may use programs that ForceField protects you from, even though those programs are used in a safe way. One convenient option is to try opening the site in an unprotected browser while leaving ForceField on. (If this does not help, see "Troubleshooting Interference with Other Programs" on page 31.)

To open an unprotected browser window while ForceField is on:

- Choose **Open Unprotected Browser** from the ForceField system tray shortcut menu.

  Remember that this unprotected browser window is not protected by ForceField! Only use it for sites that you completely trust.

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 browser window, the ForceField toolbar and browser border appear and you know you are protected.

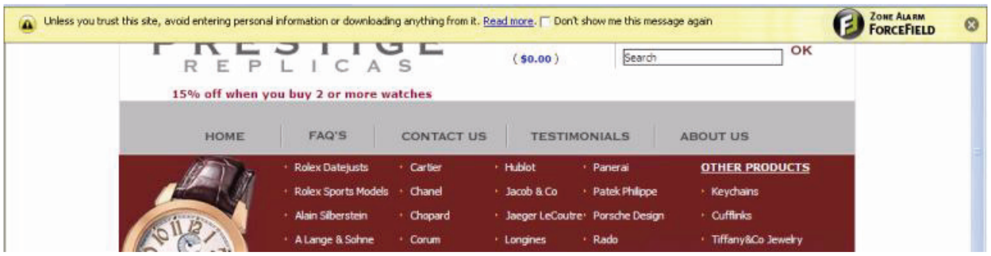
When you want ForceField to be off by default, you can deselect the **Startup** option in the **ForceField menu** | **Settings** | **Preferences** panel. However, for maximum protection keep the Startup option selected so that ForceField is always on.

Warnings You See at a Risky Site

If a site is known to be a phishing site or spyware distributor, the ForceField toolbar turns red and a warning interrupts your browsing. At sites that are questionable but not yet proven dangerous, you see a caution message strip under the toolbar.

Yellow Caution Banner

If you reach a Web site that does not have adequate security credentials, a yellow caution message appears under the toolbar. This 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.



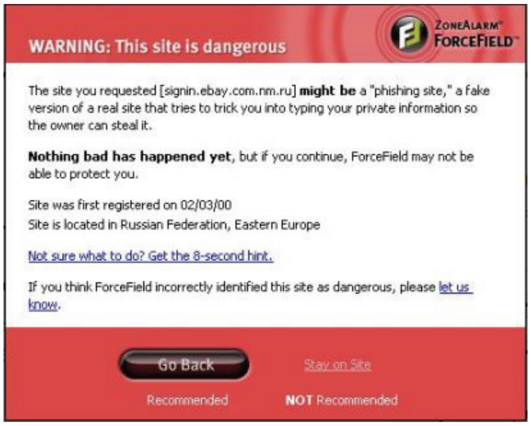
Unless you trust this site, avoid entering personal information or downloading anything from it. Read more. □ Don't show me this message again

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 about the site, click the **Site Status** button in the ForceField toolbar.

Red “Might be Phishing” Warning

If you reach a Web site where ForceField detects characteristics associated with phishing, your surfing is interrupted by a red “**might be** a phishing site.” message. This means that ForceField’s heuristic detection has found some characteristics common to phishing, but the site has not been officially reported as a phishing site. It could be a new, not-yet-discovered phishing site. Or, it could be safe.

See the **Recommendations** below for a list of questions that help you decide whether to trust this site or not.



WARNING: This site is dangerous

The site you requested [signin.ebay.com.nm.ru] **might be** a "phishing site," a fake version of a real site that tries to trick you into typing your private information so the owner can steal it.

Nothing bad has happened yet, but if you continue, ForceField may not be able to protect you.

Site was first registered on 02/03/00
Site is located in Russian Federation, Eastern Europe

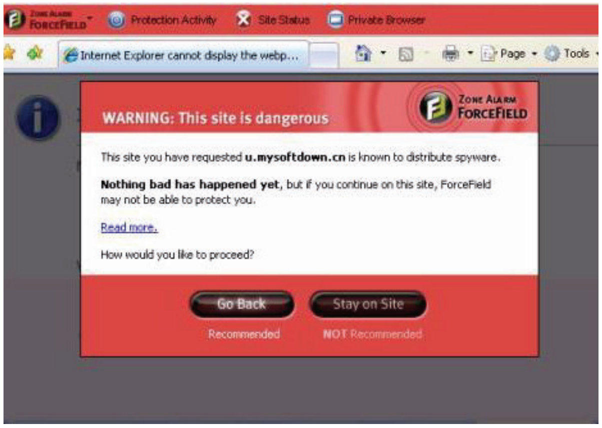
Not sure what to do? Get the 8-second hint.

