Simple Computer Security

Disinfect Your PC

CA

with Eric Geier and Jim Geier

Wiley Publishing, Inc.

Simple Computer Security

Simple Computer Security

Disinfect Your PC

CA

with Eric Geier and Jim Geier

Wiley Publishing, Inc.

Simple Computer Security: Disinfect Your PC

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-0-470-06854-0

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1B/QT/QR/QX/IN

Credits

Executive Editor
Carol Long

Senior Development Editor
Tom Dinse

Production Editor
Angela Smith

Copy Editor
Kathryn Duggan

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Joseph B. Wikert

Project Coordinator
Jennifer Theriot

Graphics and Production Specialists
Carrie Foster
Brooke Graczyk
Denny Hager
Jennifer Mayberry
Barbara Moore

Quality Control Technicians
Laura Albert
Jessica Kramer

Proofreading and Indexing
Techbooks
Estalita Slivoskey

Anniversary Logo Design
Richard Pacifico

Acknowledgments

CA would like to thank all of the people who have contributed their technical, editorial, administrative, and/or creative expertise to the making of its first series of CA Simple computer solution books.

Laural Gentry

Diana Gruhn

Lawrence Guerin

Mark Haswell

Robyn Herbert

Christopher Hickey

George Kafkarkou

David Luft

Gary McGuire

Stefana Ribaudo-Muller

Contents

Introduction

This book discusses the primary issues and threats that face all computer and Internet users. Not only does it describe the symptoms, prevalence, and affects of the most common computer security problems, it also provides simple solutions so you and your family will have a safe and pleasant online and computing experience.

The explanations, statistics, and real-world stories in this book ensure that you are informed about the facts when you're dealing with Internet issues. And the included Internet security software and the step-by-step instructions will keep you properly protected.

How This Book Is Organized

This book is organized in a simple manner, which can be summed up as follows:

- First you learn about the problems facing computer and Internet users.
- Then you learn about the solutions to combat those problems.
- Next you'll prepare to implement the solutions.
- Finally the book will help you properly employ the solutions with step-by-step instructions, illustrations, and tips.

Part I: Understand the Threats and Solutions

The chapters in this part explain the main online and computing threats, and discuss solutions that can be implemented to combat them.

Chapter 1: Viruses, Spyware, and Other Malware Infections

This chapter helps you learn about the different types of viruses and infections—such as worms, spyware, and malware—that can plague your computer and destroy your files. It discusses their symptoms and prevalence, and how they can affect your PC data and overall computing experience.

Chapter 2: Spam, PC Intrusion, and Inappropriate Content

This chapter covers a few issues relating to Internet use, such as spam, intruders, and inappropriate online content. The information about these items that the chapter provides can help you protect yourself and your family while online.

Chapter 3: Solutions to Online Threats

This chapter helps you fight online threats by discussing simple solutions to protect your data, identity, and family. It provides ways to prevent the issues from arising and to protect yourself from unforeseeable threats.

Part II: Detect and Eliminate Threats

The chapters in this part explain how to install, set up, and use two pieces of software that will protect you from the main online and computing threats discussed in Part I of this book. In addition, you'll also learn how to keep your software up-to-date to ensure that you're properly protected from the latest threats.

Chapter 4: Installing CA Internet Security Suite 2007

This chapter steps you through the installation of CA Internet Security Suite 2007, which is included with this book. This software is your first step toward active protection against threats such as viruses, spyware, and PC intrusion.

Chapter 5: Using the CA Security Center

This chapter discusses the CA Security Center, which lets you easily access and use the component products of CA Internet Security Suite—all from a single location.

Chapter 6: Detecting and Eliminating Viruses

This chapter covers the CA Anti-Virus component of CA Internet Security Suite, which protects your personal documents and your PC by detecting and eliminating all types of viral infections.

Chapter 7: Stopping Hackers from Attacking Your PC

This chapter covers the firewall component of CA Internet Security Suite, CA Personal Firewall. This software protects your personal information and PC from threats such as hacker attacks and suspicious e-mail attachments.

Chapter 8: Protecting Against Spyware and Adware

This chapter covers the CA Anti-Spyware component of CA Internet Security Suite. This software protects your identity and PC by detecting and eliminating spyware and other non-viral infections.

Chapter 9: Blocking Spam

This chapter covers the CA Anti-Spam component of CA Internet Security Suite, which helps reduce or eliminate the spam you receive.

Chapter 10: Blocking Offensive Websites

This chapter covers Blue Coat K9 Web Protection, which protects your family from web content that may be inappropriate for younger PC users.

Chapter 11: Ensuring Up-to-Date Protection

This discusses how to keep your CA Internet Security Suite up-to-date with the latest product updates. This ensures that you're properly protected from the latest Internet threats, such as new viruses, spyware, and security holes that are found every day.

Who Should Read This Book

Anyone who uses the Internet, email, or a computer should read this book.

Whether you are a self-proclaimed computer illiterate or a life-long IT professional, this book will inform you of the issues and threats associated with computer and Internet usage. It gives you the tools and understanding to properly implement solutions to combat those issues and threats, so you can be sure you don't fall victim to Internet crimes and your privacy and identity are protected.

The CA Internet Security Suite 2007 CD-ROM Included with This Book

CA Internet Security Suite 2007 provides comprehensive active protection against all the online threats discussed in this book to help ensure you and your family have a great online experience.

CA Internet Security Suite 2007 combines easy-to-use, award-winning, business-strength technology with preconfigured settings and automatic updates that take the guesswork out of PC security.

The following software applications are included in CA Internet Security Suite 2007:

- CA Anti-Virus 2007
- CA Personal Firewall 2007
- CA Anti-Spyware 2007
- CA Anti-Spam 2007
- Blue Coat K9 Web Protection 2007

Simple Computer Security

PART I

UNDERSTAND THE THREATS AND SOLUTIONS

In This Part

Chapter 1: Viruses, Spyware, and Other Malware Infections

Chapter 2: Spam, PC Intrusion, and Inappropriate Content

Chapter 3: Solutions to Online Threats

You face many threats when you use a computer for surfing the web. Being familiar with these threats and how to battle them is necessary to ensure that your documents, identity, and family are protected from things such as viruses, spyware, and hackers.

The chapters in Part I explain the main online and computing threats that you and your family face, and discuss the solutions that can be implemented to combat them.

1

VIRUSES, SPYWARE, AND OTHER MALWARE INFECTIONS

This chapter will help you learn about the different types of viruses and infections that can plague your computer and destroy your files, including the following:

- Viruses
  - Worms
  - Trojans
- Spyware
- Malware

It discusses the symptoms and prevalence of these infections, and the affects they can have on your PC's data and performance.

About Viral Infections

A computer virus is a form of malicious software, also referred to as *malware*—a catch-all term for computer programs or executable code that do bad or unwanted things. Viruses can do the following if left unchecked:

- **Damage or delete files.**

  Some viruses may delete or damage random documents or specific files that are crucial to your operating system—for example,

Windows XP system files. The damage caused by viruses can range from rendering useless just a few files to affecting your entire computer, possibly requiring you to reinstall your operating system and start from scratch.

- **Slow down your computer.**

  Viruses can run in the background, without being seen, and may cause your computer to run extremely slow.

- **Invade your email program.**

  Some forms of viruses may wreak even more havoc by spreading themselves to the contacts in your address book.

Note

Not all computer problems are caused by viruses. Even though your computer, or a particular program, may not be running properly, this could be caused by other things, such as a bug (which is simply an error in the application's code), or misconfiguration of software or hardware. Contact the software or hardware vendor to see if they are aware of any issues and if they can help.

Here are the main forms of viral infections, which are commonly referred to as *viruses*:

- **Virus**

  A "generic" computer virus is a small program that attaches itself to another program or document, such as a word processing document, and replicates it with the potential to cause damage to your computer.

  A more common type of virus is one that "invades" your email program and spreads to contacts in your address book.

- **Worm**

  This type of virus is specifically engineered to make extensive use of email and security holes in software or operating systems to spread rapidly.

- **Trojan**

  This is a type of program that pretends to be something harmless, but has a damaging or otherwise malicious intent.

  For example, a person may get a program by email or the Internet that he or she thinks is a computer game; however, when the person runs the supposed game, the program deletes files on the computer or injects viruses.

About Spyware

Spyware is a malware that is placed secretly on a computer. It tracks the user's behavior and reports information back to a central source. Some types of spyware are simply annoying because they cause increased spam or unwanted pop-ups, but others can go so far as to threaten the security of your PC and personal information.

Did you know?

The AOL/NCSA report (December 2005) reports that 61% of home users have spyware/adware installed on their PC.

Spyware can act like a peeping tom or, at worse, a geeky thief. For example, it:

- **Can be installed on your PC without your consent.**

  Typically, spyware finds its way onto PCs by "piggybacking" onto a file, such as a computer game, a music file, or a free software program (as shown in Figure 1-1), or it can be downloaded from the Internet when you visit a particular website. Pests such as spyware can often lurk silently on your computer until someone or something sets them off, or until they are found and properly removed.

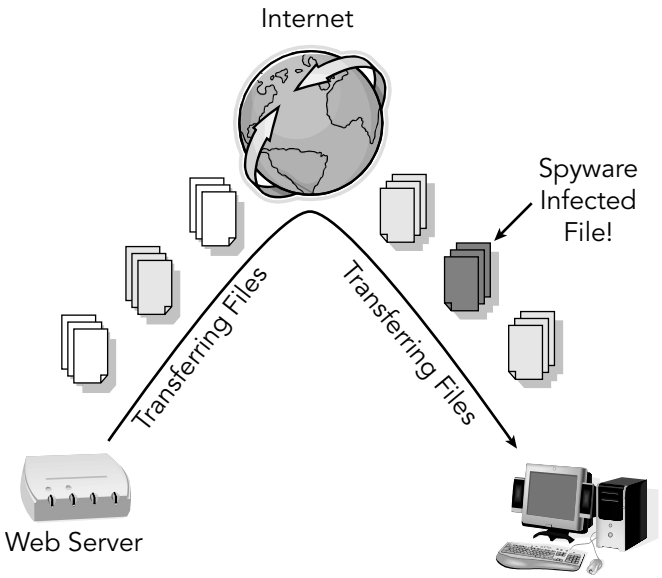

Figure 1-1: An example of how your PC may become infected

Note

While spyware may seem similar to viruses and worms, it is much different. Spyware tends to spread easily and is generally more resistant to quick-and-easy removal than most viruses.

- **Compromises your data, computing habits, and identity.**

  Spyware can monitor information about your computing habits, such as what websites you visit, or record your keystrokes, which in the end can lead to identity theft. For example, spyware can record the keystrokes that you use while keying in a credit card number and send this number to a "cyberthief." Figure 1-2 shows an example of how spyware sends your information to an unwanted, central source.

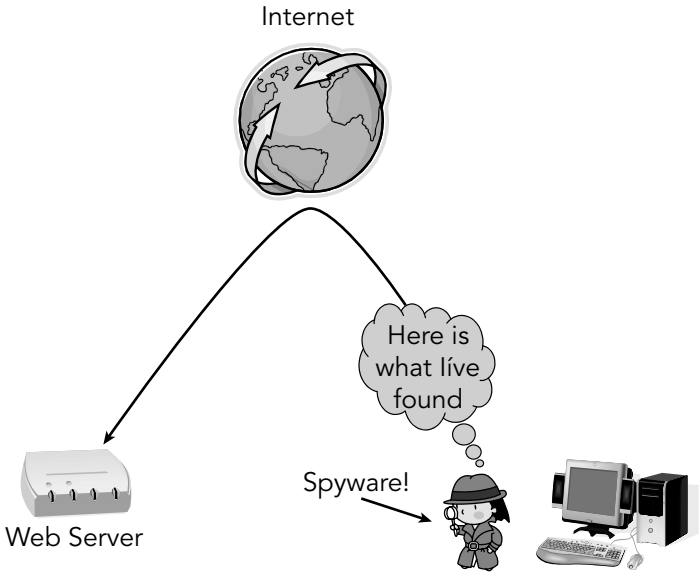

Figure 1-2: Depiction of spyware exposing your information

- **Alters PC settings.**

  Some forms of spyware can also wreak havoc by altering computer settings like your web browser home page setting or the placement of your desktop icons. This doesn't do much damage to your PC, but it's really annoying.

- **Slows down your PC.**

  Spyware can rob your PC of system speed and Internet access efficiency. This can become a big problem when you're trying to use the programs on your PC, watch videos online, or download large files.

Adware

Adware is similar to spyware — however, it may be installed with your consent. Therefore, make sure you thoroughly read installation agreements. Often there are clauses in the agreement that legally specify the installation of adware. In most cases, you probably won't notice these statements unless you read the agreement carefully.

Adware comes complete with the following disadvantages:

- **Adware takes a step further than spyware.**

  Just as with spyware, your Internet habits such as the sites you visit are tracked. In addition, however, adware uses that information to produce targeted advertising, such as pop-up ads, on your computer screen.

- **Displays arrays of annoying advertising.**

  When infected with adware, you will likely see frequent pop-up ads appear out of nowhere. This may even happen every time you open your web browser.

- **Slows down your PC.**

  The adware software working in the background and the bombardment of ads can slow your PC to a crawl.

Prevalence of Malware

After hearing descriptions of "spyware" and "adware," 43% of Internet users, or about 59 million American adults, say they have had one of these programs on their home computer.

Note

This is probably a conservative estimate, because these pests do tend to hide, and computer users may not even know if they exist on their computers, as many studies show.

Although most do not know the source of their woes, millions of home Internet users have experienced computer problems in the past year that are consistent with problems caused by computer pests and malware. For example, here are some statistics that indicate the presence of malware:

- 52% of home Internet users say their computer has slowed down or is not running as fast as it used to.
- 51% of home Internet users say their computer started freezing up or crashing, requiring them to shut down or restart.
- 25% of home Internet users say a new program appeared on their computer that they didn't install or new icons suddenly appeared on their desktop.
- 18% of home Internet users say their Internet home page changed without them resetting it.

In sum, 68% of home Internet users, or about 93 million American adults, have experienced at least one of these problems in the past year.

Sixty percent of Internet users who report computer problems do not know the source, but others cite viruses, spyware, adware, operating system flaws, and hardware glitches as the culprits. Not everyone attempted a fix, but those who did often found that they needed help, paid or unpaid. About 28 million American adults ended up spending at least $100 to get their computer working again.

Threats Affect Online Behavior

The threat of unwanted programs being secretly loaded onto computers is becoming a serious matter. As a result, many online users have begun to take precautions by changing the way they use the Internet.

Overall, 91% of Internet users say they have made at least one change in their online behavior to avoid unwanted software programs. Here are some of the changes:

- 81% of Internet users say they have stopped opening email attachments unless they are sure these documents are safe.

- 48% of Internet users say they have stopped visiting particular websites that they fear might deposit unwanted programs on their computers.
- 25% of Internet users say they have stopped downloading music or video files from peer-to-peer (P2P) networks to avoid getting unwanted software programs on their computers.
- 18% of Internet users say they have started using a different web browser to avoid software intrusions.

2

SPAM, PC INTRUSION, AND INAPPROPRIATE CONTENT

This chapter covers a few issues that relate to Internet usage, such as the following:

- Spam email
- Internet intruders and hackers
- Inappropriate online content

This chapter helps you understand these items to better protect yourself and your family while online.

About Spam

Spam is the common term for electronic "junk mail" or unwanted messages sent to a person's email account. Spam can affect your PC and productivity, and it can also be a serious threat to your security and privacy.

Did you know?
Today, 40% of all email is unsolicited, unwanted spam, as reported by the FTC.

The following are the main issues relating to spam:

- **Spam is a serious problem.**

  The billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance, and reduce overall productivity.

- **Just pressing the Delete button may not be enough.**

  Deleting spam emails seems like the simple solution, but if you add up the time spent deleting every spam email you receive, you lose a significant amount of productivity. In addition, just deleting spam does not stop it.

- **Spam can lead to worse things.**

  Spam messages may contain offensive or fraudulent material and can even be used to spread viruses.

- **Spammers are smart.**

  Along with other hijacked home computers, spammers may be using your PC to send unsolicited and possibly offensive email messages.

Did you know?
The FTC reports as much as two-thirds of spam is deceptive or false and violates the law, and as much as 30% of all spam is relayed by compromised home and home office PCs, but controlled from afar.

About PC Intrusion

Every PC connected to the Internet is a potential target for hackers. Computers are under constant attack from cyber vandals. When it comes to security, most people do not realize three very important things:

- **Internet access goes in both directions.**

  When your PC is connected to the Internet or a network, you can access the services offered by remote computers. What you might not realize (most people don't) is that other people can access your system across that same connection. Moreover, other people can take advantage of any services your system happens to be offering as well.

- **Intruders can take advantage of many things.**

  There are thousands of services that computers use, and some are more vulnerable to hackers than others. For example, most Internet users access websites through web browsers and email client software to send and receive email. However, there are thousands of other services that could be vulnerable to vandalism, including those used to send files, receive files, share printers, share files, and so on.

Did you know?
A typical unprotected PC will come under attack within 20 minutes of being connected to the Internet, says the SANS Institute.

- **By default, your PC is extremely vulnerable.**

  In the interest of ease-of-use, default settings on most machines provide wide-open access to services. To make the benefits of networking available to everyone, most manufacturers ship their systems with default configurations that allow open access among systems that might want to communicate with each other. The idea is to remove obstacles so that exchanging services and information between computers is easy. But this also makes them vulnerable to abuses, such as the following:

  - Invading your privacy and stealing copies of your files or emails.
  - Destroying your files.
  - Eavesdropping on your communications.
  - Installing malicious programs on your machines without your knowledge and permission.

Did you know?
According to the FTC, 9.9 million people suffered some form of identity theft in 2003, where PC intrusion and other online threats may have contributed to this problem, costing consumers approximately $5 billion.

Inappropriate Content

The Internet is a fascinating place, full of rich and interesting information. However, as a gigantic virtual community, it has good neighborhoods, questionable neighborhoods, and downright bad neighborhoods.

Being a part of the first generation of Internet parents may be a bit overwhelming. Nevertheless, you need to know about the following issues:

- **It really happens.**

  Even when they don't intend to, most children run into pornography, gambling, and even predators on the Internet. PC infections such as viruses and adware can also contribute to inadvertent exposure of inappropriate content to your children.

Did you know?

70% of all 15-17 year-olds who have ever gone online have accidentally stumbled across pornography while there, and 23% "very" or "somewhat" often. (Kaiser Family Foundation study, 2001)

43% of children said they do not have rules about Internet use in their homes. (Time/CNN Poll, 2000)

- **Internet predators.**

  Although some online chat rooms are monitored and violators are kicked off, many of these are full of foul language, violence, and sexual conversations. Even more frightening, instant messaging conversations are typically not monitored at all — opening the doors for Internet predators to take advantage of your children.

Did you know?

61% of parents say their teens participate in chat rooms and/or use instant messaging, as reported in the Parents' Internet Monitoring Study by the Ketchum Global Research Network.

One in five children, ages 10-17, has received a sexual solicitation over the Internet. ("The Web's Dark Secret"; *Newsweek,* 19 March, 2001)

Social networking sites, such as MySpace and Friendster, can also pose a real danger for children. Teenagers and even preteens post personal information and photographs on these sites — potential gold mines for predators.

Did you know?

17% of parents believe their children are posting online profiles, as compared to 45 percent of children who report doing this. (Internet Safety for Kids; Protocol Analysis Institute)

- **A new language.**

  This relatively new "computer age" has also affected our youth's grammar — cyberspace shorthand is most likely common in your child's online conversations. Acronyms, such as LOL (Laugh Out Loud), POS (Parent Over Shoulder) and BRB (Be Right Back), allow quick communication of emotions, comments, and other phrases. However, this may make it much more difficult for you, as a parent, to decipher your children's online activity.

3

SOLUTIONS TO ONLINE THREATS

Don't be a victim of online threats — fight back by implementing the simple solutions provided in this chapter to protect your data, identity, and family.

Fighting these online threats involves two main tasks:

- **Active Protection**

  Installing and properly using an Internet security suite — which includes protection against threats such as viruses, spyware, and PC intrusion — is vital for proper protection against the hackers, intruders, and other wrongdoers.

- **Preventative Measures**

  Even though security programs may actively detect and eliminate any threats your PC encounters, you should always help prevent these issues from ever arising.

Combat Viruses, Spyware, and Other Malware

Ensure your PC is free and stays free of malware infections by following the tips in this section.

Active Protection

- **Use Anti-Virus and Anti-Spyware software.**

You need these programs to help detect and eliminate any malware that sneaks its way onto your PC.

- **Download updates regularly.**

  New viruses and other malware emerge every day, and your security software needs to know about them in order to provide full protection.

  Security software programs, known as *signature file updates*, usually allow you to specify how to handle update downloads. The best option is to set the program to automatically update when needed, so you don't have to worry—you'll always be fully protected.

- **Run frequent full-system scans.**

  Even though most security software programs actively scan your PC for malware, you should also perform a full system scan at least once a month.

Preventative Measures

- **Keep your system up-to-date.**

  Malware often takes advantage of security holes in operating systems and software programs. You should always install any available updates for your operating system, such as Windows, and any common software you use.

  You can visit Microsoft's Windows update service at:

  `http://windowsupdate.microsoft.com`

- **Use caution when downloading files on the Internet.**

  Only download files from reputable websites by looking for signs, such as a privacy statement, full contact information, and SSL encryption of sensitive information, typically indicated by a padlock in the lower-right corner of your web browser. In addition, be wary of websites referred to you by unsolicited emails or for offers that seem too good to be true.

  To help protect yourself, you shouldn't use file-sharing programs (also known as peer-to-peer or *P2P*). In addition, trading someone else's copyrighted work is illegal, and you may end up in legal trouble.

- **Be careful with email.**

  Email is a very convenient and useful communication method; however, it's also used by hackers, spammers, and criminals to get what they want. Follow these guidelines:

- **Don't download or open unsolicited email attachments.** Only download and open email attachments from people you know.
- **Watch for phishing scams.** Criminals frequently send emails that claim to be from a legitimate enterprise in an attempt to get the user to provide private information that will be used for identity theft. This is referred to as *phishing*.

  For example, identity thieves may send a fake email saying that a particular account needs to be updated in order to prevent cancellation or fees. In the email is a link to a website that has a similar address and looks just like the organization's real site, when in reality, it sends your login and other personal information to the thief.

  Make sure you don't become a victim — if you receive emails that ask you to do something — such as login, update information, verify information, or provide sensitive information you should try to verify that it's indeed a real request and not from a thief.
- **Check your account** (via website or phone) to see if you really need to take any action specified in the email. However, don't click any links in the email and call only customer service numbers that you know to be legitimate. To access your account and check phone numbers, you should find the institution's actual website through your browser, not with the URL listed in the email.
- **Check for security alerts.** Security software sometimes can help identify fraudulent emails. If you have this type of software, try to verify the authenticity of the sender or email message.

- **Surf the Web with caution.**

  Be careful when browsing the Internet to help reduce the amount of infections your PC receives. Follow these guidelines:

  - **Review your web browser settings.** You should review and set your web browser's privacy and security settings. If necessary, refer to your browser's help section to learn more about these settings and recommendations.
  - **Don't visit illegal or adult sites.** Visiting websites that contain illegal or adult content greatly increases your chances of getting viruses, spyware, and other malware.

- **Disconnect from the Internet when you're away.** Using "always on" Internet connections such as cable and DSL increases your chances of some infections and intrusions, because your PC is always connected to the Internet. This doesn't mean you should switch back to dial-up Internet — however, you may want to disconnect from your "always on" connection when you don't plan on using it for a long period of time.

Get Rid of Spam

Tired of sorting through your junk email? This section provides some solutions that will help.

Active Protection

- **Use Anti-Spam software.**

  Not all anti-spam applications work the same; however the following are two of main methods used to get rid of spam:

  - **Sender filtering:** This method allows only messages from your approved sender list to reach your inbox — all other mail is quarantined for later review.

    This is typically the best method to properly fight spam.

  - **Key word filtering:** This method filters out email messages that contain certain key words or phrases, which are defined by you or others.

Preventative Measures

- **Keep your email address private.**

  Be careful whom you give your email address to. Before giving your address out on an online form, check if there is a website privacy policy. This policy typically informs you of how they handle your personal information.

  Signing up for free offers seen online or by email may dramatically increase your chances of receiving spam messages.

  Spammers scan websites for email addresses. Therefore, be careful about where your address is listed on the Web.

  If you do list your email address on the Web, you could use a different format and add spaces. This makes it more difficult for spammers to retrieve your email address. For

example, instead of "user@email.com," you could use "user AT email DOT com."

Most people in online forums know this trick and use it now. You could be one step ahead of the spammers and add extra spaces, such as "user AT email DOT com."

Stop PC Intrusions

Here are solutions to help ensure your PC doesn't get invaded.

Active Protection

- **Use a personal firewall.**

  A firewall acts as a barrier between your PC and the Internet, preventing unauthorized access to your PC and is an important first line of defense for computer security. It prevents unauthorized access (unauthorized programs or unauthorized Internet users) to your PC and hides your Internet-connected PC from view. All information leaving and entering your PC must pass through the firewall. It ultimately helps keep hackers away from your personal and confidential data.

Preventative Measures

- **Keep your system up-to-date.**

  Malware often takes advantage of security holes in operating systems and software programs. You should always install any available updates for your operating system, such as Windows, and any common software you use.

  You can visit Microsoft's Windows update service by visiting:

  `http://windowsupdate.microsoft.com`

- **Use caution when downloading or sharing files on the Internet.**

  Only download files from reputable websites by looking for signs, such as a privacy statement, full contact information, and SSL encryption of sensitive information, typically indicated by a padlock in the lower right hand of your web browser. In addition, be wary of websites referred to you by unsolicited emails or for offers that seem to good to be true.

  To help protect yourself, you shouldn't use file-sharing programs (also known as peer-to-peer or P2P.) In addition,

trading someone else's copyrighted work is illegal and you may end up in legal trouble.

- **Disconnect from the Internet when away.**

  Using "always on" Internet connections such cable and DSL increases your chances of some infections and intrusions as your PC is always connected to the Internet. This doesn't mean you should switch back to dial-up Internet—however, you may want to disconnect from your "always on" connection when you don't plan on using it for a long period of time.

Protect Your Family from Inappropriate Content

Follow the tips in this section to protect your family from offensive or inappropriate content on the Internet.

Active Protection

- **Use web content filtering software.**

  Web content filters, also referred to as *parental controls*, allow you to control the Internet content that is delivered to your PC. The functions and features of these filters vary greatly; however, they all generally allow you to set what content you want to allow and disallow based upon content categories, keywords, and other settings.

  Keep in mind, inappropriate pop-up windows and websites can just appear on screen even if the user isn't trying to view such material. Therefore, to protect your family you should use web content filtering to ensure only the approved material is displayed.

Preventative Measures

- **Make Internet rules.**

  Establish a set of rules for your children's Internet usage. Discuss such things as how long they can use the Internet and at what times, as well as the online services and websites they can use and those they cannot.

- **Monitor your children's Internet activity.**

  Even if you use a parental control filter, it's a good idea to know your children's online habits, such as what websites are they visiting, who they talk to, how long they stay connected, and so on.

- **Keep an eye on your children.**

  Another way to help make the Web safer for your children is to place the family PC in an exposed area, rather than in a secluded area where you can't keep an eye on them.