If you think ForceField incorrectly identified this site as dangerous, please let us know.

Risk level of Web site	MEDIUM to HIGH for entering data or downloading files from this site.
Recommendations	The site ***may not*** be a phishing site, but we recommend you click **Go Back** if any of the following are true: Did you get to this site by clicking a link in an email? Does the address start with “http” instead of “https”? Sites that ask for personal data should be secured by extra encryption and authentication, indicated by https. Is there a slight misspelling in the site address, such as “yahooo” instead of “yahoo”? Does **Site Status** indicate that the site creation date is very recent or that the site is hosted in an unexpected country?
Why is the site questionable?	Heuristic detection has found some characteristics common to phishing, but the site is not officially reported as a phishing site at this time.

Red Warning 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.



WARNING: This site is dangerous

This site you have requested **u.mysoftdown.cn** is known to distribute spyware.

Nothing bad has happened yet, but if you continue on this site, ForceField may not be able to protect you.

Read more.

How would you like to proceed?

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 11, 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 the nature in which they are blocked precludes the ability to count them.

Included in the “ForceField at Work for You” window counts	Not included in the “ForceField at Work for You” counts
The following are counted: ■ phishing sites blocked ■ spy sites blocked ■ suspicious sites detected ■ Web downloads scanned ■ spyware found in Web downloads ■ MB of possibly dangerous data prevented from reaching your PC	Certain threats are captured by the virtualization engine or otherwise blocked in a manner than cannot be counted. For this reason, the count you see does ***not*** include: ■ unrequested downloads blocked ■ keystroke recorders (keyloggers) blocked ■ screen picture grabbers blocked

Want to know more?

In “Understanding the Threats and Your Protections” on page 11, 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 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?" on page 23
- "Using Private Browser" on page 24
- "Which Records are Erased" on page 24

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 24 for more information.

Why not use Private Browser all the time?

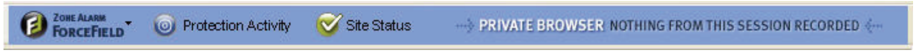
Convenience is the reason you may not want to use Private Browser all the time. You may prefer the convenience of having Web sites you trust remember you and your shopping cart information (through the use of cookies), or you might appreciate the convenience of auto-completion and auto-fill finishing 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, with the Private Browser toolbar.



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, Bookmarks/ Favorites	Any file or program you choose 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, stored passwords	

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***.
- 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.
- Any ***Bookmark or Favorite*** you created in your browser Bookmarks or Favorites list.

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.

Also, some people configure their Web browser to **store passwords** automatically. Any passwords that become stored while you are in Private Browser are deleted when you exit Private Browser.

Chapter 5

Guide to the ForceField Controls

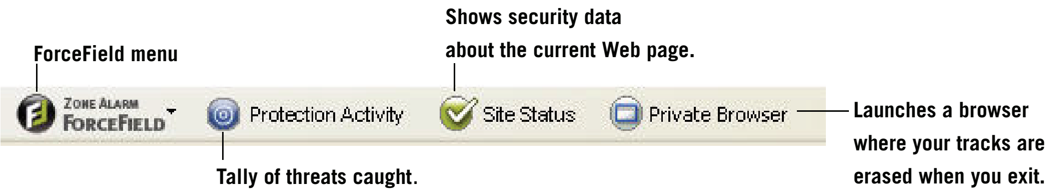
Topics:

- "The Toolbar" on page 26
- "ForceField Settings Panel" on page 27

The Toolbar

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

The Default ForceField Toolbar



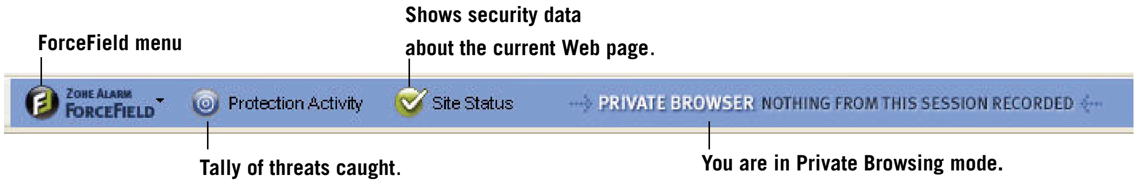
ForceField menu

Shows security data about the current Web page.

Launches a browser where your tracks are erased when you exit.