- **Know the Internet lingo.**

  If you currently review your child's online communications, or if you plan to, here are some common acronyms you should know:

  - LOL (Laugh Out Loud)
  - BRB (Be Right Back)
  - A/S/L (Age/Sex/Location)
  - POS (Parent Over Shoulder)
  - P911 (Parent Alert)
  - LMIRL (Let's Meet In Real Life)
  - JK (Just Kidding)

On the Web

The FBI's *A Parent's Guide to Internet Safety* is available at `http://www.fbi.gov/publications/pguide/pguidee.htm`.

Active Protection: CA Internet Security Suite

CA Internet Security Suite, developed by CA (formerly Computer Associates), provides comprehensive active protection against all the online threats discussed in this book to help ensure you and your family have a great online experience.

CA Internet Security Suite 2007 (see Figure 3-1) combines easy-to-use, award-winning, business-strength technology with preconfigured settings and automatic updates that take the guesswork out of PC security.

Consumer Story

My PC continually re-booted itself while I was using various programs, making it impossible for me to get any work done.

I chose CA Internet Security Suite, which immediately identified and removed the virus from my PC. Now it runs like new.

Barry Stradtner

Mishawaka, IN

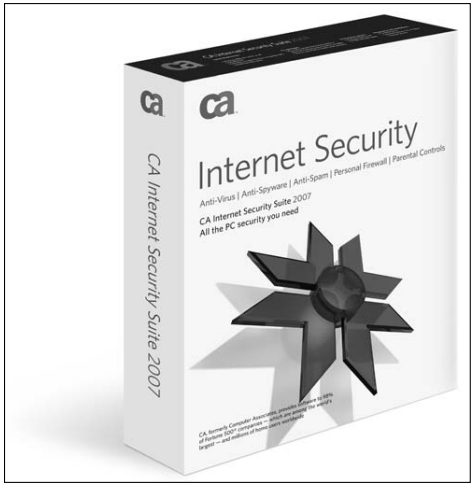

Figure 3-1: CA Internet Security Suite product box

The following software applications are included in CA Internet Security Suite:

- **CA Anti-Virus**

  If you're unprotected, viruses can invade through email, downloads, and even web pages. From there, they can destroy your photos, music, documents, and more. CA Anti-Virus provides complete protection against viruses, worms, and Trojan horse programs.

- **CA Personal Firewall**

  Every PC connected to the Internet is a potential target for hackers and identity thieves. CA Personal Firewall stops intruders, blocks malicious programs, and protects your personal information.

- **CA Anti-Spyware**

  Spyware can steal your credit card numbers and passwords, switch your home page, redirect your web searches, display annoying ads, and slow your PC to a crawl. CA Anti-Spyware (formerly *e*Trust PestPatrol Anti-Spyware) protects against a wide range of spyware threats.

- **CA Anti-Spam**

  CA Anti-Spam makes sure you get messages from people you know, and redirects messages from people you don't. It works seamlessly with Microsoft Outlook and Outlook Express to stop unwanted spam and fraudulent phishing scams.

- **Blue Coat K9 Web Protection**

  The Internet is a fascinating place, full of valuable information. But as a parent, you need a good set of guidelines about where it's safe to go. Blue Coat K9 Web Protection provides a family-safe web experience, where you control the Internet content that enters your home.

Note

To access these applications, CA Internet Security Suite provides a convenient portal screen, known as the CA Security Center (see Figure 3-2). You can get to this screen by clicking an icon in your system tray or by selecting it from the Start menu.

Figure 3-2: CA Security Center

Why Choose CA Internet Security Suite?

- **Developed by a trusted company.**

  CA provides software to 98% of Fortune 500 companies — which are among the world's largest — and to millions of home users worldwide.

- **Uses powerful technology.**

  CA Internet Security Suite gives you the same powerful technology used by the world's largest businesses, in a format that's both easy-to-use and affordable.

- **Certified and award winning.**

  CA Internet Security Suite components are ICSA-certified, and have earned numerous other certifications and awards, including Virus Bulletin 100%, West Coast Labs Checkmark certification, and PC Magazine Editor's Choice.

- **Smart design.**

  The small hard drive footprint and efficient use of system resources ensure fast installation, quick scans, and superior usability.

- **Keeps you protected.**

  With free daily protection updates, free upgrades to the latest product features, and free 24 x 7 online support, your one-year subscription helps protect you from the latest threats.

Consumer Story

My Internet experience had become so miserable that I considered disconnecting altogether. I couldn't even log on to check the news or weather without being bombarded by relentless pop-ups, adware, spyware and countless other malicious programs.

CA's user-friendly Internet Security Suite virtually eliminated my Internet problems.

Tim Pitts

Rome, GA

CA Anti-Virus: Complete Virus Protection

Here are some of the distinctive features and functionalities of CA Anti-Virus (see Figure 3-3):

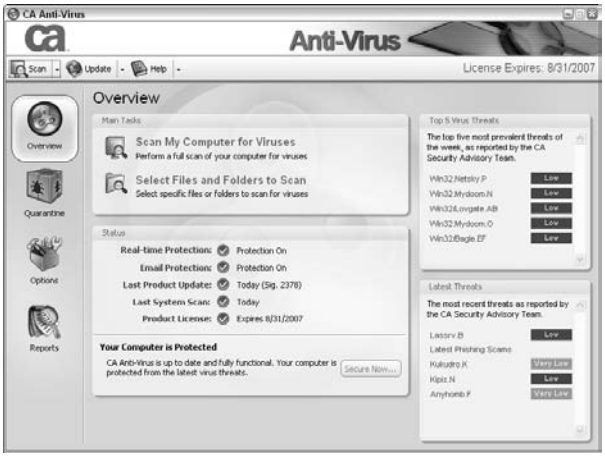

Figure 3-3: CA Anti-Virus main screen

- **Real-time, scheduled, and on-demand scanning.**

  Allows you to run a scan at any time, or schedule scans at preselected intervals to meet your needs. Real-time scanning proactively stops viruses by scanning files when they are opened, closed, or saved to your PC.

- **Automatic email scanning.**

  Protects against viruses that arrive via email, before they can cause damage.

Consumer Story

My computer had slowed down and even began to lock up. More than 1,800 viruses had infected my hard drive including some vital files in my Windows folder. I had to format my hard drive and reinstall Windows to reclaim my computer.

Before going online, I installed CA Internet Security Suite and haven't had any more Internet related problems.

David Hamilton

Colorado Springs, CO

- **File quarantine.**

  Removes malware from its current location to a secure quarantine area where you can safely review the file (see Figure 3-4).

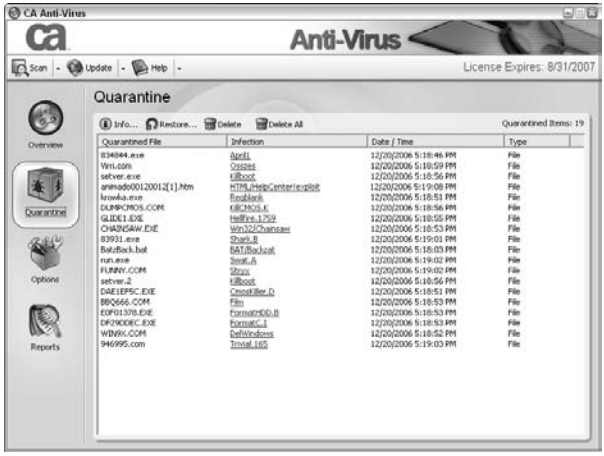

Figure 3-4: CA Anti-Virus Quarantine screen

- **Daily, fully automatic updates.**

  Easily and effectively addresses the primary reason PC users suffer attacks: out-of-date signature files.

Consumer Story

My computer crashed several times, causing me to either reboot the system or reinstall the entire operating system.

After installing CA Anti-Virus, my system has been running without failure and viruses are quickly removed.

Baskaran Muthu

Windsor, Ontario Canada

CA Personal Firewall: Complete Hacker and Privacy Protection

Here are some of the distinctive features and functionalities of CA Personal Firewall (see Figure 3-5):

Figure 3-5: CA Personal Firewall main screen

- **Pre-configured security settings.**

  Provide you with optimal protection right out of the box, and reduce firewall warnings for known programs.

- **Customized alerts.**

  Provide instant recommendations on how to handle programs' attempts to access the Internet, intrusion attempts, and other security events.

- **Ad blocking.**

  Cuts out annoying pop-up and pop-under ads, letting you surf in peace.

- **ID theft protection.**

  Alerts you when your personal information is about to leave your PC through the Internet or email, and allows you to block the transmission if desired.

Consumer Story

I found programs on my computer that I didn't voluntarily download. The programs that I did use would freeze while I was re-directed to these other programs. I've lost a lot of valuable information.

Now I use CA's firewall and anti-virus program and have not had a problem since.

Robert Fuller

Manorville, NY

CA Anti-Spyware: Comprehensive Anti-Spyware Solution

Here are some of the distinctive features and functionalities of CA Anti-Spyware (see Figure 3-6):

Figure 3-6: CA Anti-Spyware main screen

- **Comprehensive spyware detection and removal.**

  Provides complete protection against a wide range of spyware, adware, keyloggers, browser hijackers, and other threats.

- **Real-time spyware protection.**

  Prevents and removes unwanted applications, prevents malicious changes to Windows files and settings, and protects browser settings for your home page, favorites, and search pages.

- **Scheduled and on-demand scanning.**

  You can launch scans on demand or schedule regular scans to meet your needs. Custom scans allow you to select specific disks, files, and folders to scan. Figure 3-7 shows an example of a completed spyware scan.

Figure 3-7: CA Anti-Spyware Scan screen

- **Detailed scan results.**

  Shows the specific threat level of any spyware found, and allows you to link to the CA Spyware Information Center for more details.

Consumer Story

A cyber criminal gained access to my PayPal account through the Internet, and purchased nearly $1,000 in goods—with my money.

After discovering that, I installed CA Anti-Spyware and haven't had any problems since then.

Geof Steele

Calgary, AB Canada

Consumer Story

Without anyone using the computer, the Internet connection would light up and our PC would run as if it had a mind of its own. Someone was using it — unfortunately, it was no one we knew. CA Anti-Spwyare found and removed several spyware programs. Most of all it blocked the intruder's access to our PC.

Thomas Horton

Mount Airy, NC

CA Anti-Spam: Complete Spam Protection

Here are some of the distinctive features and functionalities of CA Anti-Spam (see Figure 3-8):

Figure 3-8: CA Anti-Spam toolbar

- **Blocks unwanted spam.**

  Allows only messages from your approved senders list to reach your email inbox — all other mail is quarantined for you to review later.

- **Prevents phishing attacks and email fraud.**

  Automatically verifies the authenticity of messages, and displays a clear visual warning on suspicious emails.

Consumer Story

A barrage of spam messages soliciting drugs, sex, and other offensive content streamed into my inbox. Dodging the unwanted messages was very time consuming.

By downloading CA Anti-Spam, I've almost eliminated any unwanted messages.

Jayne Stowell

Barrowby, Grantham Lincs.

- **Integrates seamlessly with Microsoft Outlook/ Outlook Expresss.**

  Provides easy access to all features directly from the toolbar in Microsoft Outlook and Outlook Express.

- **Email search.**

  Creates a search index of all information stored in Microsoft Outlook, so you can quickly and easily find messages, attachments, contacts, appointments, journal entries, and notes.

Blue Coat K9 Web Protection: Take Control

Here are some of the distinctive features and functionalities of Blue Coat K9 Web Protection (see Figure 3-9):

Figure 3-9: Blue Coat K9 Web Protection admin screen

- **Customizable web filtering policy.**

  Allows you to create filtering rules that meet your specific needs by choosing from over 55 unique categories.

- **Administrator password protection.**

  Allows you to set a password to block others from modifying settings or disabling the filtering function.

- **Extensive reporting capabilities.**

  Offers detailed reports of all Internet activity, including all websites visited and blocked, the category ratings of the sites, and the URLs of visited sites.

Consumer Story

Allowing our children Internet access made us uneasy, especially knowing of a rash of online predators living in the surrounding area.

To solve the problem, we installed CA Internet Security Suite with Parental Controls. Now we allow our children to enjoy the benefits of Internet activity with less worry.

Richard DeHart

Whitehouse, Texas

PART II

DETECT AND ELIMINATE THREATS

In This Part

The chapters in this part explain how to install, set up, and use two pieces of software—CA Internet Security Suite and Blue Coat K9 Web Protection—which will protect you from the major online and computing threats discussed in Part I. In addition, you learn how to keep your software up-to-date to ensure that you're properly protected from the latest threats.

Each chapter covers a different security software component, and begins by reviewing what the component does and the methods used to provide the protection. Along with an introduction and tour of the component's screens are step-by-step instructions to help you set up and use the component's options.

4

INSTALLING CA INTERNET SECURITY SUITE 2007

Installing CA Internet Security Suite 2007, which is included with this book, is your first step toward active protection against threats such as viruses, spyware, and PC intrusion — which is vital in this day and age to guard against hackers, intruders, and other wrongdoers.

Operating System Support

CA Internet Security Suite 2007 requires that you have one of the following operating systems installed:

- Microsoft Windows 98 (Second Edition)
- Microsoft Windows ME
- Microsoft Windows 2000 (with Service Pack 3 or later)
- Microsoft Windows XP Home Edition or Professional Edition (with Service Pack 1 or later)

You can visit the CA consumer support web site at `http://www.ca.com/consumer/support` for the latest information about supported operating systems.

Note

Windows Server based operating systems are not supported.

Blue Coat K9 Web Protection is only supported for Windows 2000 and Windows XP.

System Requirements

The following requirements must be met or exceeded for a full installation of CA Internet Security Suite 2007:

- 60MB free hard disk space
- CD-ROM drive
- Internet Explorer 5.5 or later
- Internet access

Individual Programs

Tables 4-1 through 4-4 list the system requirements (based on your operating system) that must be met or exceeded for the particular programs to install and run correctly.

Table 4-1: Microsoft Windows 98 (Second Edition)

Program	*Processor Speed*	*Memory (RAM)*	*Disk Space*
CA Anti-Virus	300MHz	256MB	25MB
CA Personal Firewall	300MHz	256MB	25MB
CA Anti-Spyware	300MHz	256MB	25MB
CA Anti-Spam	300MHz	128MB	25MB

Table 4-2: Windows ME

Program	*Processor Speed*	*Memory (RAM)*	*Disk Space*
CA Anti-Virus	300MHz	256MB	25MB
CA Personal Firewall	300MHz	256MB	25MB
CA Anti-Spyware	300MHz	256MB	25MB
CA Anti-Spam	300 MHz	128MB	25MB

Table 4-3: Windows 2000 (Service Pack 3 or later)

Program	*Processor Speed*	*Memory (RAM)*	*Disk Space*
CA Anti-Virus	300MHz	256MB	25MB
CA Personal Firewall	300MHz	256MB	25MB
CA Anti-Spyware	300MHz	256MB	25MB
CA Anti-Spam	300MHz	128MB	25MB
Blue Coat K9 Web Protection	233MHz	64MB	25MB

Table 4-4: Windows XP (Service Pack 1 or later)

Program	*Processor Speed*	*Memory (RAM)*	*Disk Space*
CA Anti-Virus	300MHz	256MB	25MB
CA Personal Firewall	300MHz	256MB	25MB
CA Anti-Spyware	300MHz	256MB	25MB
CA Anti-Spam	300MHz	128MB	25MB
Blue Coat K9 Web Protection	233MHz	64MB	25 MB

In addition, the following software is required for CA Anti-Spam installations:

- One or more POP3 or MAPI email accounts
- One of the following products:
  - Microsoft Outlook 2000, 2002, or 2003
  - Microsoft Outlook Express 5.5, 6.0, or later

Note

CA Anti-Spam is not suitable for installation on Windows 95, Windows NT, or any Windows Server operating systems.

Before Installing CA Internet Security Suite 2007

Make sure you follow these directions and recommendations before starting the installation:

- Uninstall any firewall software running on your computer. You must uninstall this software and reboot your computer before you install CA Internet Security Suite. Failure to do so may cause conflicts between the two products.

Note

However, if you use Windows XP's firewall utility don't worry about disabling or uninstalling it. CA Internet Security Suite will detect if the Windows Firewall utility is present (and running) and will disable it prior to installation. When CA Personal Firewall is uninstalled, it will then reenable Windows Firewall.

- Uninstall any anti-virus software other than a previous version of eTrust(r) EZ Antivirus, or CA Anti-Virus. You must uninstall this software and reboot your computer before you install CA Internet Security Suite. Failure to do so may cause conflicts between the two products, resulting in a system failure.
- Uninstall or shut down any existing anti-spyware software running on your computer before you install CA Internet Security Suite.
- Close all programs currently running on your computer before you install the product.

Installing CA Internet Security Suite 2007

Follow these steps to install CA Internet Security Suite 2007, which is included with this book.

Step 1

Insert the CA Internet Security Suite installation CD into your drive.

The installation will begin automatically and the Installation Menu appears.

Note
If the installation does not start automatically, you can launch it by browsing to the drive containing the CD, and double-clicking the `setup.exe` file.

Select Install from the Installation Menu.

Step 2

The welcome message appears, shown in Figure 4-1.

Figure 4-1: Welcome message

Click Next to continue.

Step 3

The CA Product License dialog appears, as shown in Figure 4-2, and displays the End-User License Agreement.

Read the End-User License Agreement.

If you agree with the terms of the agreement, scroll to the end of the agreement, select the I accept the terms of the License Agreement option button, and click Next.

Note
If you click the "I do NOT accept" button, the installation ends.

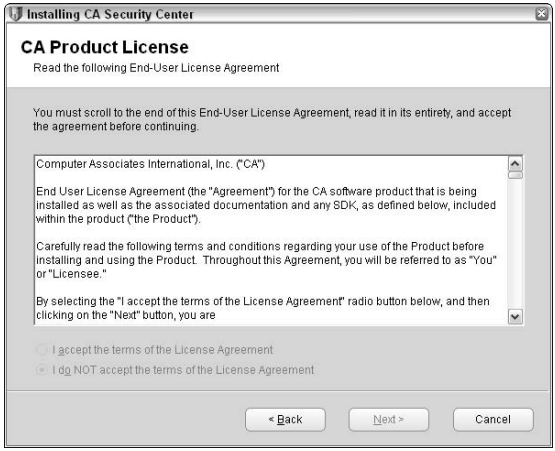

Figure 4-2: CA Product License dialog

Step 4

The Lesser General Public License (LGPL) window appears, as shown in Figure 4-3.

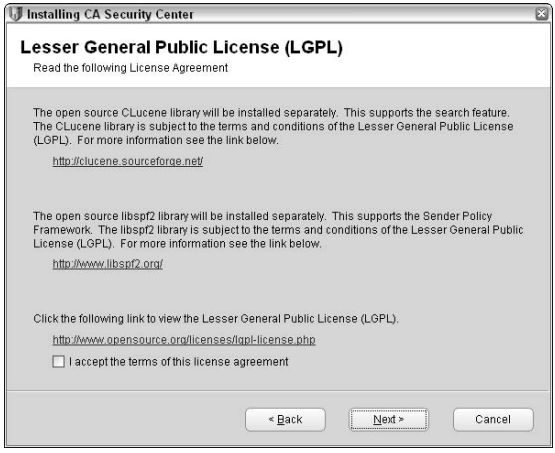

Figure 4-3: Lesser General Public License (LGPL) window

Read the LGPL agreement.

If you agree with the terms of the agreement, select the I accept the terms of this license agreement check box and click Next.

Step 5

The Enter License Key window appears, as shown in Figure 4-4.

Figure 4-4: Enter License Key window

Enter your license key and click Next.

Note

You will find your license key in the CD pocket along with the CA Internet Security Suite 2007 CDs bundled with this book.

Step 6

The Installation Path dialog appears, as Figure 4-5 shows.

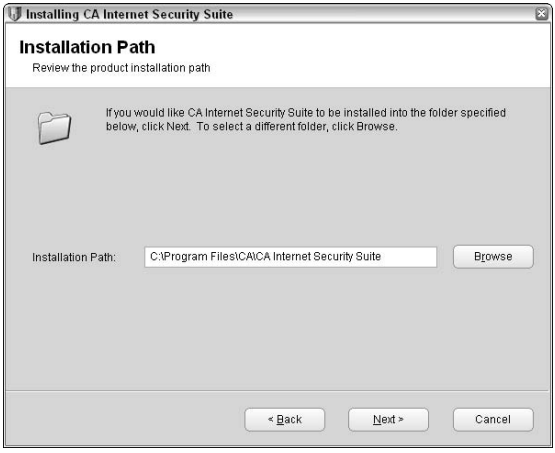

Figure 4-5: Installation Path dialog

Select the folder in which you want to install CA Internet Security Suite and click Next.

Note

The default installation folder is `C:\Program Files\CA\CA Internet Security Suite`. To install the product to a different folder, enter the folder name in the Installation Path field or click Browse to select the appropriate folder.

Step 7

The Product Options window appears, as shown in Figure 4-6.

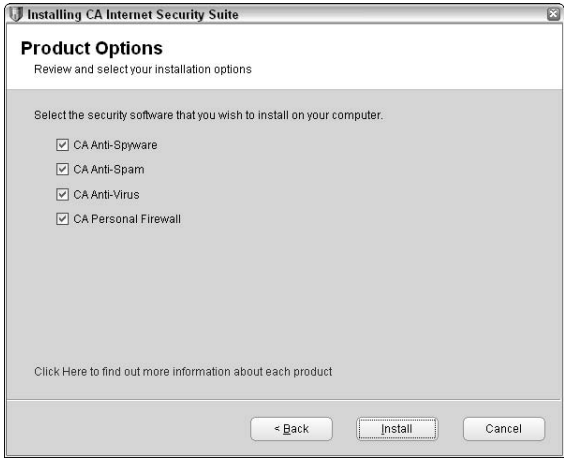

Figure 4-6: Product Options window

Select the corresponding check boxes of the security software that you want to install, and then click Install.

The installation begins copying files. It might take several minutes, depending on the speed of your computer and connection. During the process, the installation status is displayed. If you are connected to the Internet, the installation also downloads the latest product updates.

After the installation process is complete, the Product Registration dialog appears.

Note
If you previously registered your CA product using the license key entered, the Product Registration dialog box does not appear and you can skip the next step.

Step 8

If you are connected to the Internet, ensure that you register your product.

If you are not currently connected to the Internet, you can register when your computer is online by opening the CA Security Center and clicking Help, then click Product Registration.

You're Done!

The Installation Complete dialog box appears (see Figure 4-7).

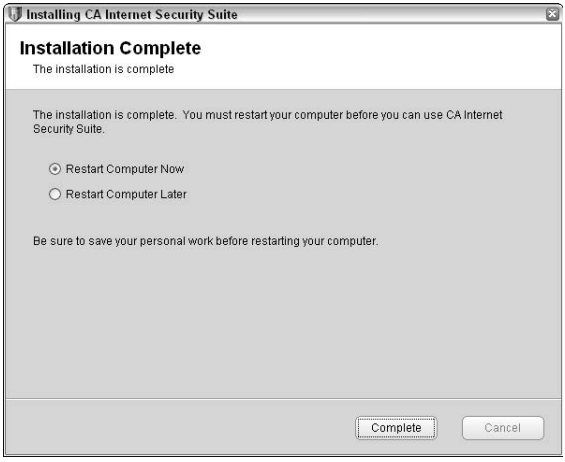

Figure 4-7: Installation Complete dialog

Specify if you would like to restart your computer now or later, and then click Complete.

Warning
It is advised that you restart immediately, as you will not have any protection until your computer is restarted.

Congratulations! CA Internet Security Suite is now installed on your computer.

Prior to Installing Blue Coat K9 Web Protection

Users of CA Internet Security Suite 2007 (with a valid license) are automatically entitled to a one-year license for Blue Coat K9 Web Protection, so keep in mind:

- You must complete the installation of CA Internet Security Suite 2007 on your computer (including restarting your PC) before starting the Blue Coat K9 Web Protection installation.

Installing Blue Coat K9 Web Protection

Follow these steps to install Blue Coat K9 Web Protection, which is included with this book.

Step 1

Insert your Blue Coat K9 Web Protection installation CD into your drive.

The Setup Wizard, seen in Figure 4-8, will begin automatically.

Figure 4-8: Blue Coat K9 Web Protection Setup Wizard

Note

If your installation fails to start automatically, you can launch it by browsing to the drive containing the CD, and double-clicking the `k9-webprotection.exe` file.

Click Next to continue.

Step 2

On the next screen, shown in Figure 4-9, you will be prompted to accept the K9 Web Protection license agreement.

Figure 4-9: K9 Web Protection License Agreement dialog

Click the I Agree button to accept the agreement.

Step 3

Now you will see the Choose Install Location dialog box, shown in Figure 4-10.

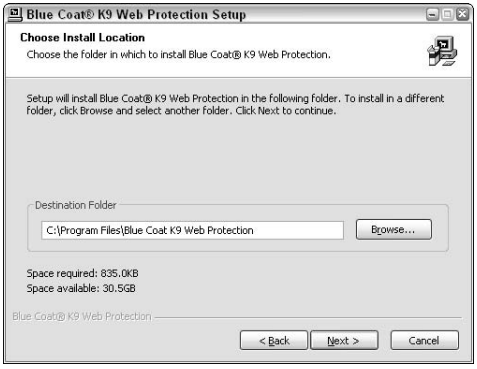

Figure 4-10: Choose Install Location dialog

Blue Coat K9 Web Protection defaults to `C:\Program Files\Blue Coat K9 Web Protection`. If you want to install the software in a folder other than this one, click the Browse button and select a different location.

When finished, click Next.

Step 4

You will now see the Install License dialog box, as shown in Figure 4-11.

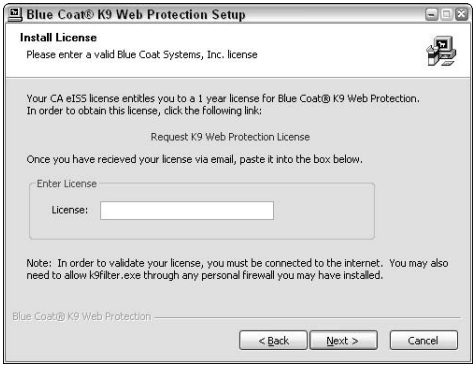

Figure 4-11: Install License dialog

Obtain your Blue Coat K9 Web Protection License as follows:

1. Click the Request K9 Web Protection License (or Get License...) link.

   This will take you to the Blue Coat K9 Web Protection website, as seen in Figure 4-12.
2. Fill out the license request form, and then click Request License.
3. Your Blue Coat K9 Web Protection license will be emailed to you shortly.

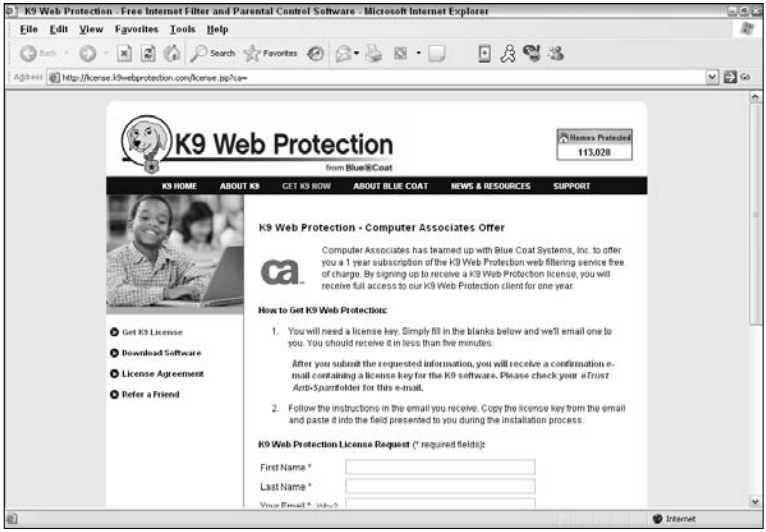

Figure 4-12: K9 Web Protection license request Web page

Note

Your email account (and/or your Internet Service Provider) may be set to disregard unwanted email (known as "spam"). To ensure that you get your K9 license email, configure your mail account to accept messages from `k9support@bluecoat.com`. If you do not see the K9 license email shortly after requesting your license, check your email account anti-spam settings, and check your "junk" folder to see if the K9 license email was routed there.

Step 5

Copy your K9 license from your email message, paste it into the Enter License box, and click Next.

Step 6

Now you will see the Install Password dialog box, as shown in Figure 4-13.

Figure 4-13: Install Password dialog

Enter and verify your password, and then click Next.

Note

The password must be 15 characters or less and can only include alphanumeric characters (A–Z and 0–9) as well as the following: !, @, #, $, %, ^, *, (,), {, and }.

This password will enable you to access the K9 Web Protection administration interface, configure the Web filtering rules according to your needs, and override blocked pages. It is also required to uninstall the application.

Step 7

Now you will see the Shortcut Placement dialog box, shown in Figure 4-14.

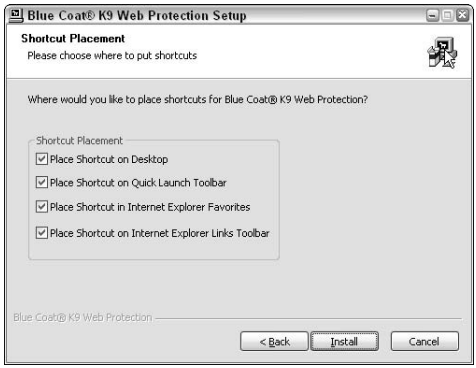

Figure 4-14: Shortcut Placement dialog

Choose which shortcuts you want by checking the appropriate boxes, and then click Install.

You're Done!

The Installation Complete dialog appears, as shown in Figure 4-15.

Figure 4-15: Installation complete dialog

Specify whether you would like to reboot your computer now or later, and then click Finish.

Warning

It is advised that you restart immediately, as you will not have any protection until your computer is restarted.

Congratulations! Blue Coat K9 Web Protection is now installed on your system

Blue Coat K9 Web Protection will begin (after the reboot) protecting your system with the Default Internet Protection Level.

To change the Internet Protection Level, you will need to log into K9 Web Protection administration interface and go to the Set Up K9 tab, which is discussed in Chapter 10.

5

USING THE CA SECURITY CENTER

The CA Security Center lets you easily access and use the component products of CA Internet Security Suite — all from a single location.

Open the CA Security Center

You can open the CA Security Center in any of the following ways:

- **A quick double-click.**

  By far the easiest way to access CA Security Center is by double-clicking on the system tray icon, which is in the lower-right corner of your desktop (see Figure 5-1).

- **System tray right-click option.**

  You can use the system tray icon to open the CA Security Center. Simply right-click on the icon and click Open CA Security Center (see Figure 5-2).

Figure 5-1: Opening CA Security Center with a quick double-click

Figure 5-2: Opening CA Security Center with the system tray option

- **Start menu.**

  If you have something against using the system tray icon, or if it has disappeared, don't worry. Browse to the following path on your Start menu:

  Programs (or All Programs) → CA → CA Internet Security Suite

  Then click CA Security Center, as shown in Figure 5-3.

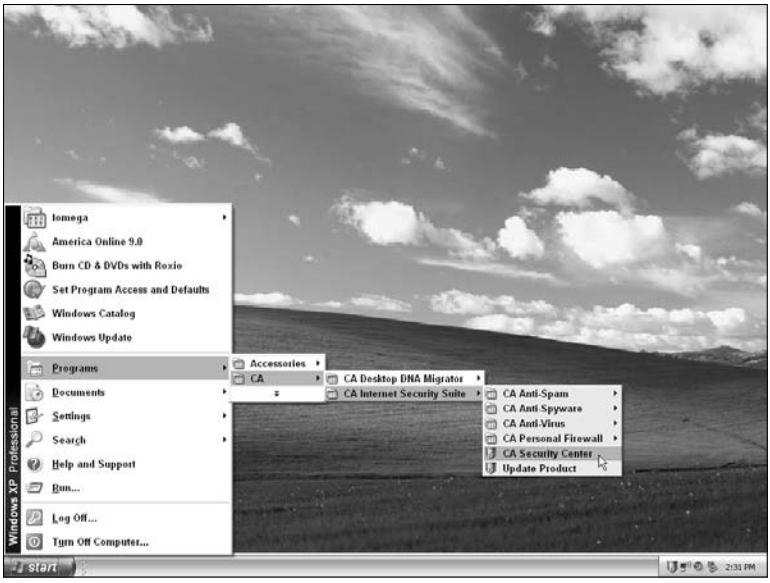

Figure 5-3: Opening CA Security Center via the Start menu

The CA Security Center Window

The CA Security Center window, shown in Figure 5-4, provides a panel for each component of the CA Internet Security Suite, whether or not the product is installed. These panels enable you to access the individual functions and settings of each component.

Figure 5-4: CA Security Center window

In addition, the CA Security Center window provides the following information:

- Component status
- License status
- Product updates
- Help documentation

Click the arrows to the right of a component to access its basic functions or to view more information about it, as shown in Figure 5-5. Another way to do this is by clicking the component icon or name.

Figure 5-5: Expanding component panels

Status Information

The CA Security Center window provides status information for the CA Internet Security Suite component products and lets you launch basic functions for your installed products.

The product panels display the following status indicators, as shown in Figure 5-6, to let you know the status of the component products:

Figure 5-6: Status of component panels

- **Protected**

  The component product is installed on your computer and is functioning as expected.

- **Attention Needed**

  The component product is installed, but there are issues to resolve. Click Secure Now to address the issues.

- **Expired**

  Your product license has expired. Click Renew License to access a website that provides information about renewing your license.

- **Not Installed**

  The component product is not installed on your computer. Click Install Now to access a website providing information about purchasing the product.

Common Functions

You can access the following common functions from the CA Security Center window:

- **Update**

  Lets you update the CA Internet Security Suite, configure proxy settings, access automatic product update options, and view update logs.

- **Help**

  Lets you view the help topics, contact Technical Support, register products, and obtain version information for the CA Internet Security Suite.

Use the System Tray Icon

CA Internet Security Suite uses a single system tray icon (shown in Figure 5-7) to represent all installed component products, although you can use component-specific sub-menus or different tray icons.

Figure 5-7: CA Internet Security Suite System Tray icon

The icon indicates warning or alert states for the installed components and some system and product activities, such as when a component's real-time protection is disabled.

You can double-click the icon for details about the warning or the alert state.

In addition to the functions available from the CA Security Center window, when the CA Security Center window is minimized, you can access task-oriented options from the tray icon on your task bar.

You can right-click the tray icon, as shown in Figure 5-8, to access the following options:

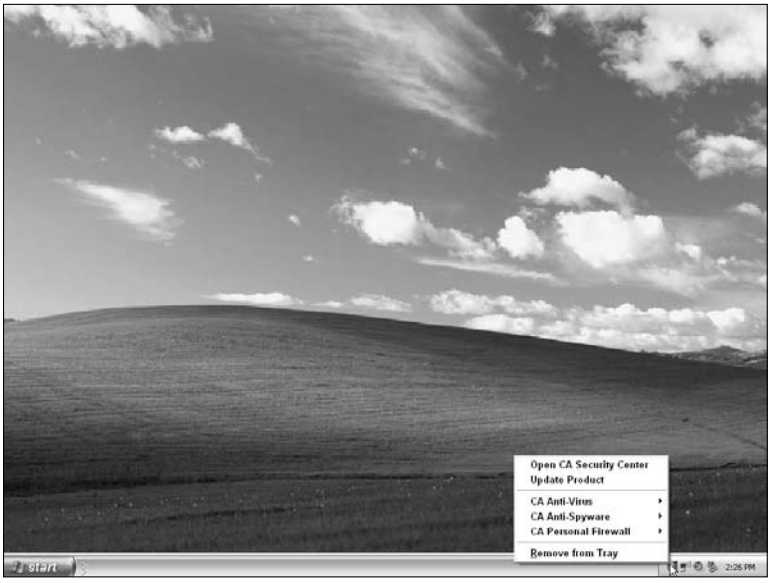

Figure 5-8: System Tray icon options

- **Open CA Security Center**

  Reopens the CA Security Center window.

- **Update Product**

  Opens the Product Update dialog box where you can download and install product updates.

- **CA Anti-Virus**

  Opens the CA Anti-Virus component or opens the Snooze Anti-Virus Protection dialog box to stop real-time scanning for a specified period of time.

- **CA Anti-Spyware**

  Opens the CA Anti-Spyware component.

- **CA Personal Firewall**

  Opens the CA Personal Firewall component, shuts down CA Personal Firewall, or stops all access to the Internet.

6

DETECTING AND ELIMINATING VIRUSES

The antivirus component of the CA Internet Security Suite protects your personal documents and your PC by detecting and eliminating all types of viral infections.

Virus Scanning and Detection Methods

CA Anti-Virus uses three main scanning methods to ensure any viral infections are detected:

- **Real-time scanning.**

  The scanning of files and emails as they are accessed. Access includes any form of action that is taken on a file or email, such as opening, copying, or moving the file or email. It may also include access that is initiated by the Windows operating system. With real-time protection enabled, each time a file or email is accessed, it is scanned for viruses.

  When a virus is detected by real-time protection, a message window appears, advising you about all aspects of the virus that was found. The message includes a link to virus-specific information on the product website. With the default configuration enabled, the virus is removed from the location where it was detected, and the system is cleaned.

- **On-demand scanning.**

  The scanning of all items on your computer, or the scanning of only the files or folders that you specify. Here are some examples of on-demand scanning:

  - Scanning that is initiated by selecting the Scan My Computer For Viruses option
  - Scanning that is initiated by configuring a scheduled scan
  - Scanning that is initiated by choosing the Selective Scanning option
  - Scanning that is initiated by right-clicking a file and selecting CA Anti-Virus from the right-click menu

- **Heuristic scanning.**

  Heuristic scanning refers to rule-based scanning. In many cases, for antivirus software to detect a virus, the virus must have been seen and analyzed before, and its detection must have been added to the signature update files. There are some families of viruses that continually change their appearance, making it impossible to detect every variant. Heuristics let virus researchers set up rules so that if an item appears to be a virus and acts like a virus, it can be detected even if it has not been seen before.

Open CA Anti-Virus

You can open CA Anti-Virus using any of the following methods:

- **CA Security Center**

  You can quickly access CA Anti-Virus from the CA Security Center.

  1. Double-click the CA Security Center system tray icon (see Figure 6-1).
  2. Expand the CA Anti-Virus component panel, and then click its arrow, icon, or name.
  3. Click Open Advanced Settings, as shown in Figure 6-2.

Figure 6-1: Double-clicking the System Tray icon

Figure 6-2: Opening CA Anti-Virus

- **System Tray Icon**

  You can also use the system tray icon to open CA Anti-Virus.

  1. Right-click the CA Security Center system tray icon, as shown in Figure 6-3.

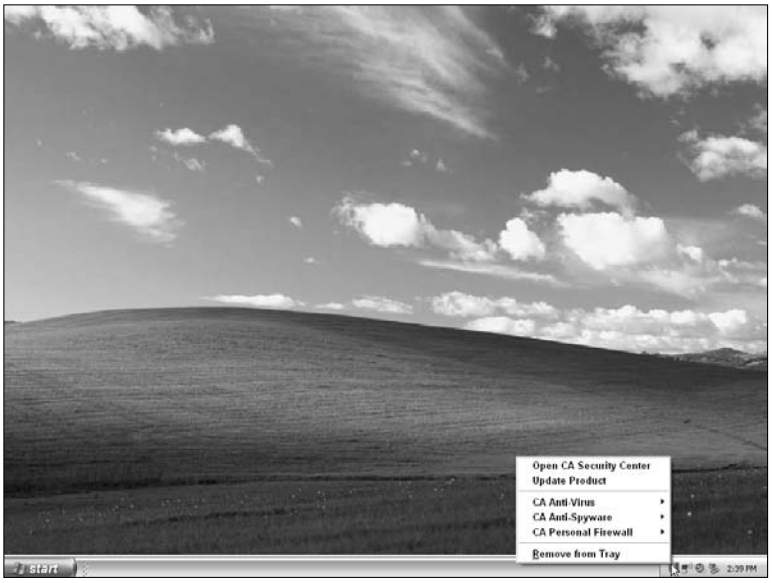

Figure 6-3: Right-clicking the System Tray icon

2. Select CA Anti-Virus.
3. Click Open CA Anti-Virus, as shown in Figure 6-4.

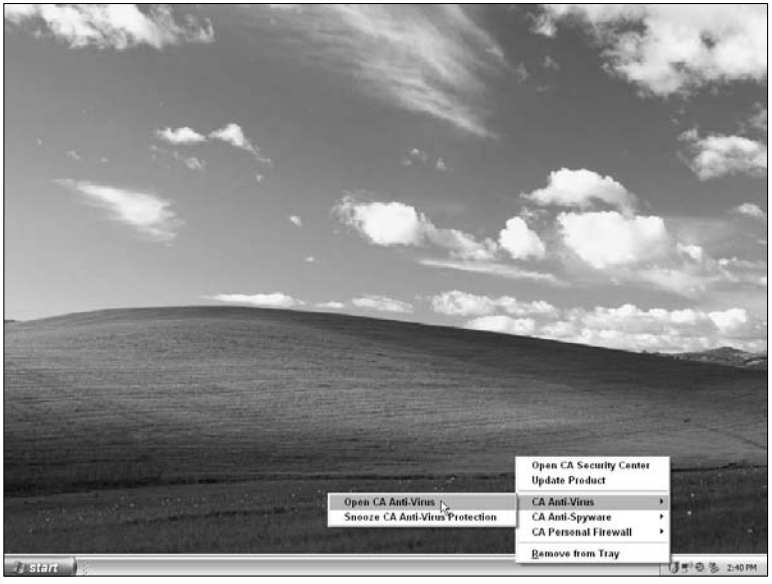

Figure 6-4: Opening CA Anti-Virus

- **Start Menu**

  If you have something against using the system tray icon and security center, or if the icon has disappeared, don't worry. Browse to the following path on your start menu:

  Programs (or All Programs) ➔ CA ➔ CA Internet Security Suite ➔ CA Anti-Virus

  Then click on CA Anti-Virus, as shown in Figure 6-5.

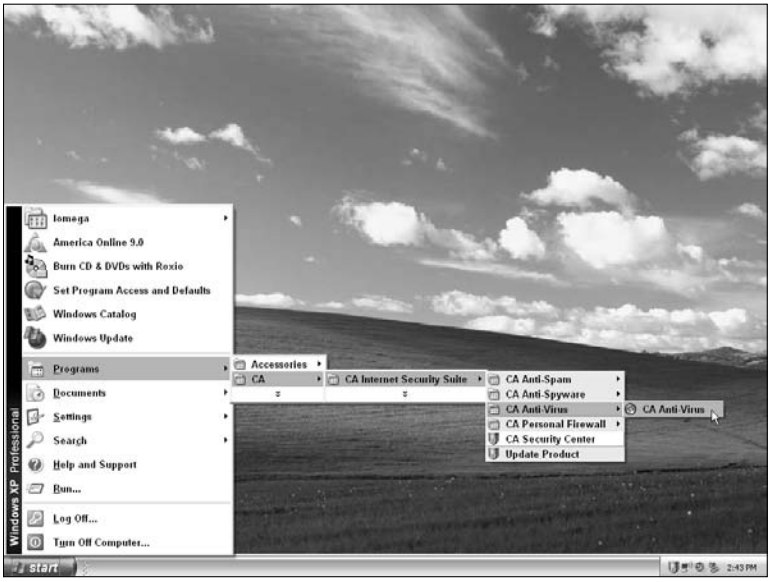

Figure 6-5: Opening CA Anti-Virus from the Start menu

CA Anti-Virus Introduction

The CA Anti-Virus screen is organized to allow quick access to the common functions and features. This section discusses the main pages or screens of CA Anti-Virus, which you access by clicking the appropriate tabs in the software.

Overview Screen

From this screen (see Figure 6-6), you can launch the virus scanner, check component status, and review the latest threats.

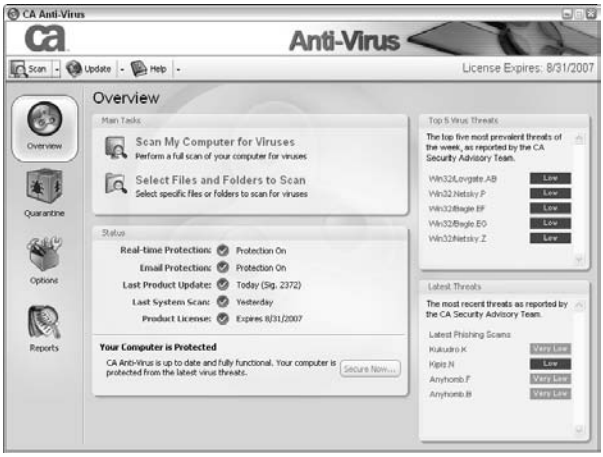

Figure 6-6: CA Anti-Virus Overview screen

The following sections discuss the status area of the overview screen, shown in Figure 6-7. Therefore, you'll understand exactly what the software is trying to tell you based all the different status indicators.

Figure 6-7: CA Anti-Virus Status area

Real-Time Protection Status

This field displays the status of your real-time (background scanning) protection.

Here are all the possible status conditions:

- **Protection On**

  Represented by a check mark, this indicates that real-time protection is active and functional.

- **Attention Needed**

  Represented by an X, this lets you know that real-time protection is not functional.

- **Warning**

  Represented by an exclamation point (!), this warns you that real-time protection has been disabled or is in Snooze mode.

- **Paused**

  Represented by a clock icon, this reminds you that real-time protection is in Snooze mode.

Note
If the status of Attention Needed or Warning is displayed, or real-time protection is in Snooze mode, you can use the Enable Now link to re-enable real-time protection.

Email Protection Status

This field displays the status of your email protection.

Here are all the possible status conditions:

- **Protection On**

  Represented by a check mark, this indicates that email protection is active and functional.

- **Attention Needed**

  Represented by an X, this lets you know that email protection is not functional.

- **Warning**

  Represented by an exclamation point (!), this warns you that email protection has been disabled or is in Snooze mode.

- **Paused**

  Represented by a clock icon, this reminds you that real-time protection is in Snooze mode.

Note
If the status of Attention Needed or Warning is displayed, or email protection is in Snooze mode, you can use the Enable Now link to reenable email protection.

Last Product Update Status

This field displays the status of your antivirus updates, based on the following conditions:

- **If you have updated within the last 7 days**

  Displays a check mark and lets you know how many days since the last update.

- **If you have not updated within the last 7 days**

  Displays an exclamation point (!) and lets you know how many days since the last update.

- **If you have never updated**

  Displays an X.

Note

If the product update has not been performed recently, you can use the Update Now link to immediately run an update.

Last System Scan Status

This field displays the status of your antivirus scan, based on the following conditions:

- **If you have performed a scan within the last 30 days**

  Displays a check mark and lets you know how many days since the last scan.

- **If you have never performed a scan or it has been more than 30 days since your last system scan**

  Displays an exclamation point (!).

Note

If the scan has not been performed recently, you can use the Scan Now link to start a scan.

Product License Status

This field displays the status of your CA Anti-Virus product license, based on the following conditions:

- **If your license is current**

  Displays a check mark and lets you know when the license expires.

- **If your license is due to expire within 30 days or has already expired**

  Displays an exclamation point (!).

- **If your license has been expired for more than 30 days**

  Displays an X.

Note
If the license has expired, you can use the Renew Now link to renew your product license.

Quarantine Screen

The Quarantine feature moves infections that cannot be cleaned or deleted from their existing location into a safe, quarantined area on your computer. When an infected item is quarantined, it can no longer be accessed by the file system, and it disappears from the location in which it was detected.

The Quarantine screen (see Figure 6-8) provides an area in which you can review infected items and restore them as you see fit. Certain infections may require further analysis by CA Anti-Virus research. After such research has been completed on the file in question, a new virus signature may be produced to allow CA Anti-Virus to clean the infection.

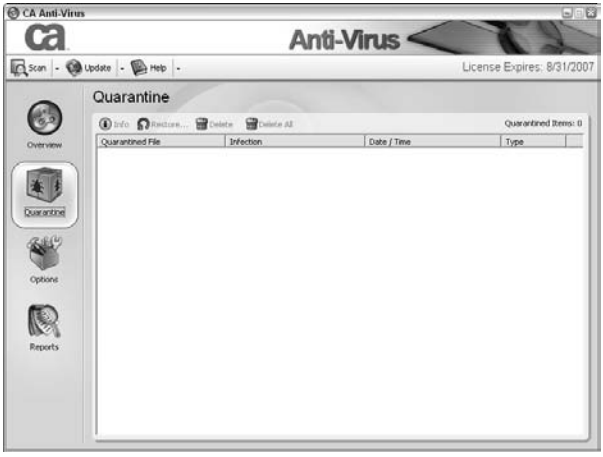

Figure 6-8: CA Anti-Virus Quarantine screen

Options Screen

The Options screen (see Figure 6-9) is where you go to change any settings or preferences related to the Anti-Virus component.

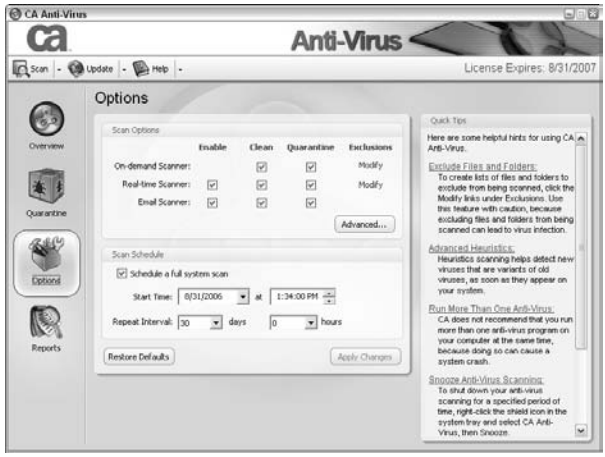

Figure 6-9: CA Anti-Virus Options screen

Reports Screen

On the Reports screen (see Figure 6-10), you can view all the logs relating to your Anti-Virus activities.

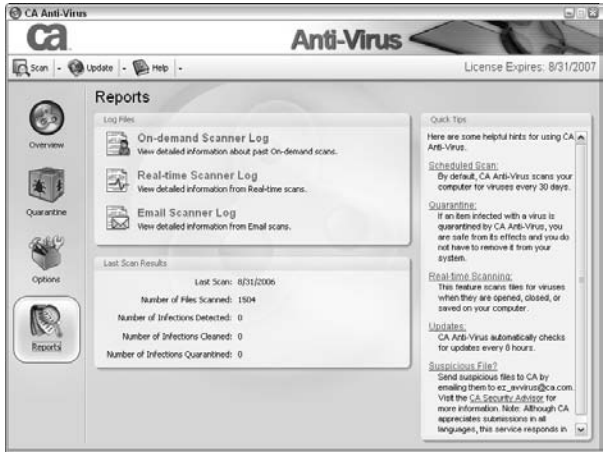

Figure 6-10: CA Anti-Virus Reports screen

Common Tasks

This section provides step-by-step directions for common tasks relating to the Anti-Virus component.

Secure Now

To fix problems associated with your anti-virus software, you can use the Secure Now feature:

Note

The Secure Now feature and the button is only available and active when an action is needed, such as to fix problems with the software.

1. Select the Overview tab on the left side of the CA Anti-Virus window.

   The Overview window appears.

2. Click Secure Now, as shown in Figure 6-11.

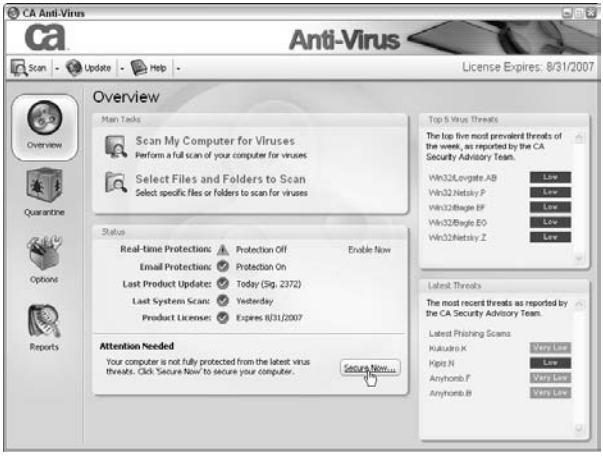

Figure 6-11: Clicking Secure Now

The Secure Now window appears, as seen in Figure 6-12.

Figure 6-12: Secure Now window

3. Review the list of actions to be performed, and click Continue.

   The software automatically performs various tasks depending on what issues need to be addressed. These tasks include automatically updating, enabling real-time protection, performing a system scan, and renewing your subscription.

Perform an On-Demand Virus Scan

To keep your PC free of infection, you should manually perform virus scans on a regular basis in order to detect and clean viruses. You have the choice of a full system scan that will check all areas of your computer (which includes items such as boot sectors, hard drives, and removable media such as ZIP drives, floppy drives, and CD/DVD drives), or you can pick out what files and/or folders to check.

Full System Scan

You can manually run a full system virus scan by following these steps:

Note

This scanning method checks all areas of your computer for viruses, including boot sectors, hard drives, and removable media such as ZIP drives, floppy drives, and CD/DVD drives.

1. Select the Overview tab on the left side of the CA Anti-Virus window.

   The Overview window appears.

2. Click Scan My Computer for Viruses, as shown in Figure 6-13 in the Main Tasks area.

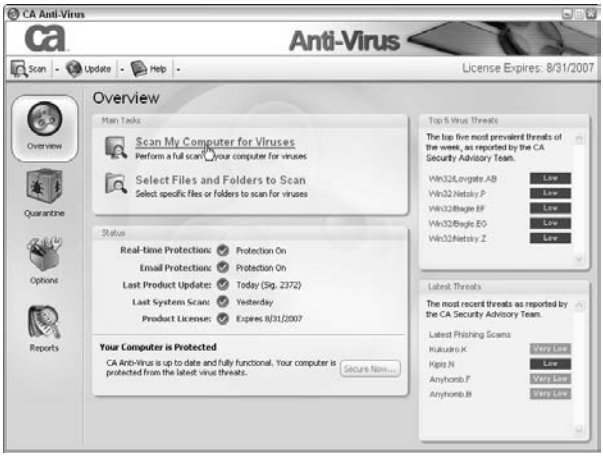

Figure 6-13: Opening the virus scanner

The Scan window appears, as shown in Figure 6-14.