Tally of threats caught.

The Private Browser ForceField Toolbar



ForceField menu

Shows security data about the current Web page.

Tally of threats caught.

You are in Private Browsing mode.

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:

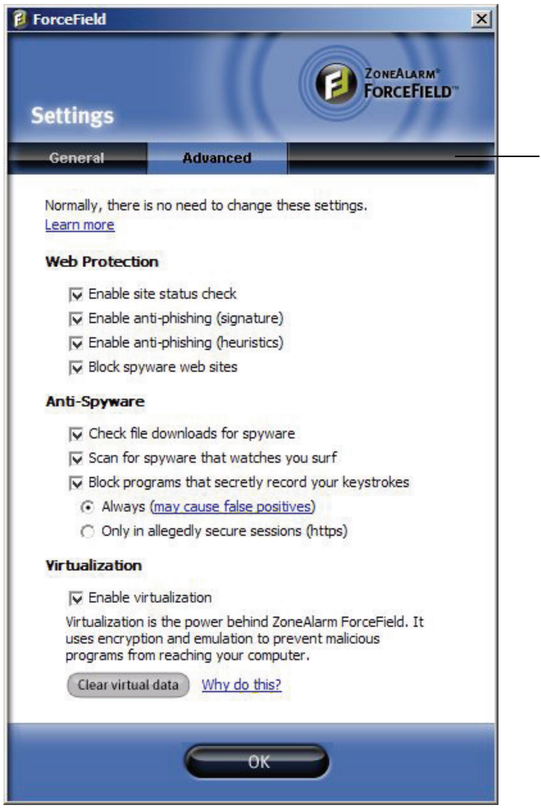
- "Using Private Browser: Leaving No Trace" on page 23
- "Protection Activity Statistics" on page 22
- "The Web Site Safety Check" on page 15

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 27
- "Advanced Settings" on page 28



Normally, there is no need to change these settings.
Learn more

Web Protection

☑ Enable site status check
☑ Enable anti-phishing (signature)
☑ Enable anti-phishing (heuristics)
☑ Block spyware web sites

Anti-Spyware

☑ Check file downloads for spyware
☑ Scan for spyware that watches you surf
☑ Block programs that secretly record your keystrokes
● Always (may cause false positives)
○ Only in allegedly secure sessions (https)

Virtualization

☑ Enable virtualization

Virtualization is the power behind ZoneAlarm ForceField. It uses encryption and emulation to prevent malicious programs from reaching your computer.

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. ***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 "Troubleshooting Interference with Other Programs" on page 31.

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, so it can catch even new sites that haven't been reported yet.

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 legitimate program that uses keylogging, such as language translation programs, volume control, online conferencing, or child monitoring programs. If you have conflicts using any of those programs, use **Only in allegedly 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 and browser cache.

Chapter 6

Troubleshooting and Customizing

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

Topics:

- "Troubleshooting Interference with Other Programs" on page 31
- "Customizing Settings" on page 32

Troubleshooting Interference with Other Programs

For maximum protection, all options on the **Advanced Settings** panel are on by default. Because some programs could conflict with these features, you may at times want to turn a setting off.

To access the Advanced Settings window:
Choose **ForceField menu** | **Settings** from the ForceField toolbar, and then click **Advanced**.

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 programs and toolbars Disappearing browser toolbars	In the **Advanced Settings** panel, disable **Virtualization | Enable Virtualization** before installing the feature or program. Be sure to turn virtualization back on after installation. (To prevent drive-by downloads, ForceField blocks ActiveX installations that it does not yet recognize.)

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** is deselected while using the online conferencing program.
Language translation programs	In the **Advanced Settings** panel, make sure that **Anti-Spyware | Block programs that secretly record your keystrokes** is deselected when using the language translation.
Volume controls on Web sites or other programs	In the **Advanced Settings** panel, make sure that **Anti-Spyware | Block programs that secretly record your keystrokes** is deselected when using these volume controls.
Taking screen snapshots	In the **Advanced Settings** panel, make sure that **Anti-Spyware | Block programs that secretly record your keystrokes** is deselected when taking screen shots. (This setting includes screen grabber blocking.)
A technical support professional is unable to use a program they need to view your computer remotely	Because tech support programs may include keylogging technology, either turn off ForceField or deselect **Advanced Settings** | **Anti-Spyware | Block programs that secretly record your keystrokes** while allowing tech support access.