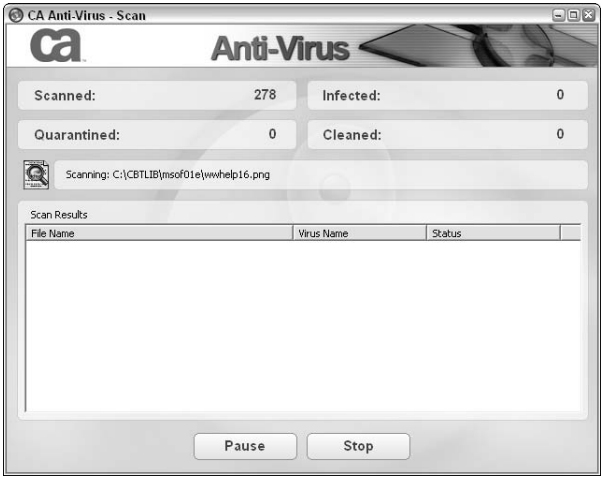

Figure 6-14: The Scan window

3. Use the Scan window to stop, pause, resume, or exit scanning if required.

CA Anti-Virus scans your computer for viruses and displays the results during the scan. Results are also displayed at the end of the scan and published to the On-demand Scanner log.

Perform a Partial On-demand Virus Scan

You can perform a virus scan on particular files or folders that you specify by following these steps:

1. Select the Overview tab on the left side of the CA Anti-Virus window.

   The Overview window appears.

2. Click Select Files and Folders to Scan, as shown in Figure 6-15 in the Main Tasks area.

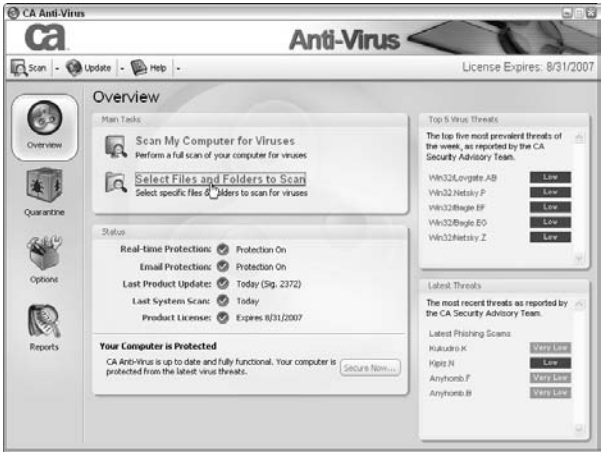

Figure 6-15: Opening the virus scanner

The Select Files and Folders to Scan window appears, shown in Figure 6-16.

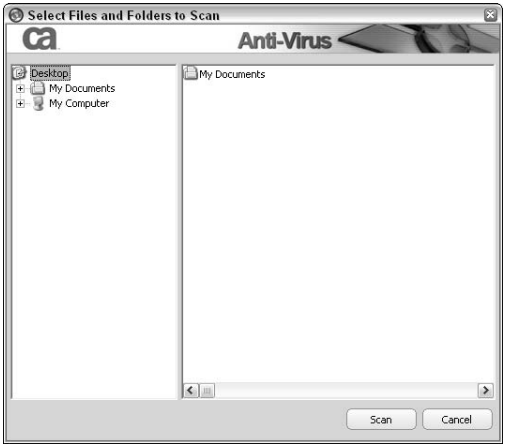

Figure 6-16: Select Files and Folders to Scan window

3. Select the files or folders you want to scan, on the right side of the window.

   You can browse through your PC by clicking through the items on the left side of the window and use the + sign to expand directories.

Note

You can choose individual files and folders within the selected directory by holding the CTRL key and clicking the items on the right that you want to scan.

4. Click Scan to begin scanning your selections.

   CA Anti-Virus scans your selections for viruses and displays the results during the scan. Results are also displayed at the end of the scan and published in the On-demand Scanner log.

Turn Real-Time Protection On or Off

Sometimes it is necessary to disable your Anti-Virus protection, such as when you're installing certain software or diagnosing computer problems. The following sections discuss the methods you can use to deactivate real-time protection.

Enable Snooze

You can use the Snooze option to temporarily disable real-time protection by following these steps (this is recommended over actually disabling it because Snooze automatically resumes protection):

Important!

Disabling real-time protection leaves your system vulnerable to virus infection.

1. Right-click the CA Security Center system tray icon on the lower right side of your screen.

   The list of menu items appears, as Figure 6-17 shows.

2. Select CA Anti-Virus.

   The CA Anti-Virus sub-menu appears.

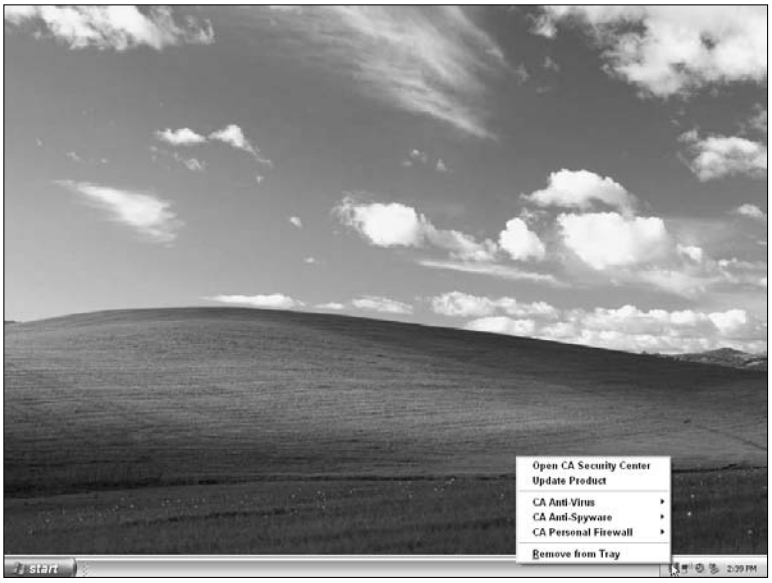

Figure 6-17: Right-clicking the System Tray icon

3. Select Snooze CA Anti-Virus Protection, as shown in Figure 6-18.

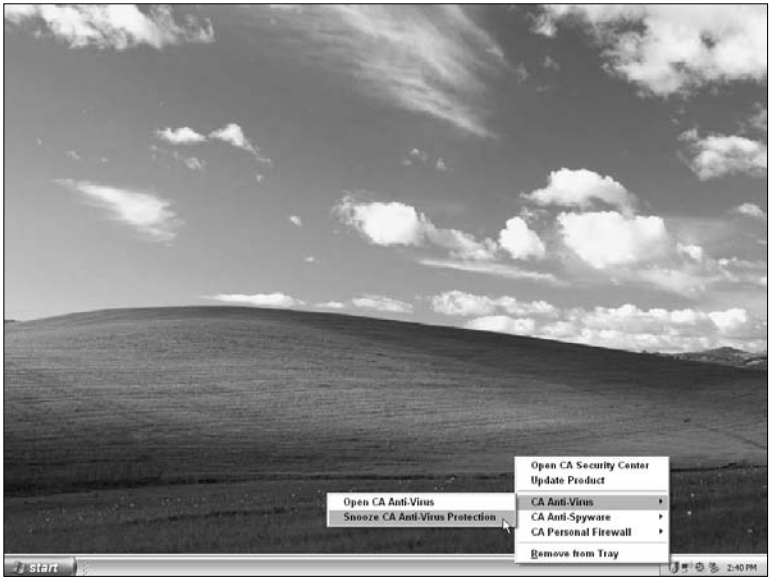

Figure 6-18: Snoozing anti-virus protection

The Snooze CA Anti-Virus Protection window appears.

4. Enter the number of minutes (1–999) for which you want to snooze your protection and then click Snooze, as shown in Figure 6-19.

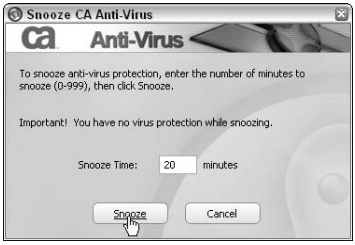

Figure 6-19: Specifying snooze time for anti-virus protection

Awake from Snooze

You can manually awake real-Time protection from sleep:

1. Right-click CA Security Center System Tray Icon on the lower right side of your screen.

   The list of menu items appears, as Figure 6-20 shows.

Figure 6-20: Right-clicking the System Tray icon

2. Select CA Anti-Virus.

   The CA Anti-Virus sub-menu appears.

3. Select Snooze CA Anti-Virus Protection, as shown in Figure 6-21.

Figure 6-21: Snoozing anti-virus protection

   The Snooze CA Anti-Virus Protection window appears.

4. Click Wake Now, as shown in Figure 6-22.

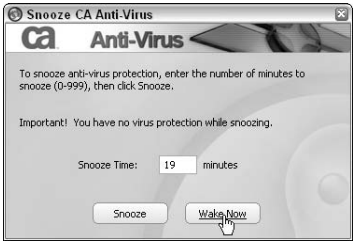

Figure 6-22: Awaking anti-virus protection from a snooze

Note

When real-time protection is in Snooze mode, it can also be enabled by selecting the Secure Now or Enable Now link located in the Overview window.

Enable the Real-time Scanner

To allow CA Anti-Virus to actively scan files in the background as they are accessed, you can enable the Real-time Scanner:

Note

The Real-time Scanner is enabled by default.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Select the Enable checkbox in the Real-time Scanner row, as shown in Figure 6-23.

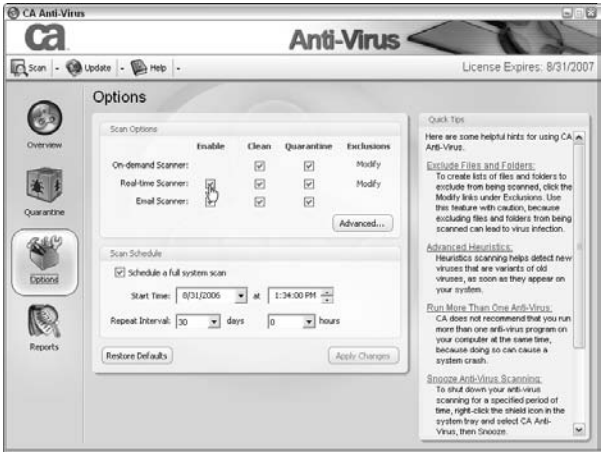

Figure 6-23: Enabling the Real-time Scanner

   The Real-time Scanner is configured to be enabled, but not active.

3. Click the Apply Changes button, as shown in Figure 6-24.

   The changes are applied and saved, and the Real-time Scanner is now active.

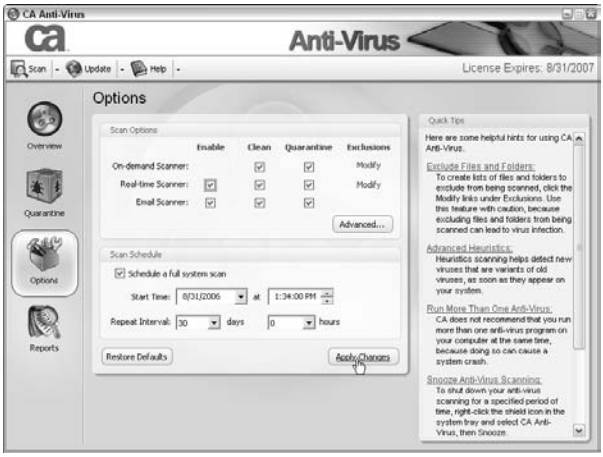

Figure 6-24: Applying option changes

Disable the Real-time Scanner

To prevent CA Anti-Virus from actively scanning files as they are accessed, you can disable the Real-time Scanner as follows:

Important!

Disabling real-time protection leaves your system vulnerable to virus infection.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Uncheck the Enable check box in the Real-time Scanner row, as shown in Figure 6-25.

   The Real-time Scanner will be disabled when changes are applied.

3. A warning message will appear. Click Yes to continue.

4. Click Apply Changes, as shown in Figure 6-26.

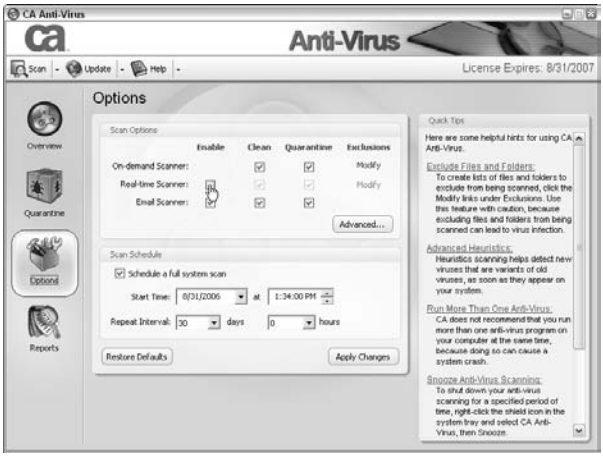

Figure 6-25: Disabling the Real-time Scanner

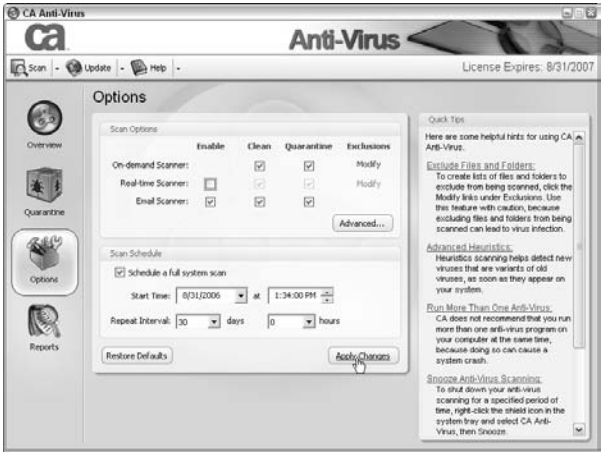

Figure 6-26: Applying option changes

The changes are applied and saved, and the Real-time Scanner is no longer active.

Enable the Real-time Email Scanner

To allow CA Anti-Virus to actively scan emails as they are delivered to your Inbox, you can enable the Real-time Email Scanner:

Note

The Real-time Email Scanner is enabled by default.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Select the Enable check box in the Email Scanner row, as shown in Figure 6-27.

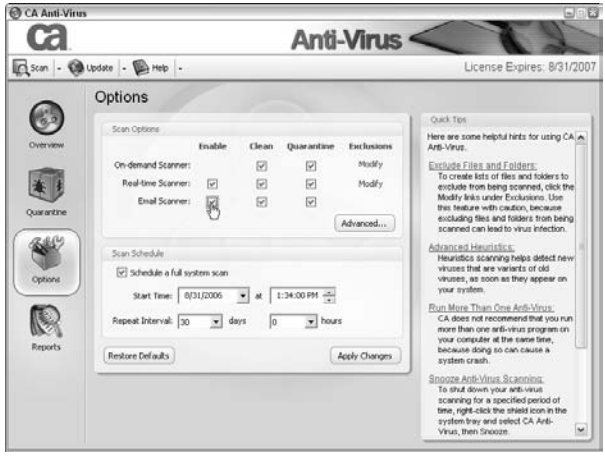

Figure 6-27: Enabling the Real-time Email Scanner

The Real-time Email Scanner is configured to be enabled, but not active.

3. Click Apply Changes, as shown in Figure 6-28.

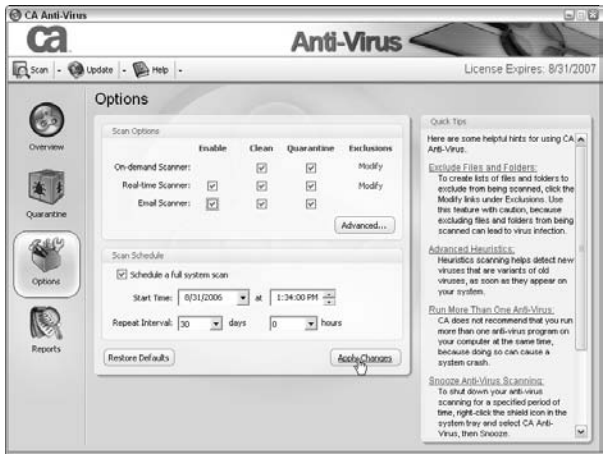

Figure 6-28: Applying option changes

The changes are applied and saved, and the Real-time Email Scanner is now active.

Disable the Real-time Email Scanner

To prevent CA Anti-Virus from actively scanning emails as they are delivered to your Inbox, you can disable the Real-time Email Scanner as follows:

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Uncheck the Enable check box in the Email Scanner row, as shown in Figure 6-29.

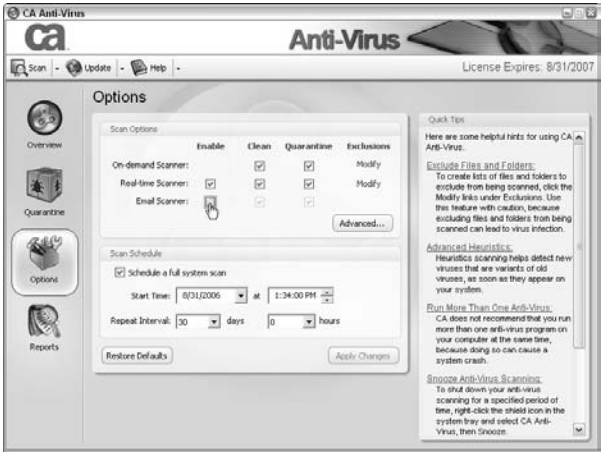

Figure 6-29: Disabling the Real-time Email Scanner

   The Real-time Email Scanner will be disabled when changes are applied.

3. Click Apply Changes, as seen in Figure 6-30.

   The changes are applied and saved, and the Real-time Email Scanner is now disabled.

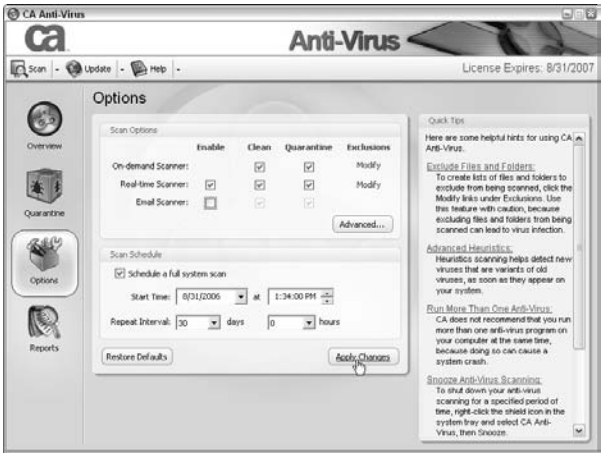

Figure 6-30: Applying option changes

Schedule Automatic Scans

To scan your computer at a regular interval that is convenient for you, you can run a scheduled scan:

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Select the Schedule A Full System Scan check box, as shown in Figure 6-31.

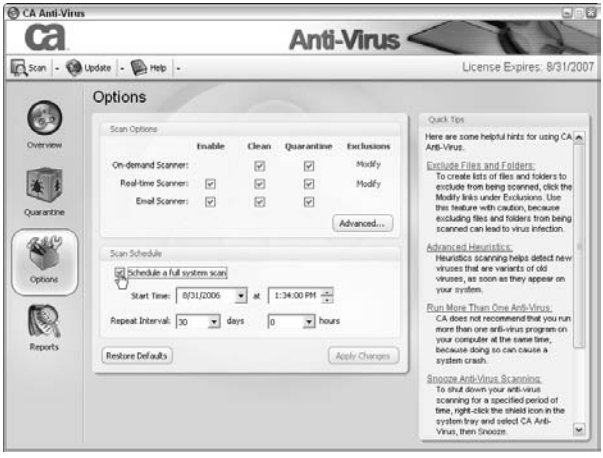

Figure 6-31: Scheduling a full-system scan

The scheduled scan is configured to be enabled.

3. Specify the start date/time and interval, as shown in Figure 6-32.

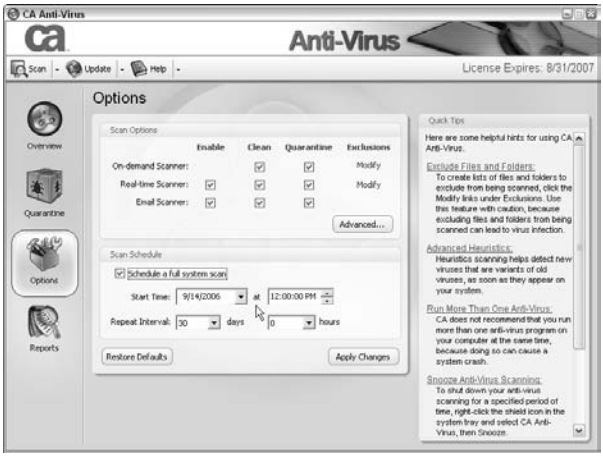

Figure 6-32: Specifying scheduled scan settings

4. Click Apply Changes, as seen in Figure 6-33.

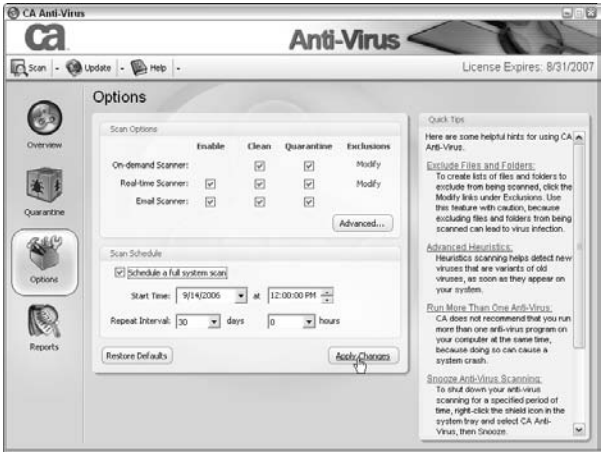

Figure 6-33: Applying option changes

Your changes are applied and saved.

Advanced Tasks

This section provides step-by-step instructions for advanced tasks relating to CA Anti-Virus.

Exclude Files and Folders from Virus Scanning

When necessary, you can exclude certain files or folders from being scanned for viruses — for instance, if problems arise in certain files that trigger a "false detection."

Add Files or Folders to the On-demand Scanner Exclusion List

Follow these steps to exclude files and/or folders from the On-demand Scanner:

Important!

If you do not have a specific reason to use the Exclusion List, we recommend that you do not experiment with it. Excluding files and folders from being scanned can lead to virus infection.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Click Modify in the On-demand Scanner row, as shown in Figure 6-34.

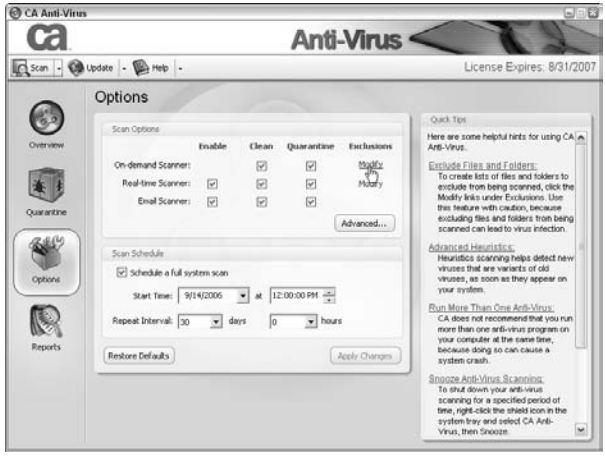

Figure 6-34: Accessing the On-demand Scanner Exclusion List

The On-demand Scanner Exclusions window opens.

3. Click Add.

   The Exclusion List Entry window appears.

4. Enter the path and name of the file or folder (see Figure 6-35 for an example) that you want to exclude from the scan.

Figure 6-35: Adding to the On-demand Scanner Exclusion List

Note

You can use the Browse button to exclude an entire folder or use wildcards to exclude an entire group of files. For example, to use a wildcard to exclude all .doc files, you can enter *.doc into the Exclusions: field.

   The name of the entry appears in the Exclusion List Edit Entry window.

5. Click OK.

   The Exclusion List is configured, and the entries listed are not scanned by the On-demand Scanner.

Edit the On-demand Scanner Exclusion List

You can modify the On-demand Scanner Exclusion List by following these steps:

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Click Modify in the On-demand Scanner row, as shown in Figure 6-36.

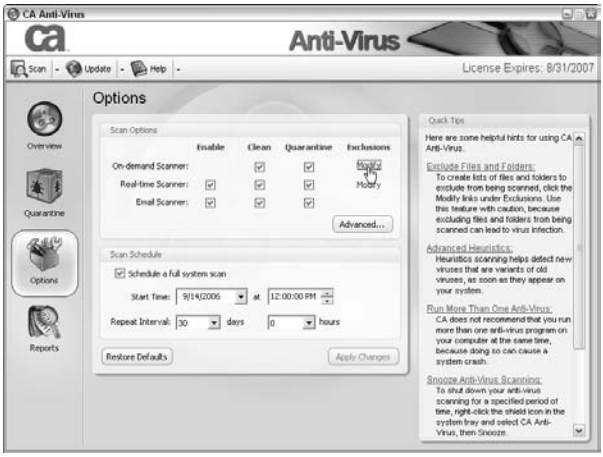

Figure 6-36: Accessing the On-demand Scanner Exclusion List

The On-demand Scanner Exclusions window opens.

3. Continue with the next steps depending upon if you're editing or removing an entry.

To edit an entry:

a. Select the entry that you want to edit.

b. Click Edit.

The Exclusion List Entry window appears.

c. In the Exclusion List Entry window, edit your entry in the field provided or use the Browse button to make the desired change (see Figure 6-37 for an example), and click OK.

Figure 6-37: Editing an On-demand Scanner Exclusion Item

The exclusion list is configured and the edited entries listed are not scanned by the On-demand Scanner.

To remove an entry:

a. Select the entry that you want to remove.

b. Click Delete.

The entry is removed from the Exclusion List.

Add Files or Folders to the Real-time Scanner Exclusion List

Follow these steps to exclude files and/or folders from the Real-time Scanner:

Important!

If you do not have a specific reason to use the Exclusion List, we recommend that you do not experiment with it. Excluding files and folders from being scanned can lead to virus infection.

1. Select the Options tab on the left side of the CA Anti-Virus window.

The Options window appears.

2. Click Modify in the Real-time Scanner row, as shown in Figure 6-38.

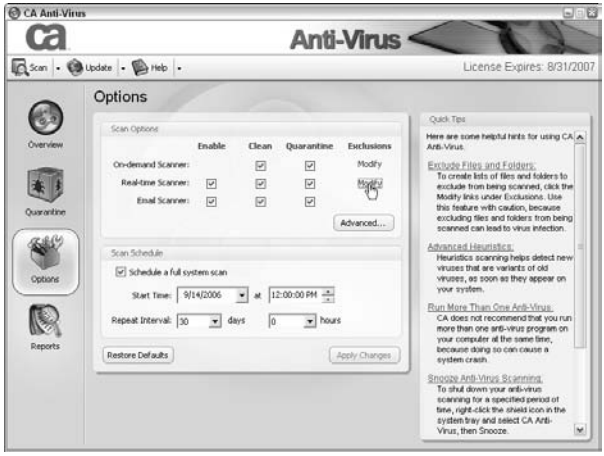

Figure 6-38: Accessing the Real-time Scanner Exclusion List

The Real-time Scanner Exclusions window opens.

3. Click Add.

The Exclusion List Entry window appears.

4. Enter the path and name of the file or folder that you want to exclude from the scan, as shown in Figure 6-39.

Figure 6-39: Adding to the Real-time Scanner Exclusion List

Note

You can use the Browse button to exclude an entire folder or use wildcards to exclude an entire group of files. For example, to use a wildcard to exclude all .doc files, you can enter *.doc into the Exclusions: field.

The name of the entry appears in the Exclusion List Edit Entry window.

5. Click OK.

The Exclusion List is configured, and the entries listed are not scanned by the Real-time Scanner.

Edit the Real-time Scanner Exclusion List

You can modify the Real-time Scanner Exclusion List by following these steps:

1. Select the Options tab on the left side of the CA Anti-Virus window.

The Options window appears.

2. Click Modify in the Real-time Scanner row, as shown in Figure 6-40.

The Real-time Scanner Exclusions window opens.

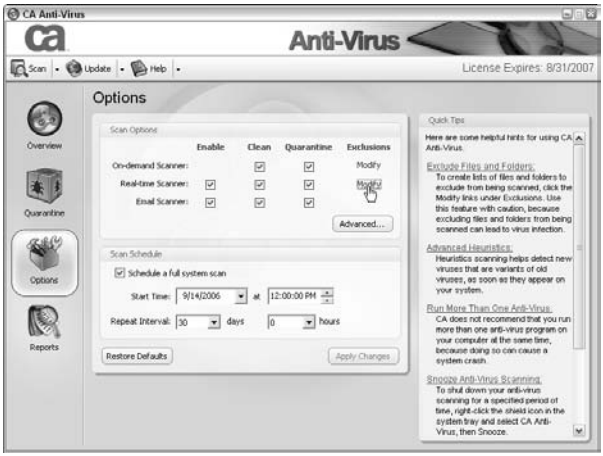

Figure 6-40: Accessing the Real-time Scanner Exclusion List

3. Continue with the next steps depending upon if you're editing or removing an entry.

To edit an entry:

a. Select the entry that you want to edit.

b. Click Edit.

The Exclusion List Entry window appears.

c. Edit your entry in the field provided or use the Browse button to make the desired change (see Figure 6-41 for an example), and click OK.

Figure 6-41: Editing a Real-time Scanner Exclusion Item

The Exclusion List is configured and the edited entries listed are not scanned by the Real-time Scanner.

To remove an entry:

a. Select the entry that you want to remove.

b. Click Delete.

The entry is removed from the Exclusion List.

Working with Quarantined Items

This section discusses the common tasks relating to quarantined items.

View Your Quarantined Items

To display a list of files or emails that have been quarantined, follow these steps:

1. Select the Quarantine tab on the left side of the CA Anti-Virus window.

   The Quarantine window appears, as seen in Figure 6-42.

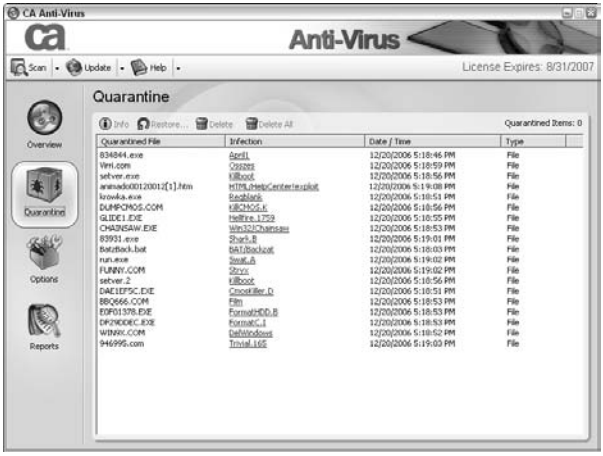

Figure 6-42: Quarantine window

2. Click the headings at the top of the quarantined items to sort them by Quarantined File, Infection, Date/Time, Type, File Location, or More Information.

If you want to view the details of quarantined files, do the following:

1. Double-click the file you want to obtain more information about.
2. The File Information window appears, as shown in Figure 6-43.

Figure 6-43: File Information window

This window displays the following information:

- **Filename:** The name of the file detected.
- **Location:** The path the file was stored in prior to being detected.
- **Date and Time:** The date and time the detection was made.
- **Infection:** The name of the virus infection.
- **Type:** File or email.
- **Status:** A status of Quarantined is displayed.
- **Engine Version:** The version of the antivirus scanning engine used to make the detection.
- **Signature:** The number of the signature file used to make the detection.
- **Scanner Type:** The type of scanner used to make the detection. This can be on-demand or real-time.

Delete Items

To remove unwanted quarantined items from your computer, you can delete a selection of items or all items from the quarantined list:

1. Select the Quarantine tab on the left side of the CA Anti-Virus window.

   The Quarantine window appears, as shown in Figure 6-44.

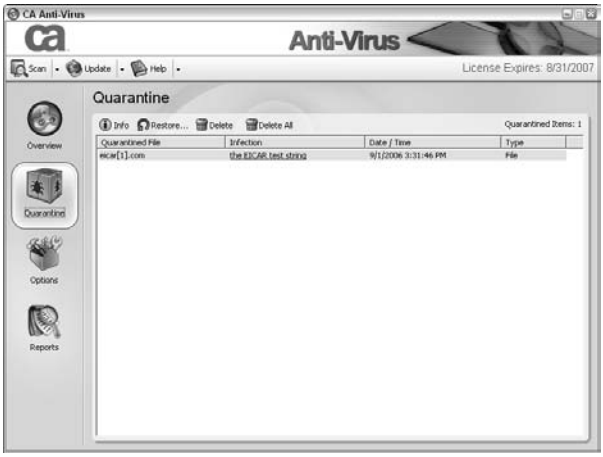

Figure 6-44: Quarantine window

To delete a selection of items:

a. Select the item(s) that you want to delete.

Note
To select multiple items hold down the CTRL key and then use the mouse to select the items.

b. Click Delete, as shown in Figure 6-45.

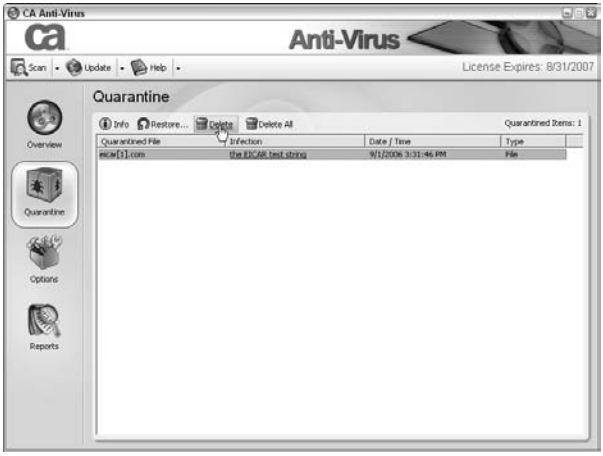

Figure 6-45: Deleting quarantined items

The selected items are deleted.

To delete all items:

a. Click Delete All, as seen in Figure 6-46.

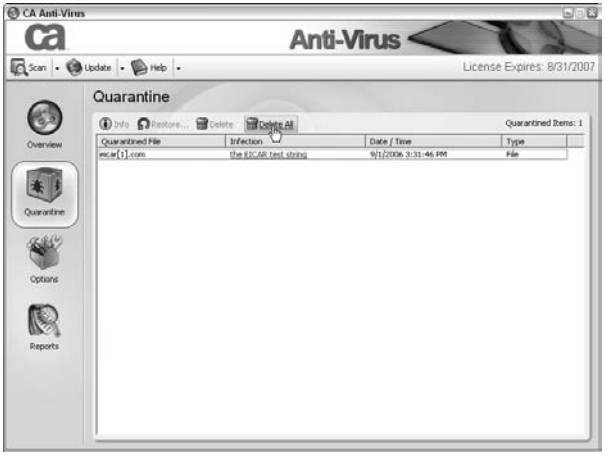

Figure 6-46: Deleting all quarantined items

The Confirm Remove window appears.

b. Click Yes.

All quarantined items are deleted.

Restore Items

To revoke the quarantining of selected items, you can restore selected quarantined items to their original location.

1. Select the Quarantine tab on the left side of the CA Anti-Virus window.

The Quarantine window appears, as seen in Figure 6-47.

2. Select the item or items that you want to restore to the original location.

Note

To select multiple items, hold down the CTRL key and then using the mouse to select the items.

The selected items are highlighted.

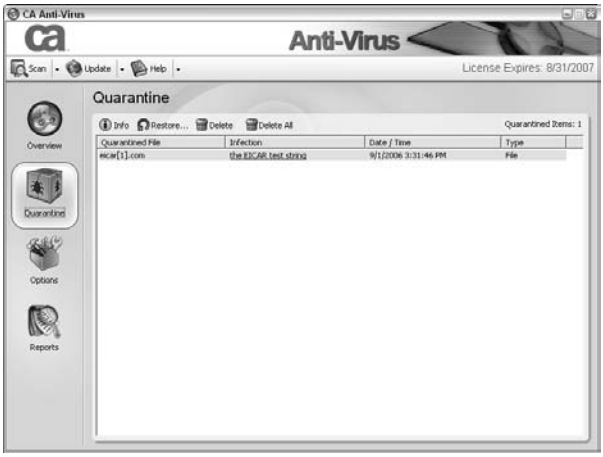

Figure 6-47: Quarantine window

3. Click Restore, as shown in Figure 6-48.

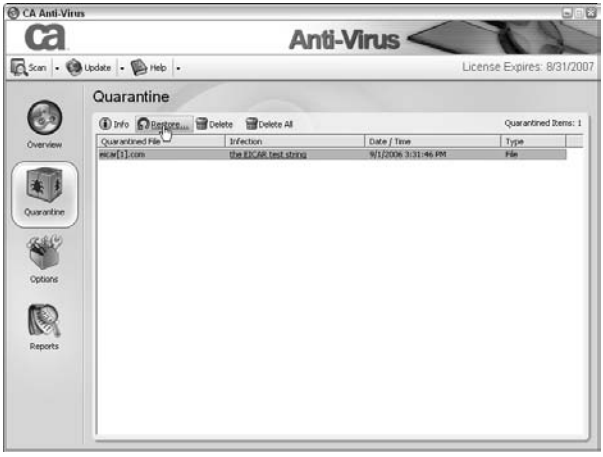

Figure 6-48: Restoring quarantined items

The Restore Infected File window appears.

4. Click OK to accept the default folder to restore the file to, or click Browse to choose a new location.

Note

If you want CA Anti-Virus to attempt to clean the file during the restore process, click the Attempt To Clean The Infected File check box before clicking OK.

The selected items are restored to their original or chosen location.

Enable or Disable Automatic Quarantine

If it becomes necessary, you can disable or enable the automatic quarantine of detected infections, for each type of scanning method.

On-demand Scanning

To allow or disable CA Anti-Virus to automatically quarantine all infections that are detected by the On-demand Scanner, you can enable or disable the scanner's Quarantine option.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the On-demand Scanner row, check or uncheck the Quarantine box (see Figure 6-49).

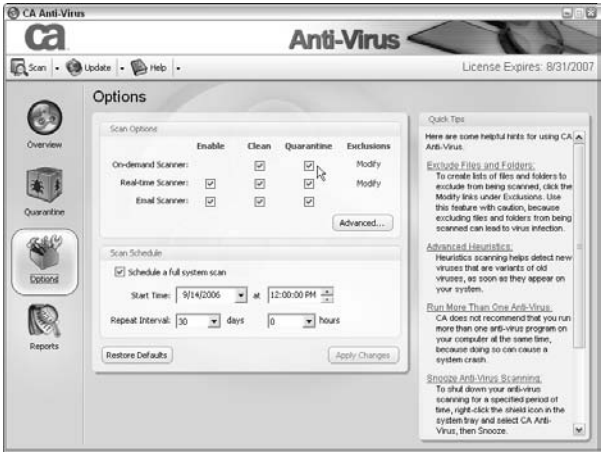

Figure 6-49: The Quarantine check box

3. Click Apply Changes.

   Your changes are applied and saved.

Real-time Scanning

To allow or disable CA Anti-Virus to automatically quarantine all infections that are detected by the Real-time Scanner, you can enable or disable the scanner's Quarantine option.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Real-time Scanner row, check or uncheck the Quarantine box (see Figure 6-50).

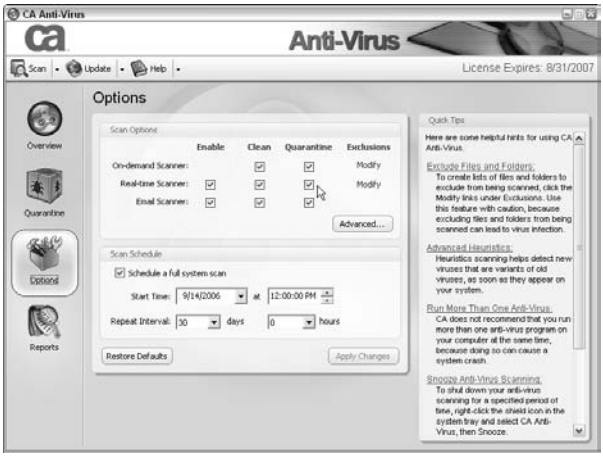

Figure 6-50: The automatic quarantine check box

3. Click Apply Changes.

   Your changes are applied and saved.

Real-time Email Scanning

To allow or disable CA Anti-Virus to automatically quarantine all infections that are detected by the Real-time Email scanner, you can enable or disable the scanner's Quarantine option.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Email Scanner row, check or uncheck the Quarantine box (see Figure 6-51).

3. Click Apply Changes.

   Your changes are applied and saved.

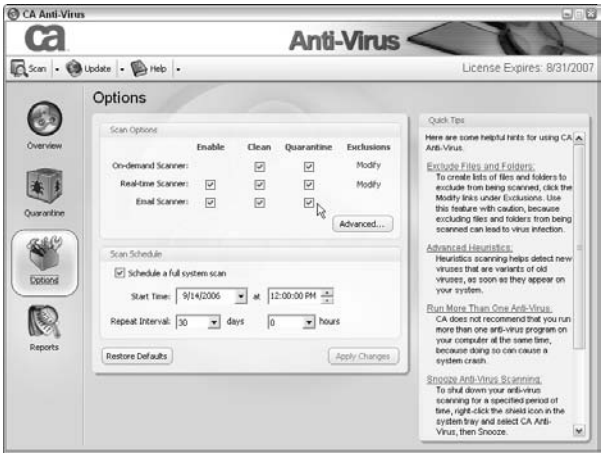

Figure 6-51: The quarantine check box

Enable or Disable Additional Scanning Methods

You may need to disable the advanced scanning methods of your Anti-Virus protection for some reason, such as when you're diagnosing computer problems or when a problem arises with the scanning method.

Note

These scanning methods are enabled by default.

On-demand Heuristic Scanning

To allow or prevent CA Anti-Virus to use heuristic on-demand scanning methods, you can enable or disable the Heuristic Scan option for the On-demand Scanner.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Scan Options section, click the Advanced button, as shown in Figure 6-52.

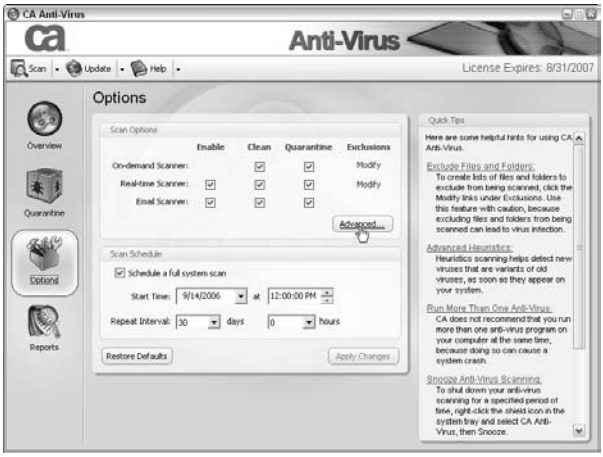

Figure 6-52: Opening advanced scanning options

The Advanced Options window appears.

3. In the Advanced On-demand Scanning Options section, check or uncheck the Use Advanced Heuristic Scanning box (see Figure 6-53).

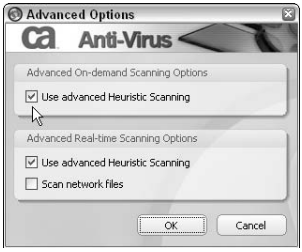

Figure 6-53: The Use Advanced Heuristic Scanning check box

4. Click OK.

   The Advanced Options window closes.

5. Click Apply Changes.

   Your changes are applied and saved.

Real-time Scanner Heuristic Scanning

To allow or disallow CA Anti-Virus to use heuristic real-time scanning methods, you can enable or disable the Heuristic Scan option for the Real-time Scanner.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Scan Options section, click the Advanced button, as shown in Figure 6-54.

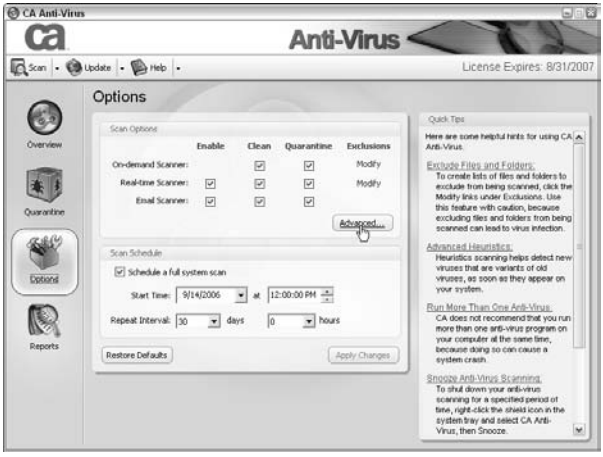

Figure 6-54: Opening advanced scanning options

3. In the Advanced Real-time Scanning Options section, check or uncheck the Use Advanced Heuristic Scanning box (see Figure 6-55).

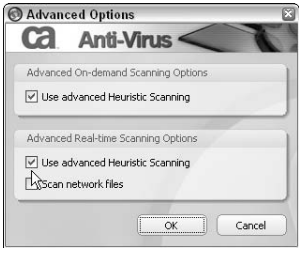

Figure 6-55: The Use Advanced Heuristic Scanning check box

4. Click OK.

   The Advanced Options window closes.

5. Click Apply Changes.

   Your changes are applied and saved.

Network File Scanning

To allow CA Anti-Virus to scan files in real-time as they are accessed over a network, you can enable the Scan Network Files option for the Real-time Scanner.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Scan Options section, click the Advanced button, as shown in Figure 6-56.

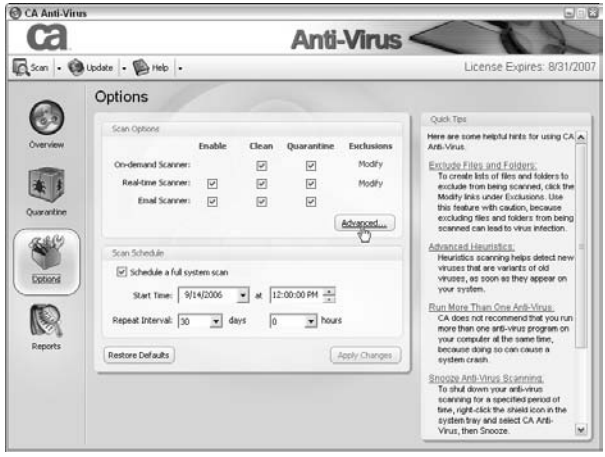

Figure 6-56: Opening advanced scanning options

   The Advanced Options window appears.

3. In the Advanced Real-time Scanning Options section, check or uncheck the Scan Network Files box (see Figure 6-57).

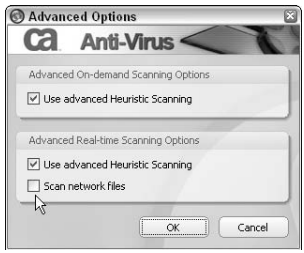

Figure 6-57: The Scan Network Files check box

4. Click OK.

   The Advanced Options window closes.

5. Click Apply Changes.

   Your changes are applied and saved.

Enable or Disable Virus Cleaning Methods

If it becomes necessary, you can disable or enable the automatic cleaning of detected infections, for each type of scanning method.

On-demand Scanning

To allow or disallow CA Anti-Virus to automatically clean infections that are detected while running an on-demand scan, you can enable or disable cleaning for the On-demand Scanner.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the On-demand Scanner row, check or uncheck the Clean box, as shown in Figure 6-58.

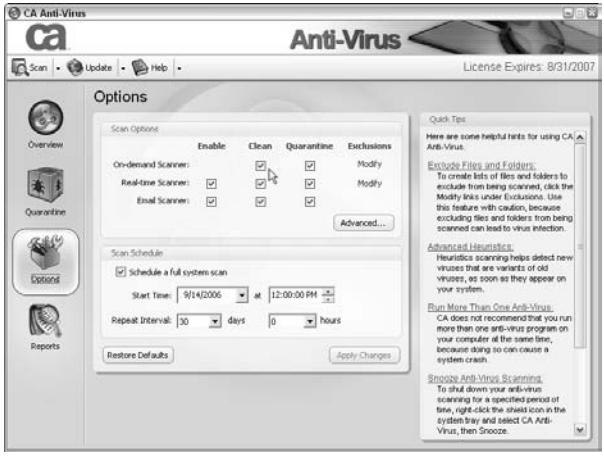

Figure 6-58: The Clean check box

3. Click Apply Changes.

   Your changes are applied and saved.

Real-time Scanning

To allow or disallow CA Anti-Virus to automatically clean infections that are detected by the Real-time Scanner, you can enable or disable cleaning.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Real-time Scanner row, check or uncheck the Clean check box, as shown in Figure 6-59.

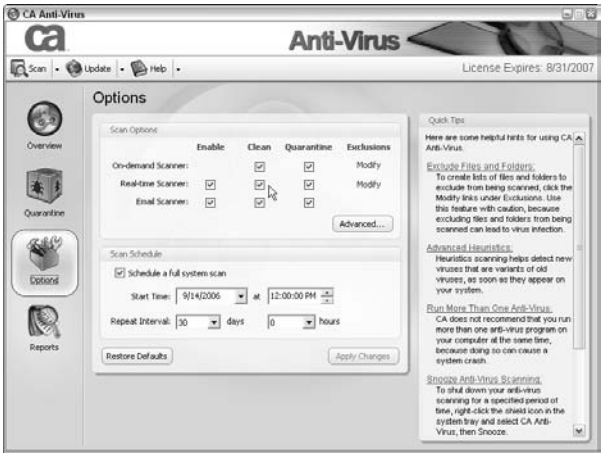

Figure 6-59: The Clean check box

3. Click Apply Changes.

   Your changes are applied and saved.

Real-time Email Scanning

To allow or disallow CA Anti-Virus to automatically clean infections that are detected by the Real-time Email Scanner, you can enable or disable cleaning for the Real-time Email Scanner.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. In the Email Scanner row, check or uncheck the Clean check box, as shown in Figure 6-60.

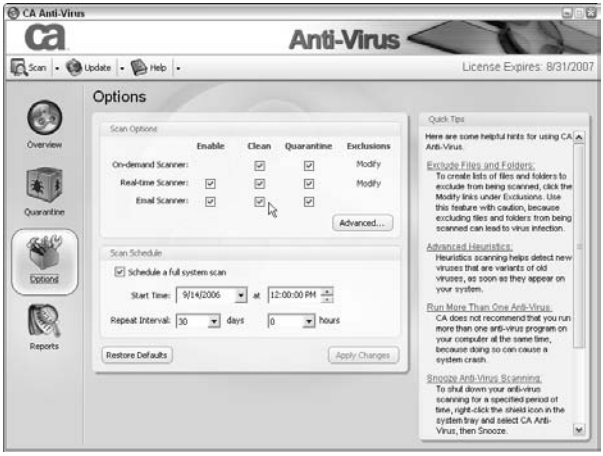

Figure 6-60: The Clean check box

3. Click Apply Changes.

   Your changes are applied and saved.

Restore Scan Settings Defaults

To reset your scan options to their default settings, you can use the Restore Defaults feature.

1. Select the Options tab on the left side of the CA Anti-Virus window.

   The Options window appears.

2. Click Restore Defaults in the Scan Options section, as shown in Figure 6-61.

   The scan settings are reset to the default settings.

3. Click Apply Changes.

Your changes are applied and saved.

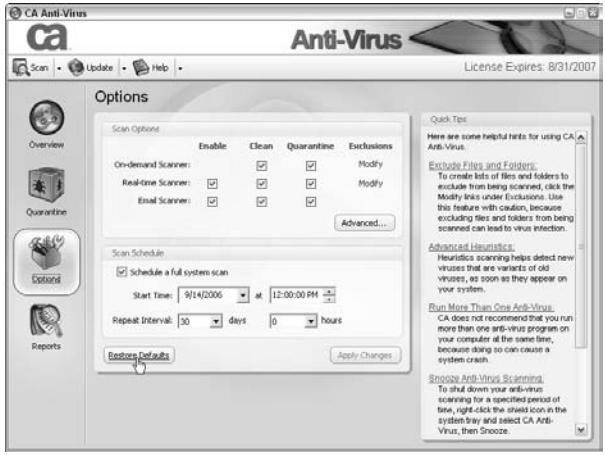

Figure 6-61: Restoring the scanning settings defaults

7

STOPPING HACKERS FROM ATTACKING YOUR PC

The firewall component of CA Internet Security Suite, which is CA Personal Firewall, protects your personal information and PC by stopping hacker attacks, monitoring your email for suspicious attachments, and more, all of which protects you from identity theft.

This chapter is organized into these main sections:

- **Firewall and Protection Methods**

  You can learn about some of the methods used in CA Personal Firewall.

- **CA Personal Firewall Introduction**

  This section takes you through all the screens of CA Personal Firewall, which lets you know where everything is located and what it does.

- **Common Tasks**

  This section provides step-by-step directions for common tasks relating to the firewall component.

- **Advanced Tasks**

  This section provides step-by-step directions for tasks typically less commonly performed.

Firewall and Protection Methods

As mentioned in Chapter 5, a firewall such as CA Personal Firewall acts as a gate between your PC and the Internet. All information passing through the gate must be authorized, as shown in Figure 7-1, which ultimately helps keep hackers and intruders away from your personal and confidential data.

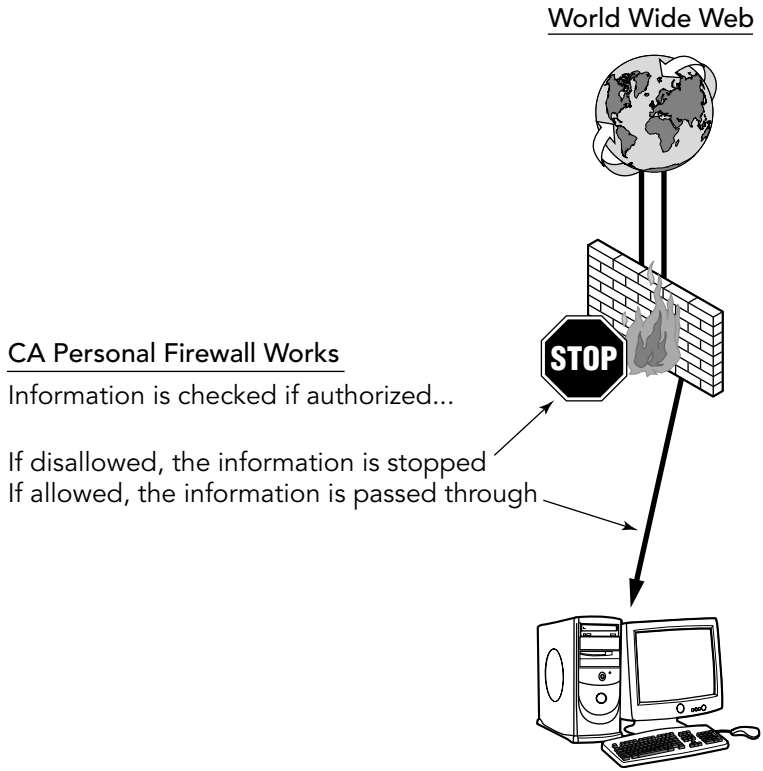

Figure 7-1: Example of a personal firewall

The following sections discuss the methods used by CA Personal Firewall.