Did this solve your problem? If not:

- If the trouble you have is at a particular Web site you trust, try using that site without ForceField, by choosing **Open Unprotected Browser** from the ForceField system tray shortcut menu.
- Check the Readme for known issues and workarounds in this release. Choose **Start** | **All Programs** | **ZoneAlarm ForceField** | **Readme**.
- Check “Frequently Asked Questions” on page 34.
- 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 Product 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. Use this if you or someone else may have trusted a site you now prefer to be warned about.
- **Advanced Settings** to solve problems that may arise from software conflicts, as described in "Troubleshooting Interference with Other Programs" on page 31.

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 27 for information about these settings.

Chapter 7

Frequently Asked Questions

Questions about interactions with other products

- "Do ForceField settings override ZoneAlarm or Web browser settings?" on page 35
- "What happens when I use IM or email within my Web browser?" on page 35
- "Does ForceField let me install a browser plug-in or PDF reader?" on page 35

Is there another program or site you are having trouble with? See "Troubleshooting Interference with Other Programs" on page 31 to resolve other program interference issues.

Other questions about ForceField

- "What does ForceField add to the protection of other ZoneAlarm products?" on page 36
- "Does ForceField hide my IP address?" on page 36
- "Does ForceField protect me from spyware and viruses?" on page 36
- "Does ForceField let me keep files I download?" on page 37
- "Does the Private Browser include the same protections as default ForceField?" on page 37

Have another question or problem?

- 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 Product Support**.

Questions about interaction with other products

- "Do ForceField settings override ZoneAlarm or Web browser settings?" on page 35
- "What happens when I use IM or email within my Web browser?" on page 35
- "Does ForceField let me install a browser plug-in or PDF reader?" on page 35

Is there another program or site you are having trouble with? See "Troubleshooting Interference with Other Programs" on page 31 to resolve other program interference issues.

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, Bookmarks or Favorites
- Records of what you have downloaded (download list)
- auto-complete, auto-fill, browser-stored passwords

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?

ForceField catches, in its virtual file system, 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 common search engine toolbars, but is not aware of all safe ActiveX programs. To install less common plug-ins in your Web browser: Turn ForceField off temporarily, and turn it back on after you install the plug-in. See "Turning ForceField On and Off," on page 18.

Other questions about ForceField

- "What does ForceField add to the protection of other ZoneAlarm products?" on page 36
- "Does ForceField hide my IP address?" on page 36
- "Does ForceField protect me from spyware and viruses?" on page 36
- "Does ForceField let me keep files I download?" on page 37
- "Does the Private Browser include the same protections as default ForceField?" on page 37

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

If you have ZoneAlarm, why do you need ForceField? ForceField does a number of key things that ZoneAlarm alone does not do:

- ForceField can stop "zero day" drive-by downloads, which are not yet discovered by antivirus and antispyware databases and have no known solution.
- ForceField warns you when you go to sites that do not have adequate security credentials.
- ForceField 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).
- ForceField includes the Privacy Browser option so you can choose to leave no trace on your computer of what you've typed or where you've been.
- ForceField 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 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 to your PC from 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 14.

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 15 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

A

ActiveX, blocking 35
ActiveX, trouble with 31
Adobe Acrobat reader 35
Advanced Settings panel 28
Advanced Settings, when to change 28
Anti-Spyware Settings 29
antivirus 36
auto-completion 24, 25
auto-fill 25

B

Botnets 14

C

Child monitoring programs, troubleshooting 31
Cookies 25

D

dangerous sites, detection 14
Drive-by downloads 13
drive-by downloads 12

E

email 35

H

heuristics 14
History 25

I

Identity protection 11
interaction with other products 35

K

keyloggers 16

L

Language translation sites, trouble with 32

M

Messages 28
might be phishing, warning 20

O

Online conference programs 32
Open Unprotected Browser 18

P

PDF reader 35
phishing, defined 13
phishing, signs of 20
Private Browser 23
Private Browser, differences from standard 24
Private Browser, using 24
Private Browser, what happens in 23
Private Browser, when not to use 24
Protection Activity statistics 22

R

records erased versus saved 24
red alerts 21

S

screen grabbers 16
Settings panel 27
spy site, defined 13
spyware protection 36

spyware, defined 13
SSL certificate 15, 16
Startup 28
stealth actions, blocking of 16

T

toolbar installations disappearing 31
Toolbar, ForceField 26
toolbars, installing 35

U

Updates 28

V

virtualization 8
Virtualization Settings 29
viruses 36
Volume controls, trouble with 32

W

Web Protection settings 28
Web Site Info window 15
Webex 32

Y

yellow warnings 19

Z

Zero Day threats 13