Authorization Methods

There are basically two ways you can give authorization to information in order to pass through CA Personal Firewall, or the gate:

- **Pop-up Alerts**

  CA Personal Firewall uses pop-up alerts to inform you of certain situations, such as when an application is trying to access the Internet and its access privileges haven't been assigned yet. When an alert is displayed, as shown in Figure 7-2, you can either allow access or deny it.

Figure 7-2: Example of an application pop-up alert

Another type of alert you'll probably receive, as Figure 7-3 shows, will be about assigning a newly discovered network adapter to one of the zones, which are discussed in the next section.

Figure 7-3: Example of a network adapter pop-up alert

- **Manual**

  You can also manually add (or remove) applications and the protocols and ports associated with them to the CA Personal Firewall application list, such as Figure 7-4 shows. The list allows you specify much more specific rules and conditions for each of your applications.

Figure 7-4: Example of where to manually give authorization

The Firewall Zones

CA Personal Firewall uses Firewall Zones to categorize areas of local networks and the Internet that you are exposed to.

The following zones are used by the firewall:

- **Safe Zone**

  You would assign this zone to a part of the network that you trust. The network traffic that occurs in this zone is considered to be safe.

- **Restricted Zone**

  This zone is used for computers and networks that are not trusted. All traffic in this zone is blocked by default. When an access attempt is made from a certain application it is logged so that you may review it later.

- **Unassigned Zone**

  This is a default zone that is used for interfaces that have not been assigned. There is no access permitted for interfaces categorized in the Unassigned zone.

These zones are pre-configured with certain settings, such as protocols and ports which are authorized on the selected local network or Internet, based upon the zone type chosen. You can change the configuration to allow different types of access for the items contained within each zone.

Application Control

Application Control lets you monitor and control the local network and Internet access of the applications that are installed on your computer. You can perform the following tasks for each installed application:

- Control the access that each application has to the local network or Internet.
- Control the access of applications that attempt to act as servers, such as file sharing programs and other applications that allows incoming connections.
- Control the access that each application has for sending email.

Identity Theft and My Safe

It's likely that you have personal information on your computer that should be kept private to avoid identity theft, fraud, or other misconduct.

One form of personal or private information is commonly overlooked, which is the information collected by your Internet browser and Windows operating system when you use the Internet, such as:

- Internet and document history
- Temporary files
- AutoComplete forms and passwords

Hackers can attempt to steal your identity and personal information by using malicious software to copy your data, or attempt to connect to your computer and view or manipulate your data. If your computer is used by other users, hackers can potentially find your sensitive information if it is not kept safe. However, you can use the Cache Cleaner feature, which is discussed later, to clean up this type of personal information.

It's likely you also have private documents on your PC that contain very sensitive information, such as:

- Passwords used to access various restricted websites, or other computers.

- Credit card details and bank account numbers used to conduct financial transactions.
- Private numbers including Social Security numbers, passport numbers, and phone numbers.

A feature in CA Personal Firewall, called My Safe, can protect your personal information by storing it safely and using a password to protect it. If you ensure that your personal information is only kept in My Safe, it will not be exposed to unauthorized viewing or use.

My Safe allows you to create entries for information that you want to keep private, and then determine if this information should be available to specific websites that are considered trusted or un-trusted. You can also set My Safe security to ask you before allowing the data out to the Internet (in medium protection) or block the information automatically (in high protection). Additionally, you can block your defined private data from being used in emails.

Here are examples of items that you can store in My Safe:

- Access PINs
- Addresses
- Banking account information
- Passport number
- Passwords
- Phone numbers

Email Protection

Certain email attachments you receive in your mailbox are a potential threat to your computer's security if they contain malicious programs such as viruses. In addition, certain security threats can use your email account to send viruses or spam without your authorization.

The Email Protection feature in CA Personal Firewall lets you quarantine potentially malicious email attachments, prevent mass-mailing email worms, and safeguard your email. You can set CA Personal Firewall to automatically rename with a new extension potentially dangerous attachments that are received in your mailbox to prevent opening or execution of the infected attachment. You can also block email from being sent from your email account based on a set of defined options.

Mobile Code Protection

Although usually safe, mobile code can pose a risk to your PC and is typically overlooked by the majority of computer users. CA Personal Firewall provides the ability to block several common types of mobile code. Mobile code is scripts that can be stored remotely and accessed over a network, such as the Internet, then executed on your computer.

Here are a few examples of mobile code:

- JavaScript
- VBScript
- ActiveX controls
- Java applets

These types of items can pose a security risk if they're executed from a distrusted remote site and can cause malicious activity. These types of mobile code can also be completely safe and are used often by most computer users. Web sites often contain these mobile codes to provide interactive menus, pop-up windows, display videos, and web applications such as stock tickers and online calculators.

Security issues that can occur due to the use of mobile code include gaining access to confidential information, denial of service, and destruction or modification of data. In addition, Mobile Code is typically used by adware and spyware vendors. For example, a user would be browsing a webpage and mobile code would automatically download and run on their system installing some sort of adware or spyware.

Expert Firewall Rules

Expert rules let advanced users have greater control over access to applications, local network, and Internet resources that are specified in the rules.

Rules can be established to allow, block, or ask for access for specific network protocols, ports, and IP addresses. You can configure rules to run continually or at specific times. You can enable auditing to provide you with an alert or log of access attempts to configured items specified in the rules. You can select from a list of well-known protocols using pre-determined ports, or add your own ports, protocols, and IP addresses to base rules on.

Here are examples of protocols that you can configure with expert rules:

- **HTTP Out**

  Refers to outbound HTTP requests. HTTP is the protocol used by computers that are connected to the Internet. For example, when a URL is typed into a browser address bar, the outbound HTTP request is made.

- **HTTPS Out**

  Refers to outbound HTTPS requests. HTTPS is the protocol used by web servers that require a secure connection. Examples include banking websites and secure internal company websites.

- **SMTP Out**

  Refers to outbound SMTP (Simple Mail Transfer Protocol) connections. This protocol is used to send email between computers.

- **POP3 Out**

  Refers to outbound POP3 (Post Office Protocol) connections. This protocol is used for the retrieval of email messages from an email server.

- **IMAP Out**

  Refers to outbound IMAP (Internet Message Access Protocol) connections. This protocol is used to access email stored on an email server.

- **Outlook All**

  Refers to connections made by Microsoft Outlook.

CA Personal Firewall Introduction

The CA Personal Firewall component and its screens are organized to allow quick access to the common functions and features. The following sections discuss the main screens of CA Personal Firewall, which are accessed through the appropriate tabs in the software.

Open CA Personal Firewall

There are a few ways to open CA Personal Firewall:

- **CA Security Center**

  You can quickly access CA Personal Firewall from the CA Security Center:

  1. Double-click on the system tray icon, as shown in Figure 7-5.

Figure 7-5: Double-clicking the System Tray icon

  2. Expand the CA Personal Firewall component panel; click on its arrow, icon, or name.
  3. Click Open Advanced Settings, as shown in Figure 7-6.

Figure 7-6: Opening CA Personal Firewall

- **System Tray Icon**

  You can also use the system tray icon to open CA Personal Firewall:

  1. Right-click on the system tray icon, as shown in Figure 7-7.

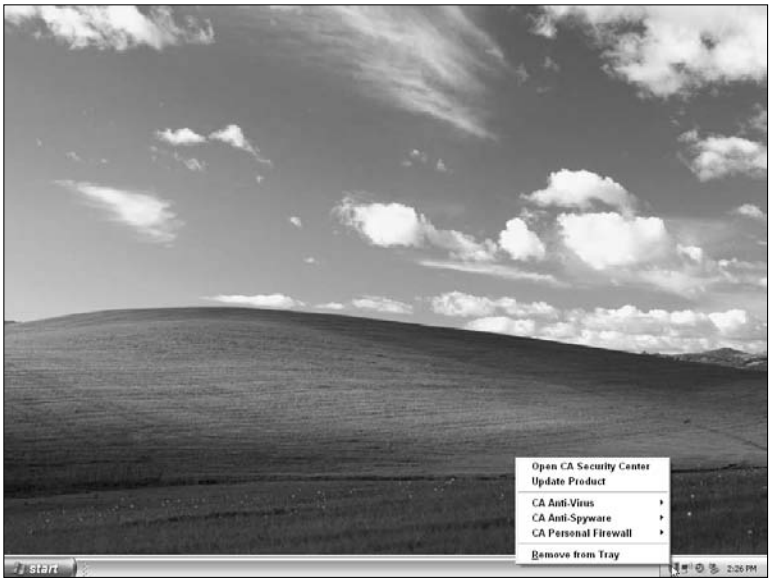

Figure 7-7: Right-clicking the System Tray icon

  2. Select CA Personal Firewall.
  3. Click Open CA Personal Firewall, as shown in Figure 7-8.

Figure 7-8: Opening CA Personal Firewall

- **Start Menu**

  If you have something against using the system tray icon and security center, or if the icon has disappeared, don't worry. Browse to the following path on your start menu:

  Programs (or All Programs) ➔ CA ➔ CA Internet Security Suite ➔ CA Personal Firewall

  Then click on CA Personal Firewall, as shown in Figure 7-9.

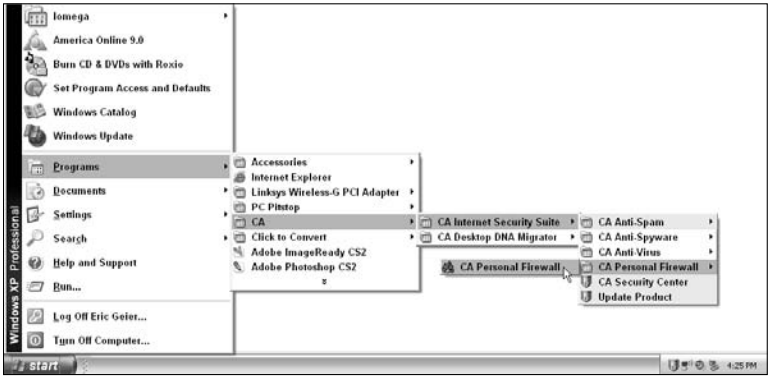

Figure 7-9: Opening CA Personal Firewall

Overview Screen

From this screen (see Figure 7-10) you can check the status of the product, fix any problems with the product, and view product statistics.

Figure 7-10: CA Personal Firewall Overview screen

In addition, the following two main tasks of CA Personal Firewall can be accessed on the Overview screen:

- **Block all Internet Access**

  You can quickly stop all Internet access by blocking all outbound and inbound traffic to the Internet. This may be useful if you are planning to leave your computer unattended, or if you suspect that there is malicious Internet activity occurring on your computer, for example, a virus infection or a hacking attempt.

- **Clean Cache**

  You can use the Clean Cache Now feature to clean your computer's common cache locations including the browser cache, and cached files stored on your hard disk. Using this feature regularly saves space on your hard disk, and removes private information including Internet usage information, document history, and saved passwords.

The following sections discuss the status area of the overview screen, as shown in Figure 7-11. Therefore, you'll understand exactly what the software is trying to tell you based all the different status indicators.

Figure 7-11: CA Personal Firewall status indicators

- **Firewall Protection Status**

  This field displays the status of your firewall protection. Here are all the possible status conditions:

  - **Protection On:** A checkmark indicates that firewall protection is enabled. The Safe and Restricted Zone protection levels are both set to medium or higher.
  - **Attention Needed:** An exclamation point indicates that your firewall protection needs attention. For this indication to occur, you would have to disable CA Personal Firewall from the system tray icon.
  - **Protection Off:** An X indicates that firewall protection is disabled. Either the Safe or Restricted Zone protection levels are switched off.

- **Privacy Protection Status**

  This field displays the status of your privacy protection. Here are all the possible status conditions:

  - **Protection On:** A checkmark indicates that privacy protection is enabled. The ID theft, Cookie Control and Ad/Pop-up blocker protection levels are set to medium or higher, and the cache cleaner is scheduled to run automatically.
  - **Attention Needed:** An exclamation point indicates that your privacy protection is using customized settings. The ID theft level is set to medium, the Cookie Control and Ad/Pop-up blocker levels are set to Custom.
  - **Protection Off:** An X indicates if one of the following is disabled:
    - Privacy protection
    - ID theft level
    - Cache cleaner

- Cookie control
- Ad/pop-up blocker

- **Email Protection Status**

  This field displays the status of your email protection. Here are all the possible status conditions:

  - **Protection On:** A checkmark indicates the email protection is enabled. Both inbound and outbound email protection is enabled.
  - **Attention Needed:** An exclamation point indicates that your Internet email protection needs attention. Either your inbound or outbound protection is disabled.
  - **Protection Off:** An X indicates the email protection is disabled. Inbound and outbound email protection is disabled.

- **Product License Status**

  This field displays the status of your product license. Here are all the possible status conditions:

  - **If your license is current:** A checkmark indicates that your license is current, and provides you with the expiration date.
  - **If your license is due to expire within 30 days:** An exclamation point indicates that your license will expire soon. The number of days left on your license is displayed.
  - **If your license is expired for more than 30 days:** An X indicates that your license has expired. A link will be available in this section to renew your license if it has expired.

Note

If your license has expired, or is close to expiration, a link is provided to renew your product license online.

Firewall Screen

The firewall screen (see Figure 7-12) is where you can manage the firewall software and lets you perform the following tasks:

Figure 7-12: CA Personal Firewall screen

- **Application Control**

  You can manage the access granted to applications on your computer. Using application control, you can assign specific access rights to applications, and control their access to the local network and Internet.

- **Define Zones**

  You can set protection levels for the Safe Zone and Restricted Zone. Setting protection levels lets you to restrict your computer and applications to a level of access and visibility of your choice. These protection levels are explained in detail in the topics mentioned below.

- **Customize Rules**

  Adding expert firewall rules allow you to control access to many types of protocols and specified IP addresses.

Application Control Tab

By default, CA Personal Firewall alerts you to all launched programs that attempt to use the local network or Internet — for example, browsers, download managers, or anti-virus software. When an alert is displayed, you can either allow the connection or refuse it. After making your selection in the alert pop-up window, the program that attempted to access the Internet is added to the list of applications in the Application Control window.

Note

You can also use the Application Control window to manually add applications for which you want to configure access to the local network or Internet.

The Application Control tab, as shown in Figure 7-13, contains the following items:

Figure 7-13: Application Control tab

- **Advanced Application Control**

  Provides a list of applications and the access that they have been granted. Using the following buttons and fields, you can add or delete programs from the list, and access rules settings for listed applications.

  - **Add:** Lets you add applications to the Application Control window.
  - **Edit:** Lets you edit the access for selected applications.
  - **Delete:** Lets you delete selected applications from the Application Control list.

- **Active**

  Indicates that the program is currently running.

- **Program Application**

  The name of the application.

- **Access**

  Shows the level of access the application has in the Safe Zone and Restricted Zone. Access refers to the application in question being permitted to use the local network, or Internet.

  Here are all the possible status conditions:

  - **Checkmark:** Indicates that access is granted.
  - **Stop Sign:** Indicates that access is denied.
  - **Question Mark:** Indicates that you will be asked whether you want to grant access when an application attempts to gain access.

- **Server**

  Shows the level of access for applications that are acting as servers in the Safe Zone and Restricted Zone. The Server setting refers to applications that require incoming connections. For example, if you wish to use a file sharing application that allows incoming connections, you will need to grant that application Server access.

  Here are all the possible status conditions:

  - **Checkmark:** Indicates that access is granted.
  - **Stop Sign:** Indicates that access is denied.
  - **Question Mark:** Indicates that you will be asked whether you want to grant access when an application attempts to gain access.

- **Send Mail**

  Shows the level of access for applications attempting to send email. A checkmark indicates that access is granted. A stop sign indicates that access is denied. A question mark indicates that you will be asked whether you want to grant access when an application attempts to gain access.

Zones Tab

The Zones Tab, as shown in Figure 7-14, contains the following items:

Figure 7-14: The Zones tab

- **Safe Zone Protection Level**

  The Safe Zone is a part of the network that you trust. The following Safe Zone protection levels are available:

  - **High:** All traffic is blocked unless you explicitly add rules to allow traffic. Your computer cannot be seen by hackers. Access to Windows NetBIOS services, and network file and printer sharing is blocked. Ports are blocked unless you have provided permission for a program to use them.
  - **Medium:** All traffic is allowed unless you explicitly add rules to block traffic. You are protected, but your computer is visible to others so that you can use network sharing. Access to Windows NetBIOS services and network file and printer sharing is enabled. Program access permissions are still enforced.
  - **Off:** You are not protected from hackers and other threats. Access to Windows NetBIOS services, and network file and printer sharing is allowed.

- **Restricted Zone Protection Level**

  The Restricted Zone is a part of a network that is not trusted, and is considered vulnerable to security threats from unknown entities. The following Restricted Zone protection levels are available.

- **High:** All traffic is blocked unless you explicitly add rules to allow traffic. Your computer cannot be seen by hackers. Access to Windows NetBIOS services, and network file and printer sharing is blocked. Ports are blocked unless you have provided permission for a program to use them.
- **Medium:** All traffic is allowed unless you explicitly add rules to block traffic. You are protected, but your computer is visible to others so that you can use network sharing. Access to Windows NetBIOS services, and network file and printer sharing is enabled. Program permissions are still enforced.
- **Off:** You are not protected from hackers and other threats. Access to Windows NetBIOS services, and network file and printer sharing is allowed.

- **Zones Assignments**

  The Zones Assignments shows all the network adapters and other ports that are attached to your computer, and the current zone that they are assigned to. Zones Assignments contains the following fields:

  - **Name:** Provides a numbered list of each network adapter or port (for example, LPT, or serial port). Connected network adapters display the IP address in use.
  - **Assigned To:** Displays the zone that the adapter or port is assigned to. If the adapter or port has not been assigned to a zone, the status Unassigned appears.

Expert Rules Tab

The Expert Rules tab, as shown in Figure 7-15, lets you view rules that configure access permissions to various protocols, ports, and IP addresses.

Figure 7-15: The Expert Rules tab

This window contains the following buttons and fields:

- **Add**

  Lets you add new expert rules.

- **Edit**

  Lets you edit existing selected rules.

- **Delete**

  Lets you delete selected rules from the expert rules list.

- **Enabled**

  A graphical symbol indicates whether the rule is enabled or not. A checkmark indicates the rule is enabled. A stop sign indicates the rule is disabled.

- **Access**

  Displays one of three available settings that indicate how access is permitted.

  - **Allow:** Access is allowed.
  - **Prevent:** Access is prevented.
  - **Ask User:** Indicates that you will be asked whether you want to grant access when an application attempts to gain access.

- **Description**

  Displays the name of the rule.

- **Audit Level**

  Displays one of three available settings that indicate how rules are monitored.

  - **Ignore:** No alerts will be generated by access attempts that breach rules.
  - **Monitor:** Attempts to access items contained in rules will be logged.
  - **Alert:** Generates an alert when an attempt is made to access items specified in rules.

- **Source Address**

  Displays the source port the rule is assigned to.

- **Destination Address**

  Displays the destination port the rule is assigned to.

- **Protocol**

  Displays the protocol the rule is assigned to.

- **Time**

  Displays the time the rule is programmed to run.

Privacy Screen

From the Privacy screen (see Figure 7-16), you can access all the settings and features of CA Personal Firewall designed to protect your privacy and identity.

Figure 7-16: CA Personal Firewall Privacy screen

The following are the three main sections of this screen:

- **Internet Browser Protection**

  Lets you manage websites and control the settings that your browser uses when browsing the Internet. Settings that can be configured include blocking cookies, ads, pop-up windows, and mobile code.

- **Cache Cleaner**

  Lets you schedule automatic cleaning of your computer and Internet cache to remove unwanted files and sensitive personal information. You can also clean the cache directly from this location using the Clean Cache Now button.

- **ID Theft**

  Lets you set the ID Theft Protection Level. Also provides an area for management and storage of personal information in a specialized encrypted location called My Safe, and the management of trusted Internet sites.

Internet Browser Protection Tab

The Internet Browser Protection tab, as shown in Figure 7-17, contains the following items:

Figure 7-17: Internet Browser Protection tab

- **Manage Site List Window**

  The Manage Site List window, (see Figure 7-18) accessible from the Manage Sites button, lets you manage advanced browser settings for individual websites.

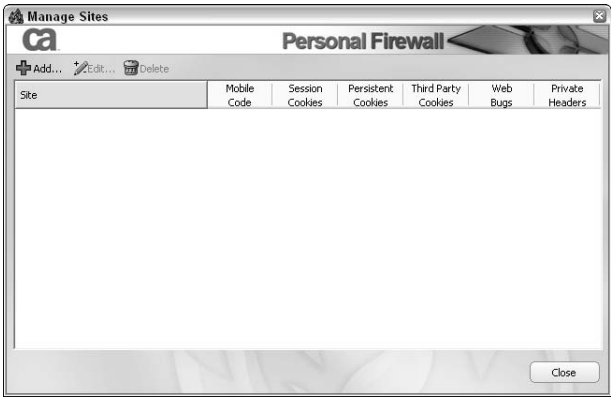

Figure 7-18: Manage site list window

This window contains the following fields:

- **Mobile Code:** A stop sign indicates that mobile code is blocked and a checkmark indicates that it is allowed.
- **Session Cookies:** Cookies that are stored in memory when your browser is loaded and removed when you close your browser.

  A stop sign indicates that session cookies are blocked and a checkmark indicates that they are allowed.
- **Persistent Cookies:** Cookies that are stored on the hard drive until they expire, or until they are deleted.

  A stop sign indicates that persistent cookies are blocked and a checkmark indicates that they are allowed.
- **Third-Party Cookies:** Cookies that do not come from the domain of the website that you are viewing. For example, a cookie issued by an advertising website that wants to track your web usage.

  A stop sign indicates that third-party cookies are blocked and a checkmark indicates they are allowed.

- **Web Bugs:** Web bugs are images stored on a web page or in an HTML email that are designed to monitor the usage of the page or email. They are generally invisible to the eye because they are one pixel wide and one pixel long, and often transparent.

  Web bugs are often used in junk email to report the infiltration of the spam, monitor the success of a marketing campaign.

  Information that is typically monitored includes the IP address of your PC, the amount of time that you viewed the page, the type of browser used, and possibly information previously stored in a cookie.

  A stop sign indicates web bugs are blocked and a checkmark indicates they are allowed.

- **Private Header:** Private header information refers to information that is stored in cookies that can be used to track users as they browse the Internet.

  A stop sign indicates private header information is blocked and a checkmark indicates it is allowed.

- **Cookie Control Protection Level**

  The Cookie Control protection level determines your exposure to cookies while using the Internet. The following cookie control protection levels are available:

  - **High:** Only session cookies are allowed. These are cookies that are stored in memory when your browser is open, then removed when you close your browser.
  - **Medium:** All third-party cookies are blocked. These are cookies that do not come from the domain of the website you are viewing. For example, a cookie issued by an advertising website wanting to track your web usage.
  - **Custom:** A customized level of protection is set. For more information, see Customize the Cookie Control Protection Level.
  - **Off:** No cookies are blocked.

- **Ad/Pop-up Blocker Protection Level**

  The Ad/Pop-up Blocker protection level determines your exposure to ads and pop-up windows while you are using

the Internet. The following Ad/Pop-up Blocker protection levels are available:

- **High:** All Internet ads and pop-ups are blocked.
- **Medium:** All pop-ups and animated ads are blocked.
- **Custom:** A customized level of protection is set. For more information, see Change the Ad/Pop-up Blocker Protection Level.
- **Off:** No ads or pop-ups are blocked.

- **Mobile Code Control Protection Level**

  You can view and set your level of mobile code protection. The following mobile code protection levels are available:

  - **On:** Mobile code control is on. Mobile code is blocked when you are using the Internet.
  - **Custom:** A customized level of protection is set.
  - **Off:** Mobile code is not blocked.

Cache Cleaner Tab

The Cache Cleaner tab, as shown in Figure 7-19, contains the following items:

Figure 7-19: The Cache Cleaner Tab

- **Cache Cleaner**

  You specify how often you want your cache cleaned, or deleted.

- **Clean Cache Now**

  This cleans, or deletes, your cache now.

- **Advanced**

  The advanced button takes you to where you can customize the cache cleaning settings.

ID Theft Tab

The ID Theft tab, as shown in Figure 7-20, contains the following items:

Figure 7-20: The ID Theft tab

- **ID Theft Protection Level**

  The ID Theft Protection Level lets you choose from three levels of protection for the personal information you've entered into My Safe.

  - **High:** All personal information secured in My Safe will automatically be blocked from being sent out through email or over the Internet.

    One exception would be if you have added a trusted site to your Trusted Site list. Information sent over the Internet to a Trusted Site would not be blocked.

- **Medium:** Any time there is an attempt to send personal information secured in My Safe through email or over the Internet, you will be prompted to either allow or deny access.

  One exception would be if you have added a trusted site to your Trusted Site list. You would not be prompted to allow/deny information sent over the Internet to a Trusted Site.

- **Off:** Any personal information in My Safe would not be protected from being sent out through email or over the Internet.

- **My Safe**

  My Safe is the area within CA Personal Firewall where you would add your personal information that should be protected from being used on websites, or in emails.

- **Trusted/Untrusted Sites**

  You can use Trusted/Untrusted Sites to manage which websites have access to your personal information.

  Using the trusted sites functionality, you assign one of the following three rules for each URL that you specify:

  - **Always Ask User:** Specified websites will always ask for permission before personal information is used. This setting will override an Identity Theft Protection Level of High.
  - **Allow Access:** Specified websites can access your private information.
  - **Deny Access:** Specified websites cannot access your private information.

Email Screen

The Email screen (see Figure 7-21) lets you quarantine potentially malicious email attachments, prevent mass-mailing email worms, and safeguard your email.

Figure 7-21: CA Personal Firewall Email screen

Protection Settings

The Protection Settings tab, as shown in Figure 7-22, contains the following items:

Figure 7-22: The Protection Settings tab

- **Inbound Email Protection**

  Inbound Protection monitors email attachments. You can configure the list of attachment types using the Email Attachments tab.

- **Outbound Email Protection**

  Outbound Protection monitors outbound emails. You can configure a set of monitoring options to monitor outbound emails for potential security threats using the Advanced button. If these types of emails are detected they will be blocked.

Email Attachments

The Email Attachments tab, as shown in Figure 7-23, contains the following items:

Figure 7-23: The Email Attachments tab

- **Add**

  Lets you add a suspected malicious email attachment file type to the list, blocking emails matching the type specified.

- **Edit**

  Lets you edit entries of email attachment file types.

- **Delete**

  Lets you delete entries of email attachment file types.

- **Description**

  Gives a description of the email attachment file type entry.

- **Extension**

  Gives the extension (such as .exe or .zip) of the email attachment file type entry.

- **Quarantine**

  Shows whether or not an attachment type will be quarantined. A checkmark indicates that the attachment type (extension) will be quarantined. A stop sign indicates that the attachment type (extension) will not be quarantined.

Reports Screen

CA Personal Firewall initiates alert notifications that pop up when a breach of security or privacy is detected. The Reports screen (see Figure 7-24) lets you change the frequency of alert notifications. In addition, this is where you change the configuration of event and program logging, and view log files.

Figure 7-24: CA Personal Firewall Reports screen

Settings Tab

The Settings tab, as shown in Figure 7-25, contains the following items:

- **Alert Events Notification Level**

  The alert events notification level determines the level of alerts displayed for firewall and privacy events. The following alert events notification levels are available.

  - **High:** All alerts generated by the firewall are displayed.
  - **Medium:** Only alerts requiring your attention are displayed.

Figure 7-25: The Settings tab

- **Event Logging**

  You can specify whether or not to log all the events related to CA Personal Firewall.

- **Application Logging**

  You can specify whether or not to log application events related to CA Personal Firewall.

Log Viewer

The Log Viewer tab, as shown in Figure 7-26, contains the following items:

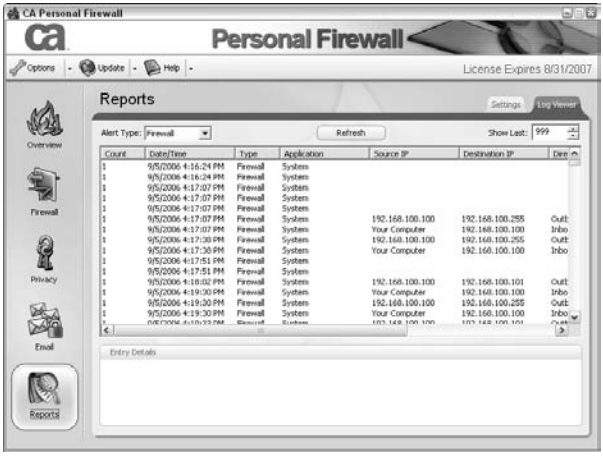

Figure 7-26: The Log Viewer tab

- **View the Firewall Log**

  You can view the firewall log to check information about firewall events.

- **View the Application Log**

  You can view the application log to check information about which applications were allowed or denied access.

Option Menus

The Option menus, which the next several sections discuss, can be accessed by the drop down list in the upper left corner of CA Personal Firewall, as shown in Figure 7-27.

Figure 7-27: Options drop-down list

General Options

The following items are available on the General Options menu, as shown in Figure 7-28:

- **General Options**
  - **Load CA Personal Firewall when Windows starts up.** You can configure whether or not to have CA Personal Firewall automatically start when Microsoft Windows starts.

Keep in mind, CA Personal Firewall must be loaded to allow unattended firewall features to run — for example, network monitoring, email protection and application control.

- **Use a password to protect your security settings.** You can set a password to protect your security settings.

Figure 7-28: General Options dialog

- **Backup and Restore Options**

  You can save a copy of your current firewall settings; therefore, they can be easily restored if your settings are lost, such as from a system crash or software issues.

  You can also reset all settings to their defaults by selecting the first backup.

Firewall Options

You can configure specific security requirements for your network using the Firewall Options menu, as Figure 7-29 shows. You can also control incoming and outgoing network traffic using various protocols and ports. However, programs that have been authorized, such as by Application Control, to connect using various ports and protocols take priority over these settings.

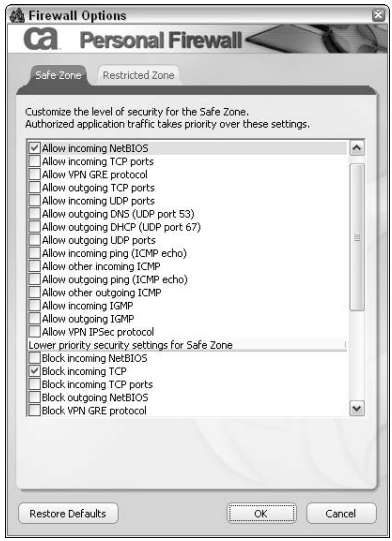

Figure 7-29: Firewall Options dialog

Firewall options let you customize the level of security that you want to apply to both the Safe Zone and the Restricted Zone by using many different options.

Privacy Options

The following sections discuss the privacy options available on all the tabs of the Privacy Options menu.

Cookie Control Tab

The following items are available on the Cookie Control tab, as shown in Figure 7-30:

- **General**
  - **Block Session Cookies.** Session cookies can cause security vulnerabilities. Although patches for affected software have been posted, you might still want to block session cookies if you are unsure whether your software is vulnerable.

    To block cookies that are used only when your browser is loaded, you can enable the Block session cookies option.

Figure 7-30: Cookie Control tab

- **Block Persistent Cookies.** Persistent cookies are stored on your computer hard disk until they are deleted or they expire. Some web servers use these types of cookies to identify users and perform tracking tasks.

  To block cookies that are stored on your hard disk, you can enable the Block persistent cookies option.

- **Expire Cookies.** To immediately expire cookies, or to set a period of days prior to expiration, you can use the Expire cookies option.

- **Third Party Cookies**
  - **Block Third-party Cookies.** Third-party cookies (also known as Tracking Cookies or Spyware Cookies) track your Internet usage. This can be considered a breach of privacy. To disallow this type of tracking, you can enable the Block third party cookies option.
  - **Remove Private Header Information.** Private header information refers to information that is stored in cookies that can be used to track users as they browse the Internet.

    To remove this type of sensitive information in headers, you can enable the Remove private header information option.

- **Disable Web Bugs.** Web bugs are used to track users of particular websites. To disable this type of monitoring, you can enable the Disable web bugs option.

- **Privacy Advisor**
  - **Show Privacy Advisor Alerts.** The Privacy Advisor can warn you by displaying a pop-up alert when an attempt is made to breach any of your privacy options.

    To display an alert indicating that a Privacy event was blocked, you can enable the Show privacy advisor alerts option.

Ad/Pop-up Control Tab

The following items are available on the Ad/Pop-up Control tab, as shown in Figure 7-31:

Figure 7-31: Ad/Pop-up Control tab

- **Banner/Skyscraper Ads**

  Ads displayed on websites can lead to slower loading of pages, and increased download volume.

  To stop banner or skyscraper ads from being displayed when you visit web pages, you can enable the Banner/Skyscraper ads option.

- **Pop-up/Pop-under Ads**

  Ads displayed on websites can lead to slower loading of pages, and increased download volume.

  To stop pop-up or pop-under ads from being displayed when you visit web pages, you can enable the Pop-up/Pop-under ads option.

- **Animated Ads**

  Ads displayed on websites can lead to slower loading of pages, and increased download volume.

  To stop animated ads from being displayed when you visit web pages, you can enable the Animated Ads option.

Mobile Code Tab

The following items are available on the Mobile Code tab, as shown in Figure 7-32:

Figure 7-32: Mobile Code tab

- **Block JavaScript**

  JavaScript can be a potential threat to the security of your computer if a script with malicious intent is run unexpectedly. To block JavaScript from running while you are accessing Internet resources, you can enable the Block JavaScript option.

- **Block VBScripts**

  VBScript can be potential threat to the security of your computer if a script with malicious intent is run unexpectedly. To block VBScript from running while you are accessing Internet resources, you can enable the Block VBScripts option.

- **Block Embedded Objects**

  Embedded objects can be a potential threat to the security of your computer if a web page or email contains a malicious object embedded into the HTML code. To block embedded objects, including ActiveX and Java, from running while accessing the Internet or email, you can enable the Block embedded objects option.

- **Block MIME Objects**

  MIME or Multipurpose Internet Mail Extensions is a format used for email. MIME objects can include malicious files and data include viruses, worms, and spyware. To block MIME objects from running while you are accessing the Internet or email, you can enable the Block mime objects option.

Cache Cleaner Tab

The Cache Cleaner tab, as Figure 7-33 shows, lets you configure the items that you want to be cleaned when you run the cache cleaner, which are the following:

- **Browser Cache**
  - **Cache:** Files that are cached by your browser when you visit websites.
  - **URL history:** A list of recent websites you have visited.
  - **Saved form data:** Text that you have previously entered into fields on web forms. For example, your name and address.
  - **Saved passwords:** Passwords that have been entered that have been saved by your browser so you don't have to re-enter them.
  - **Typed URL history/address Bar:** Recent entries you have typed into the browser's address bar.
  - **Cookies:** All types of cookies that the browser has stored.

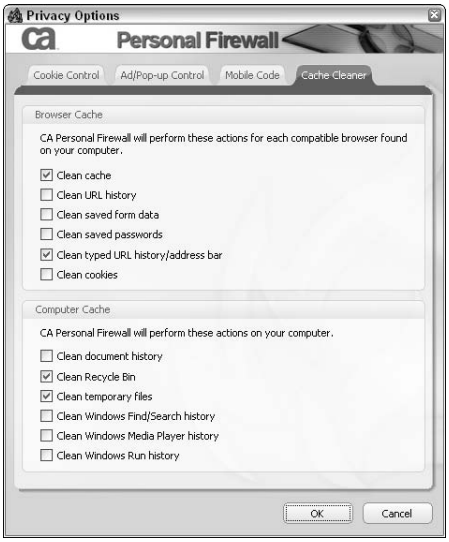

Figure 7-33: Cache Cleaner tab

- **Computer Cache**
  - **Document history:** A list of recent documents you have been using, for example, Word documents or Excel spreadsheets.
  - **Recycle Bin:** Items that you have recently deleted are stored in the Recycle bin.
  - **Temporary Files:** Directories that have been created by the installation of software, or browsing the Internet.
  - **Windows Find/Search History:** A list of recent files or computer searches that has been performed using the Windows Search or Find feature.
  - **Windows Media Player history:** A list of recent media (audio or video) that has been played using Windows Media Player.
  - **Windows Run history:** A list of items that have recently been entered into the Windows Run dialog.

Email Options

The following options are available on the Email Options menu, as Figure 7-34 shows:

Figure 7-34: Email Options dialog

- **Too Many Emails Are Sent at Once**

  Sending a large amount of email simultaneously can lead to network congestion. Additionally, your computer could become infected by a virus or worm that propagates the infection by sending out many emails simultaneously.

  To display an alert when too many outbound emails are sent simultaneously, you can enable the Too many emails are sent at once option.

- **A Message Has Too Many Recipients**

  Sending an email with many recipients can lead to network congestion. Additionally, your computer could be infected by a virus or worm that propagates the infection by sending itself to multiple recipients.

  To display an alert when an outbound email has too many recipients, you can enable the A message has too many recipients option.

- **The Sender's Address Is Not in This List**

  If your computer security is compromised, an unknown user may attempt to send malicious software using your email.

  To display an alert when an outbound email is sent from an unknown sender, you can enable the The Sender's Address Is Not in This List option.

Common Tasks

This section provides step-by-step directions for common tasks relating to the Firewall component.

Secure Now

To fix problems associated with your firewall software, you can use the Secure Now feature:

Note

The Secure Now feature only becomes active when it is determined that the software is not configured for the minimum recommended security settings.

1. Select the Overview tab on the left side of the CA Personal Firewall window.

   The Overview window appears.

2. Click Secure Now, as shown in Figure 7-35.

Figure 7-35: Clicking Secure Now

The Secure Now window appears, as shown in Figure 7-36.

Figure 7-36: Secure Now window

3. Review the list of actions to be performed, and click Continue.

   The software automatically performs various tasks depending on the issues that need to be addressed. These tasks include automatically updating and enabling certain security options to ensure that your computer is not exposed to online threats. The configuration that is enabled after running the Secure Now feature is the recommended configuration.

Block All Internet Access

To block all access to the Internet on your computer, use the Block All Internet Access quick task:

1. Select the Overview tab on the left side of the CA Personal Firewall window.

   The Overview window appears.

2. Click Block All Internet Access, as shown in Figure 7-37, in the Main Tasks area.

   You are asked to confirm that you wish to block Internet Access.

3. Click Yes.

   Access to the Internet is blocked until you re-enable it.

Note

When Internet access is blocked, all Internet connections — including remote desktop connections — are lost.

Figure 7-37: Blocking all Internet access

Restore Internet Access

If you have blocked Internet access, you can restore it with the link provided in the Main Tasks area:

1. Select the Overview tab on the left side of the CA Personal Firewall window.

   The Overview window appears.

2. Click Restore Internet Access, as shown in Figure 7-38, in the Main Tasks area.

Figure 7-38: Restoring Internet access

Internet access is re-enabled.

Clean Cache Now

To clean all configured browser and hard drive cache items, use the Clean Cache Now quick task:

1. Select the Overview tab on the left side of the CA Personal Firewall window.

   The Overview window appears.

2. Click Clean Cache Now, as shown in Figure 7-39, in the Main Tasks area.

Figure 7-39: Cleaning cache

   You are prompted to confirm your selection.

3. Click Yes.

   Hard drive and browser cache items are cleaned based on the settings selected.

Advanced Tasks

This section provides step-by-step directions for tasks typically less commonly performed.

Firewall

This section provides step-by-step directions for tasks relating to firewall settings.

Add an Application

To control the access that an application has to the Internet or the local network, you can add them to the Application Control list:

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

   The Firewall window appears.

2. Select the Application Control tab, as shown in Figure 7-40.

Figure 7-40: Selecting the Application Control tab

   The list of applications appears.

3. Click Add.

   The Please select a file window appears.

4. Select an application from the file browser, and then click OK, as shown in Figure 7-41.

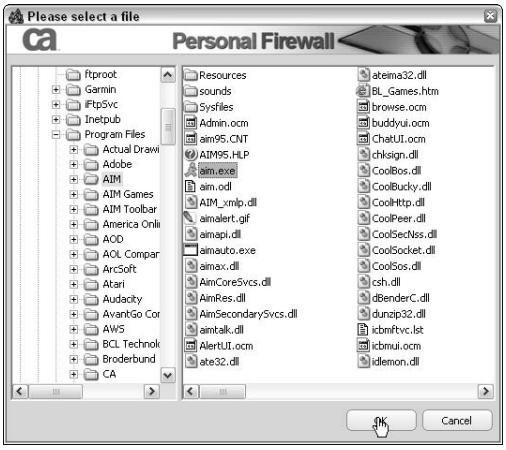

Figure 7-41: Selecting an Application from the file browser

The application appears in the Application Control list.

Edit Application Access

You can change the access that an application has to the Internet or the local network:

1. Click the Firewall Tab on the left side of the CA Personal Firewall window.

   The Firewall window appears.

2. Select the Application Control tab, as shown in Figure 7-42.

Figure 7-42: Selecting the Application Control tab

The list of applications appears.

3. Continue with the next steps depending on whether you're editing or removing an entry:

To edit an entry:

a. Right-click on the specific application and authorization type you want to edit, as shown in Figure 7-43, and then choose from the following options:

Figure 7-43: Editing an application entry

- **Allow:** Access is allowed for the selected application.
- **Prevent:** Access is denied for the selected application.
- **Ask User:** You will be asked by the firewall if access can be granted for the selected application.

To remove an entry:

a. Select the application that you want to delete, and then click Delete, as shown in Figure 7-44.

Note

If the application attempts to use the local network or Internet again, an alert will appear.

Figure 7-44: Deleting an application entry

Add Expert Rules to an Application

If you want to add specific access conditions to an application in the Advanced Application Control section, you can add expert rules to it:

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

   The Firewall window appears.

2. Select the Application Control tab, as shown in Figure 7-45.

Figure 7-45: Selecting the Application Control tab

The Application Control window appears.

3. Select the application that you want to add expert rules to, and then click Edit, as shown in Figure 7-46.

Figure 7-46: Editing Expert Rules for an application

The Application Rules window appears.

4. If the program changes frequently, select the This Program Changes Frequently check box.

5. Click the Add button on the upper left side of the window, as Figure 7-47 shows.

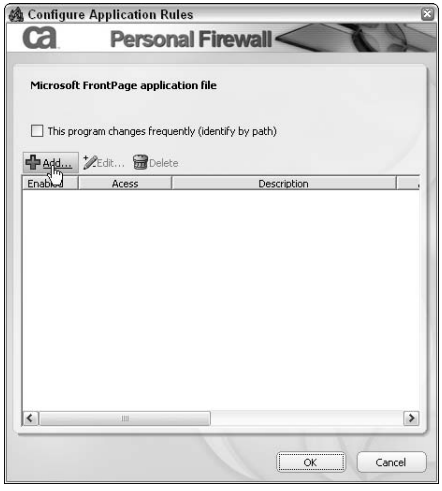

Figure 7-47: Adding an Expert Rule

The Expert Rule Configuration window appears.

6. Enter a name for the rule in the Rule Description field, then click the Enable rule check box at the top of the Expert Rule Configuration window.

   You can now configure the Protocol tab.

7. Click the Protocol tab, then click the drop-down arrow in the Protocol & Ports field and select one of the listed protocols that rules can be established for, as shown in Figure 7-48.

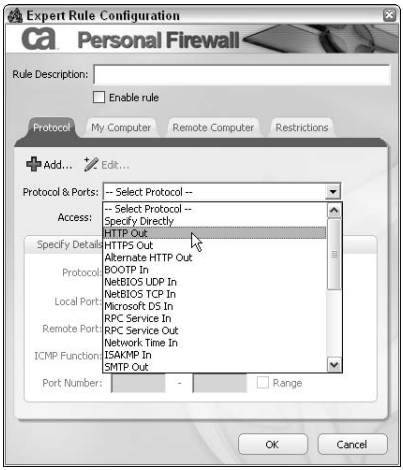

Figure 7-48: Selecting a protocol

Note

For details on the available protocols, see Expert Rules.

   a. (Optional) Click Add to add a new protocol that you want to specify.

      The Add Protocols and Ports window appears.

   b. If you've selected Specify Directly, complete the fields provided in the Specify Details section, as shown in Figure 7-49, and then click OK.

      Your protocol is selected.

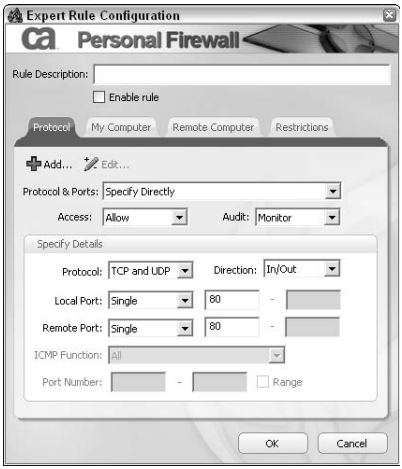

Figure 7-49: Specifying details

c. Choose from one of the following access types from the **Access** field using the drop-down arrow:

- **Prevent:** No access by the selected protocol is permitted.
- **Allow:** Access by the selected protocol is permitted.
- **Ask User:** You will be asked when an access attempt is made by the selected protocol is made.

The selected access type is displayed in the Access field.

d. Choose from one of the following audit types that you require for this rule from the Audit field using the drop-down arrow:

- **Ignore:** No alerting or logging is performed.
- **Monitor:** Access to this protocol is logged.
- **Alert:** An alert is displayed when access to this protocol is attempted.

The selected audit type is displayed in the Audit field.

e. If you want to specify further details for this rule, click the Edit button and use the fields provided in the Specify Details section, then click OK.

You are now ready to configure the My Computer tab.

8. Select the My Computer tab, as Figure 7-50 shows, and complete the following sections:

Figure 7-50: Selecting the My Computer tab

Note

My Computer refers to connections initiated by the computer you are currently configuring.

a. Use the drop-down arrow located in the IP Address field to select from one of the following preset IP settings provided:

- **All addresses**
- **My Computer**
- **Safe Zone**
- **Restricted Zone**
- **Specify Directly**
- **LAN**
- **Loopback**

Note

If you choose Specify Directly, you must complete the Specify Details section located at the bottom of this window.

b. (Optional) Click Add to add a new IP address to the drop-down list of preset IP addresses.

The Add IP Address window appears.

c. Complete the fields provided, then click OK.

Your Local Computer IP address is selected. You are now ready to configure the Remote Computer tab.

9. Select the Remote Computer tab, as Figure 7-51 shows, and complete the following sections:

Figure 7-51: Selecting the Remote Computer tab

Note

Remote Computer refers to connections initiated by other computers on the local network, or Internet.

a. Use the drop-down arrow located in the IP Address field to select from one of the following preset IP settings provided:

- **All addresses**
- **Specify Directly**
- **LAN**
- **Loopback**

Note

If you choose Specify Directly, you must complete the Specify Details section located at the bottom of this window.

b. (Optional) Click Add to add a new IP address to the drop-down list of preset IP addresses.

The Add IP Address window appears.

c. Complete the fields provided, then click OK.

Your Remote Computer IP address is selected. You are now ready to configure the Restrictions tab.

10. Click the Restrictions tab, as shown in Figure 7-52, and complete the following sections:

Figure 7-52: Selecting the Restrictions tab

a. Use the drop-down arrow located in the Time field to specify whether the rule should be run all the time, or according to a determined schedule.

If you select Specify Time to Run in the Time field, the list of days becomes visible.

b. Click the check box provided for the day or days on which you want the rule to run.

The From and To fields become visible.

c. Select the start and end times for the rule using the up and down arrows.

Your rule configuration is complete.

11. Click OK.

    Your expert rule is saved and active.

Add Expert Firewall Rules

To add specific access conditions to a network port, protocol, and IP address, you can add expert rules:

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

   The Firewall window appears.

2. Select the Expert Rules tab, as shown in Figure 7-53.

Figure 7-53: Selecting the Expert Rules tab

   The expert rules list appears.

3. Click the Add button located on the upper left side of the window.

   The Expert Rule Configuration window appears.

4. Enter a name for the rule in the Rule Description field and select the Enable rule check box at the top of the Expert Rule Configuration window, as shown in Figure 7-54.

Figure 7-54: Configuring an Expert Rule

You can now configure the Protocol tab.

5. Select the Protocol tab, as shown in Figure 7-55, then click the drop-down arrow in the Protocol & Ports field and select one of the listed protocols for which rules can be established.

Figure 7-55: Selecting the Protocol tab

Note

For details on these protocols, see Expert Rules.

a. (Optional) Click Add to add a new protocol that you want to specify.

The Add Protocols and Ports window appears.

b. Complete the fields provided in the Specify Details section, then click OK.

Your protocol is selected.

c. Choose from one of the following access types from the Access field using the drop-down arrow:

- **Prevent:** No access by the selected protocol is permitted.
- **Allow:** Access by the selected protocol is permitted.
- **Ask User:** You will be asked when an access attempt is made by the selected protocol.

The selected access type is displayed in the Access field.

d. Choose from one of the following audit types that you require for this rule from the Audit field using the drop-down arrow:

- **Ignore:** No alerting or logging is performed.
- **Monitor:** Access to this protocol is logged.
- **Alert:** An alert is displayed when access to this protocol is attempted.

The selected audit type is displayed in the Audit field.

e. If you want to specify further details for this rule, click the Edit button and use the fields provided in the Specify Details section, then click OK.

You are now ready to configure the My Computer tab.

6. Select the My Computer tab, as shown in Figure 7-56, and complete the following sections:

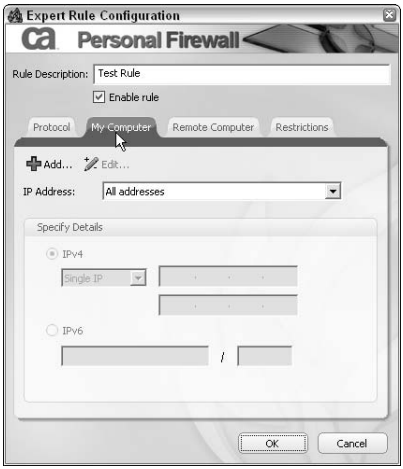

Figure 7-56: Selecting the My Computer tab

a. Use the drop-down arrow located in the IP Address field to select one of the following preset IP settings:

- **All addresses**
- **My Computer**
- **Safe Zone**
- **Restricted Zone**
- **Specify Directly**
- **LAN**
- **Loopback**

Note

If you choose Specify Directly, you must complete the Specify Details section located at the bottom of this window.

b. (Optional) Click Add to add a new IP address to the drop-down list of preset IP addresses.

The Add IP Address window appears.

c. Complete the fields provided, then click OK.

Your Local Computer IP address is selected. You are now ready to configure the Remote Computer tab.

7. Select the Remote Computer tab, as shown in Figure 7-57, and complete the following sections:

Figure 7-57: Selecting the Remote Computer tab

a. Use the drop-down arrow located in the IP Address field to select from one of the following preset IP settings provided:

- **All addresses**
- **Specify Directly**
- **LAN**
- **Loopback**

Note

If you choose Specify Directly, you must complete the Specify Details section located at the bottom of this window.

b. (Optional) Click Add to add a new IP address to the drop-down list of preset IP addresses.

The Add IP Address window appears.

c. Complete the fields, and then click OK.

Your Remote Computer IP address is selected. You are now ready to configure the Restrictions tab.

8. Select the Restrictions tab, as shown in Figure 7-58, and complete the following sections:

Figure 7-58: Selecting the Restrictions tab

a. Use the drop-down arrow located in the Time field to specify whether the rule should be run all the time, or according to a determined schedule.

If you select Specify Time to Run in the Time field, the list of days becomes visible.

b. Click the check box provided for the day or days on which you want to run the rule.

The From and To fields become visible.

c. Use the up and down arrows to select the time at which you want to start and end the rule.

Your rule configuration is complete.

9. Click OK.

Your expert rule is saved and active.

Zone Protection Levels

This section provides step-by-step directions for tasks relating to your protection zones.

Change Your Safe Zone

To change the level of protection available in your Safe Zone or to customize your Safe Zone:

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

   The Firewall window appears.

2. Select the Zones tab, as shown in Figure 7-59.

Figure 7-59: Selecting the Zones tab

   The Firewall Zone Protection Levels appear.

3. Continue with the next steps depending on whether you're changing or customizing.

   To change your Safe Zone Protection Level:

   a. Use the slider bar to adjust to the level of protection, as shown in Figure 7-60, that you require for your Safe Zone.

      The new protection level for your Safe Zone is now active.

Figure 7-60: Adjusting the slider bar

To customize your Safe Zone Protection Level:

a. Click the Advanced button located in the Safe Zone Protection Level section.

The Advanced Firewall Options window appears, allowing you to customize aspects of the firewall when using this zone.

For procedures on this type of customization, see Firewall Options.

b. When you have completed customizing the firewall options, click OK.

Note

If you wish to return to the default installation settings, click the Restore Defaults button in the Advanced Firewall Options window.

Change Your Restricted Zone

To change the level of protection available in your Restricted Zone or customize your Restricted Zone:

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

The Firewall window appears.

2. Select the Zones tab, as shown in Figure 7-61.

Figure 7-61: Selecting the Zones tab

The Firewall Zone Protection Levels appear.

3. Continue with the next steps depending upon if you're changing or customizing.

To change your Restricted Zone Protection Level:

a. Use the slider bar to adjust to the level of protection, as shown in Figure 7-62, that you require for your Restricted Zone.

Figure 7-62: Adjusting the slider bar

The new protection level for your Restricted Zone is now active.

To customize your Restricted Zone Protection Level:

a. Click the Advanced button located in the Restricted Zone Protection Level section.

The Advanced Firewall Options window appears, allowing you to customize aspects of the firewall when using this zone. For procedures on this type of customization, refer to the "Firewall Options" section earlier in this chapter.

b. When you have completed customizing the firewall options, click OK.

Note

If you wish to return to the default installation settings, click the Restore Defaults button in the Advanced Firewall Options window.

Assign Network Adapters and Ports to Zones

You can assign network adapters and input/output ports used on your computer to zones.

1. Select the Firewall tab on the left side of the CA Personal Firewall window.

The Firewall window appears.

2. Select the Zones tab, as shown in Figure 7-63.

Figure 7-63: Selecting the Zones tab

The Firewall Zones Assignments section appears at the bottom of the window.

3. Right-click the Assigned To status of the adapter or port you wish to assign to a zone, then choose from Safe or Restricted to assign it to that zone. See Figure 7-64 for an example.

Figure 7-64: Assigning a network adapter to a zone

Note

The status of the adapter or port is located in the Assigned To column.

Internet Browser Protection

This section provides step-by-step directions for tasks relating to your Internet browser protection.

Manage Sites

You can specify security settings for various websites, using Manage Sites functionality:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the Internet Browser Protection tab, as shown in Figure 7-65.

   The Internet Browser Protection window appears.

Figure 7-65: Selecting the Internet Browser Protection tab

3. Click the Manage Sites button located at the upper-right side of the window.

   The Manage Site List window appears. You can now add a new site.

4. Enter the URL of the site you wish to manage in the URL field, and then select the Cookies tab to configure the following options:

   - **Block session cookies**
   - **Block persistent cookies**
   - **Enable cookie expiration**
   - **Disable third-party cookies**
   - **Remove private header information**
   - **Disable web bugs**

5. Select the Ad/Pop-up Blocker tab to configure the following options:

   - **Block Banner/Skyscraper ads**
   - **Block Pop-up/Pop-under ads**
   - **Block animated ads**

6. Select the Mobile Code tab to configure the following options:

   - **Block JavaScript**
   - **Block VBScripts**

- **Block embedded objects (Java, ActiveX, etc.)**
- **Block MIME-type integrated objects**

7. Click OK.

Your managed site configuration is saved and active.

Change the Cookie Control Protection Level

To set the amount of exposure or to customize your level of protection that you have from cookies while you are using the Internet:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

The Privacy window appears.

2. Select the Internet Browser Protection tab, as shown in Figure 7-66.

Figure 7-66: Selecting the Internet Browser Protection tab

The Internet Browser Protection window appears, and the Cookie Control settings are displayed.

3. Continue with the next steps depending upon if you're changing or customizing.

To change the Cookie Control Protection Level:

a. Use the slider bar to adjust to the level of protection, as shown in Figure 7-67, that you require.

Figure 7-67: Adjusting the slider bar

Your new protection level for cookie control is now set.

To customize your Cookie Control Protection Level:

a. Use the slider bar to adjust to the level of protection to Custom, as shown in Figure 7-68.

Figure 7-68: Adjusting the slider bar to custom level

Your protection level is now determined by the cookie control privacy options, which can be customized.

b. Click Advanced.

The cookie control options appear, allowing you to customize all aspects of cookie control.

For more information on this type of customization, refer to the "Cookie Control Tab" section earlier in this chapter.

Change the Ad/Pop-up Blocker Protection Level

To set the amount of exposure or to customize your level of protection that you have to ads and pop-ups while using the Internet:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the Internet Browser Protection tab, as shown in Figure 7-69.

Figure 7-69: Selecting the Internet Browser Protection tab

The Internet Browser Protection window appears, and the Ad/Pop-up Blocker settings are displayed.

3. Continue with the next steps depending upon if you're changing or customizing:

   To change the Ad/Pop-up Blocker Protection Level:

   a. Use the slider bar to adjust to the level, as in Figure 7-70, of protection that you require.

Figure 7-70: Adjusting the slider bar

Your new protection level for ads and pop-ups is now set.

To customize your Ad/Pop-up Blocker Protection Level:

a. Use the slider bar to adjust to the level of protection to Custom, as shown in Figure 7-71.

Figure 7-71: Adjusting the slider bar to custom level

Your protection level is now determined by the Ad/Pop-up Blocker privacy options, which can be customized.

b. Click Advanced.

The ad/pop-up blocker options appear, allowing you to customize all aspects of the ad/pop-up blocker.

For more information on this type of customization, refer to the "Ad/Pop-up Control Tab" section earlier in this chapter.

Change the Mobile Code Protection Level

To set the amount of exposure or to customize your level of protection that you have from mobile code while you are using the Internet, follow these steps:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

The Privacy window appears.

2. Select the Internet Browser Protection tab, as shown in Figure 7-72.

Figure 7-72: Selecting the Internet Browser Protection tab

The Internet Browser Protection window appears, and the mobile code settings are displayed.

3. Continue with the next steps depending on whether you're changing or customizing:

To change the Mobile Code Protection Level:

a. Use the slider bar to adjust to the level of protection, as shown in Figure 7-73, that you require.

Figure 7-73: Adjusting the slider bar

Your new protection level for mobile code is now set.

To customize your Mobile Code Protection Level:

a. Use the slider bar to adjust to the level of protection to Custom, as shown in Figure 7-74.

Figure 7-74: Adjusting the slider bar to custom level

Your protection level is now determined by the Mobile Code privacy options, which can be customized.

b. Click Advanced.

The mobile code options appear, allowing you to customize all aspects of mobile code protection.

For more information on this type of customization, refer to the "Mobile Code Tab" section earlier in this chapter.

Cache Cleaner

This section provides step-by-step directions for tasks relating to your protection zones.

Schedule the Cache Cleaner

To let CA Personal Firewall automatically clean your computer cache, you can schedule the Cache Cleaner:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the Cache Cleaner tab, as shown in Figure 7-75.

Figure 7-75: Selecting the Cache Cleaner tab

3. Use the up and down arrows in the Cache Cleaner area, as pointed out in Figure 7-76, to select the number of days to wait between automatic cache cleaning.

Figure 7-76: Scheduling the Cache Cleaner

Your configuration is active. The cache will be cleaned according to the interval that you selected.

Clean Cache Now

To instantly clean all of the items that are configured to be cleaned by the cache cleaner, you can use the Clean Cache Now button:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the Cache Cleaner tab, as shown in Figure 7-77.

Figure 7-77: Selecting the Cache Cleaner Tab

3. Click Clean Cache Now, as shown in Figure 7-78.

Figure 7-78: Using the Clean Cache Now Button

All of the configured items are cleaned.

Customize the Cache Cleaner

To determine what items will be cleaned by the Cache Cleaner, you can customize your Cache Cleaner using the Advanced button:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the Cache Cleaner tab, as shown in Figure 7-79.

Figure 7-79: Selecting the Cache Cleaner tab

3. Click Advanced, as shown in Figure 7-80.

Figure 7-80: Customizing the Cache Cleaner

The Cache Cleaner Options appear, allowing you to customize all aspects of the Cache Cleaner.

For more information on this type of customization, refer to the "Cache Cleaner Tab" section earlier in this chapter.

ID Theft

This section provides step-by-step directions for tasks relating to ID Theft and My Safe.

Add Private Information to My Safe

To ensure that certain private information is protected when you are using the Internet and email, you can add the information to My Safe:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the ID Theft tab, as shown in Figure 7-81.

Figure 7-81: Selecting the ID Theft tab

The ID Theft options appear.

3. Click My Safe, as shown in Figure 7-82.

Figure 7-82: Accessing your Safe

The Manage My Safe window appears.

4. Click Add.

   The Configure Personal Information window appears, allowing you to enter the details of the private information that you want to protect.

5. Type a description for your private information in the Description field.

   You can now select a category.

6. Use the drop-down arrow to select a list of personal information you would like to protect.

   You can now enter the details in the Data field.

7. Enter the details of the information that you want to protect in the Data field, and if required, repeat the entry in the Confirm Input field.

   You can now specify whether you want to use one-way encryption to make the information unreadable.

8. If you want to use one-way encryption, select the Use one-way encryption to store data check box.

   You can now specify whether you want to protect the information when you are using the Internet and email.

9. If you want to protect this information when using the Internet and email, select the Email and Web check boxes, then click OK. See Figure 7-83 for an example.

Figure 7-83: Example of adding information to My Safe

Your private information is now protected.

Edit Private Information in My Safe

If you want to make changes to your private information, you can edit My Safe:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the ID Theft tab, as shown in Figure 7-84.

Figure 7-84: Selecting the ID Theft tab

   The ID Theft options appear.

3. Click My Safe, as shown in Figure 7-85.

Figure 7-85: Accessing your Safe

   The Manage My Safe window appears.

4. Continue with the next steps depending upon if you're editing or deleting an entry.

To edit an entry:

a. Select an entry from the My Safe list that you want to edit.

   The entry appears highlighted.

b. Click Edit, as shown in Figure 7-86, on the upper left side of the Manage My Safe window.

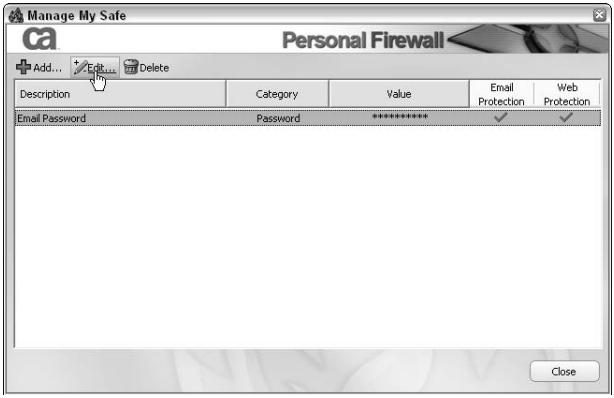

Figure 7-86: Accessing details of a Safe entry

   The Configure Personal Information window appears, allowing you to edit the details of the protected information.

c. After you finish editing the details of the entry, click OK.

   Your private information is updated.

To delete an entry:

a. In the My Safe list, select the entry that you want to delete, and click the Delete button. See Figure 7-87 for an example.

   The entry is deleted from My Safe.

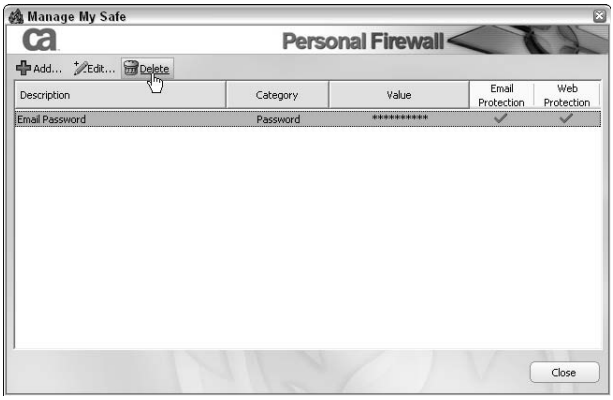

Figure 7-87: Deleting a Safe entry

Add a Trusted Site

To control the access that a website has to your personal data, you can add it to the Trusted/Untrusted Sites list:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the ID Theft tab, as shown in Figure 7-88.

Figure 7-88: Selecting the ID Theft tab

The ID Theft options appear.

3. Click Add below the Trusted/Untrusted Sites heading.

   The Configure Site window appears.

4. In the URL field, enter the URL of the site that you want to add. See Figure 7-89 for an example.

Figure 7-89: Example of URL to add as trusted site

   You can now select the type of access for the site.

5. Select the corresponding radio button to choose a type of access:

   - **Allow Access:** The site will be allowed to gain access to your personal data and information.
   - **Deny Access:** The site will not be allowed to gain access to your personal data and information.
   - **Always Ask User:** The firewall will ask you whether you want to allow the website to gain access to your personal data and information.

6. Click OK.

   Your selections are saved and active.

Edit a Trusted Site

To change or delete your trusted sites, which have access to your personal information:

1. Select the Privacy tab on the left side of the CA Personal Firewall window.

   The Privacy window appears.

2. Select the ID Theft tab, as shown in Figure 7-90.

Figure 7-90: Selecting the ID Theft tab

The ID Theft options appear.

3. Continue with the next steps depending upon if you're editing or deleting an entry.

To edit an entry:

a. Select a URL from the list of URLs presented, then click Edit below the Trusted/Untrusted Sites heading. See Figure 7-91 for an example.

Figure 7-91: Accessing details of trusted site entry

The Configure Site window appears.

b. In the URL field, enter the URL of the site that you want to edit.

You can now select the type of access for the site.

c. Select the corresponding radio button to choose a type of access:

- **Allow Access:** The site will be allowed to load.
- **Deny Access:** The site will be blocked.
- **Always Ask User:** The firewall will ask you whether you want to allow the website to load.

d. Click OK.

Your selections are saved and active.

To delete an entry:

a. Click the trusted site that you want to delete.

The trusted site appears highlighted.

b. Click Delete, as shown in Figure 7-92.

Figure 7-92: Deleting a trusted site entry

A confirmation window appears asking you to confirm your selection.

c. Click Yes to delete the trusted site.

The site is deleted from the trusted sites list.

Email

This section provides step-by-step directions for tasks relating to your Email protection.

Enable or Disable Inbound Email Protection

You can enable or disable inbound email protection, which automatically renames potential threatening email attachments to prevent opening or execution of the attachment:

1. Select the Email tab on the left side of the CA Personal Firewall window, and then select the Protection Settings tab, as shown in Figure 7-93.

Figure 7-93: Selecting Protection Settings tab in the Email tab

The Email Options window appears.

2. Continue with the next steps depending on whether you're enabling or disabling inbound email protection.

   To enable:

   a. Select the On option in the Inbound Email Protection section.

      Inbound email protection is enabled. All configured email attachments that are sent to your email address are automatically renamed with a .efw extension preventing access.

To disable:

a. Select the Off option in the Inbound Email Protection section.

Inbound email protection is disabled. No email attachments will be monitored.

Enable or Disable Outbound Email Protection

You can enable or disable outbound email protection, which prevents and block viruses from being sent from your email account, based on a set of defined options:

1. Select the Email tab on the left side of the CA Personal Firewall window, and then select the Protection Settings tab, as Figure 7-94 shows.

Figure 7-94: Selecting the Protection Settings tab in the Email tab

The Email Options window appears.

2. Continue with the next steps depending upon if you're enabling or disabling.

To enable:

a. Select the On option in the Outbound Email Protection section.

Outbound email protection is enabled. Emails that match the configured outbound email restrictions will be blocked.

To disable:

a. Select the Off option in the Outbound Email Protection section.

Outbound email protection is disabled. No outbound emails will be monitored.

Add Attachments to Inbound Email Protection List

To prevent unwanted email attachments, you can add an attachment type to a list of files that will be blocked when inbound email protection is enabled:

1. Select the Email tab on the left side of the CA Personal Firewall window, and then select the Email Attachments tab, as shown in Figure 7-95.

Figure 7-95: Selecting the Email Attachments tab in the Email tab

The Email Options window appears.

2. Click the Add button on the upper-left side of the window.

The Configure Attachment window appears.

3. Type a description and extension in the fields provided. Figure 7-96 shows an example.

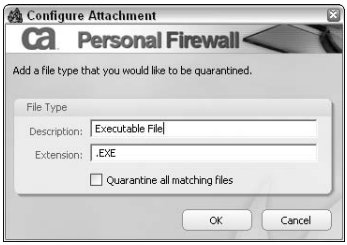

Figure 7-96: Example of specifying details

4. To quarantine this type of extension, select the Quarantine all matching files check box.

   Your email protection options for this type of attachment are configured.

5. Click OK.

   Your changes are saved and active.

Edit Attachments in the Inbound Email Protection List

You can edit or delete attachments in the inbound email protection list:

1. Select the Email tab on the left side of the CA Personal Firewall window, and then select the Email Attachments tab, as shown in Figure 7-97.

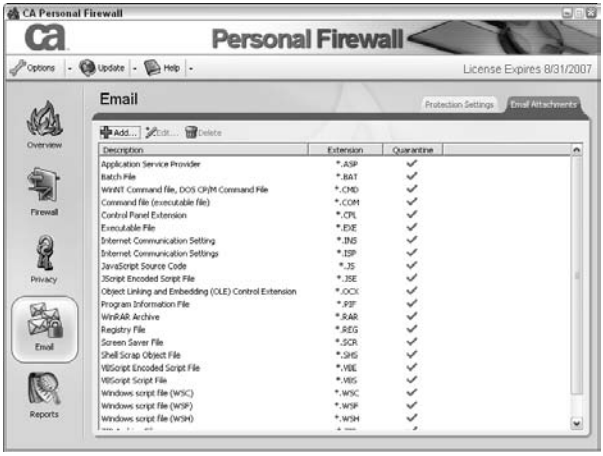

Figure 7-97: Selecting the Email Attachments tab in the Email tab

The Email Options window appears.

2. Continue with the next steps depending upon if you're editing or deleting attachments.

To edit an entry:

a. Click the Edit button on the upper left side of the window.

The Configure Attachment window appears.

b. Type a description and extension in the fields provided, then choose if you want to Quarantine all matching files by using the check box. Figure 7-98 shows an example.

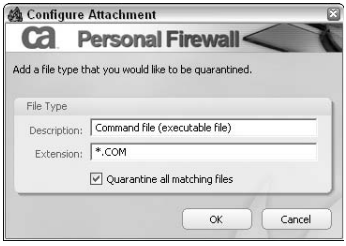

Figure 7-98: Example of editing an attachments entry

Your email protection options for this type of attachment are configured.

c. Click OK.

Your changes are saved and active.

To delete an entry:

a. Select an entry from the list of attachments.

b. Click the Delete button on the upper left side of the window, such as shown in Figure 7-99.

The Confirm Delete window appears.

c. Click Yes.

Your selected attachment is deleted from the list.

Figure 7-99: Deleting an attachment entry

Configure Advanced Outbound Email Protection

To determine the types of emails that outbound email protection will block, you can configure the advanced outbound email protection options.

1. Select the Email tab on the left side of the CA Personal Firewall window, and then select the Protection Settings tab, as shown in Figure 7-100.

Figure 7-100: Selecting the Protection Settings tab in the Email tab

The Email Options window appears.

2. Click Advanced on the lower right side of the Email Options window.

   The Email Protection Options appear. Use the check boxes provided to configure your outbound email protection.

   For more information about this window, refer to the "Email Options" section earlier in this chapter.

8

PROTECTING AGAINST SPYWARE AND ADWARE

The Anti-Spyware component of CA Internet Security Suite, which is CA Anti-Spyware, protects your identity and PC by detecting and eliminating spyware and other non-viral infections.

This chapter is organized into these main sections:

- **Anti-Spyware Scanning Methods**

  This section introduces the scanning methods used in CA Anti-Spyware.

- **CA Anti-Spyware Introduction**

  This section takes you through each of the CA Anti-Spyware screens, letting you know where everything is located and what each option does.

- **Common Tasks**

  This section provides step-by-step instructions for common CA Anti-Spyware tasks.

- **Advanced Tasks**

  This section provides step-by-step instructions for CA Anti-Spyware tasks performed less often.

Anti-Spyware Scanning Methods

CA Anti-Spyware provides the following scanning methods to help you to keep your computer free of spyware:

- **Real-time Scanning**

  By detecting malicious activity as it occurs, CA Anti-Spyware prevents and removes unwanted ActiveX controls, Browser Helper Objects, and browser toolbars; prevents malicious changes to the Windows Hosts file, Registry, and Startup Programs list; and protects Internet Explorer settings, including your home page, favorites, and search pages. This new functionality builds on existing real-time capabilities to detect and remove tracking cookies and spyware programs running in memory.

  When an infection is found, CA Anti-Spyware sends you a warning, with the name of the file that is performing the harmful or suspicious action, and tells you how to proceed. See Figure 8-1 for an example of a CA Anti-Spyware warning message.

Figure 8-1: CA Anti-Spyware warning example

  If a scan detects a specific type of spyware that requires you to restart your computer to remove it (for example, spyware that has installed itself in your Windows startup programs list), CA Anti-Spyware prompts you to restart your computer and describes the reason for the restart.

- **On-demand Scanning**
  - **Quick Scan:** Scans memory and common spyware locations in about 3 minutes. Quick Scan can find about 98 percent of the spyware on your system.
  - **Select Files and Folders to Scan:** Allows you to choose what to scan. You can scan the full hard drive or just one folder.

- **Scheduled Scanning**
  - **Scheduled Scan.** Runs a quick scan of common spyware locations and memory. The default schedule is once after installation and then once every 30 days.
  - **Run a Scan at Startup.** Runs a quick scan when your computer boots. This is an easy way to ensure your PC is protected from new threats, because the scan at startup typically occurs right after a product update is performed. You must select this option from the Options tab.

Note

Because remote control applications, browser plug-ins, and network traffic analysis tools can be potentially harmful to network and system security, CA Anti-Spyware detects them as spyware.

If you use these programs, it's recommend that you exclude them from the Spyware scanning. Refer to the following sections for more information:

"Excluding Files or Folders from On-Demand Spyware Scanning"

"Excluding Files or Folders from Real-Time Spyware Scanning"

CA Anti-Spyware Introduction

The CA Anti-Spyware screens are organized to allow quick access to the common functions and features. The following sections discuss the main screens of CA Anti-Spyware, which you access by opening the appropriate tabs in the software.

Open CA Anti-Spyware

There are a few ways to open CA Anti-Spyware:

- **CA Security Center**

  You can quickly access CA Anti-Spyware from the CA Security Center:

  1. Double-click the CA Security Center system tray icon, as shown in Figure 8-2.

Figure 8-2: Double-clicking the system tray icon

2. Expand the CA Anti-Spyware component panel; click on its arrow, icon, or name.
3. Click Open Advanced Settings, as shown in Figure 8-3.

Figure 8-3: Opening CA Anti-Spyware

- **System Tray Icon**

  You can also use the system tray icon to open CA Anti-Spyware:

  1. Right-click the CA Security Center system tray icon, as shown in Figure 8-4.

Figure 8-4: Right-clicking the system tray icon

2. Select CA Anti-Spyware
3. Click Open CA Anti-Spyware (see Figure 8-5).

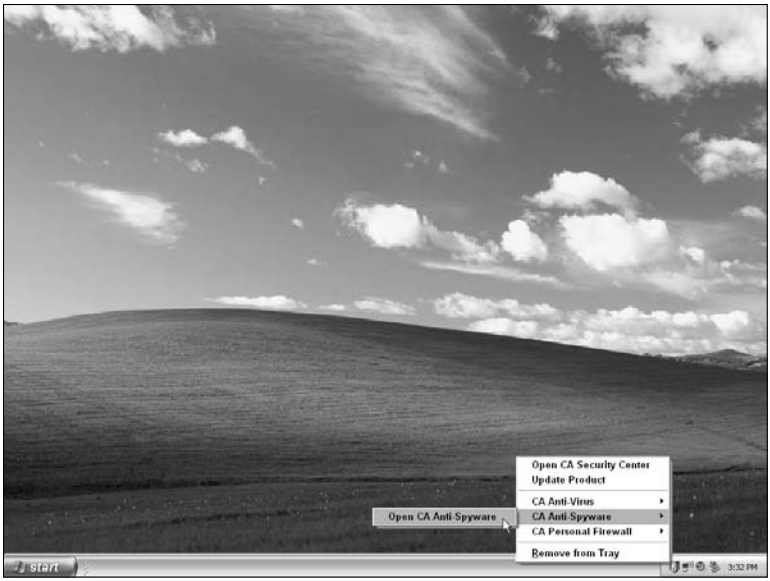

Figure 8-5: Opening CA Anti-Spyware

- **Start Menu**

  If you have something against using the system tray icon and security center, or if the icon has disappeared, don't worry. Take a breath and browse to the following path on your Start menu:

  Programs (or All Programs) ➔ CA ➔ CA Internet Security Suite ➔ CA Anti-Spyware

  Then click on CA Anti-Spyware, as shown in Figure 8.6.

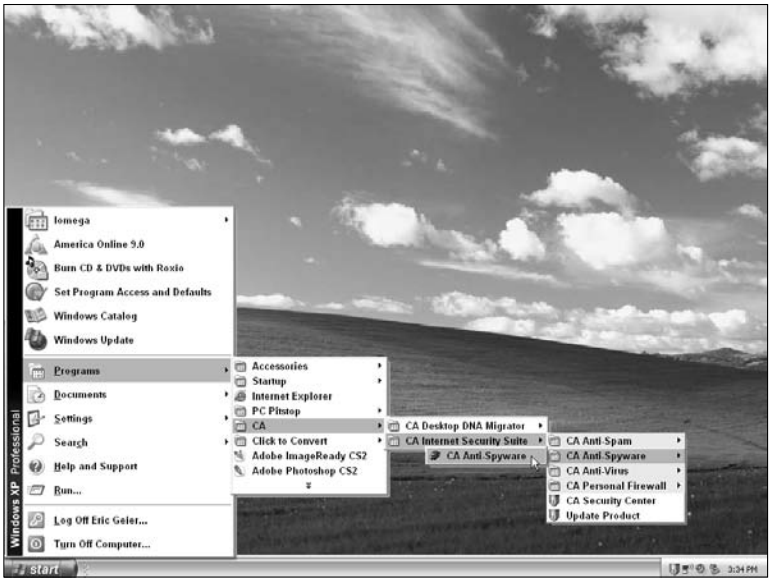

Figure 8-6: Opening CA Anti-Spyware from the Start menu

Overview Screen

Figure 8-7 shows the Overview screen in CA Anti-Spyware. From this screen, you can check the status of the product, fix any problems with the product, and review the latest threats.

In addition, you can access the following main tasks of CA Anti-Spyware from the Overview screen:

- **Start a Quick Scan**

  You can perform a Quick Scan which scans memory and common spyware locations in about 3 minutes. Quick Scan can find about 98% of the spyware on your system.

- **Select Files and Folders to Scan (Perform Selective Scans)**

  You can direct CA Anti-Spyware to perform an on-demand scan of specific drives, files, and folders.

- **Help CA Fight Spyware**

  You can participate in CA's ongoing spyware research by submitting your scan results to their research department. No personal data is sent with your scan results, and you can discontinue your participation at any time.

Figure 8-7: CA Anti-Spyware Overview screen

The following status indicators are used on the Overview screen to show you the current status of the CA Anti-Spyware software (see Figure 8-8):

Figure 8-8: CA Anti-Spyware status indicators

- **Real-time Protection**

Identifies whether real-time anti-spyware protection is enabled on your computer.

- **Last Product Update**

  Identifies the date of the last spyware signature update. If the product hasn't been updated within 7 days, an Update Now link appears, which you can click to update the product. However, if the product has been updated within the past 7 days, you can click Update at the top of the screen to schedule the next update.

- **Last Scan for Spyware**

  Identifies the date of the last spyware scan run on your computer. If a scan has been done in the past 30 days, you can click Start a Quick Scan in the main tasks; otherwise, click the Scan Now link.

- **Product License**

  Identifies the expiration date of your product license.

  If your license has expired or is due to expire within the next 30 days, you can click the Renew Now link to renew your product license online.

The status section also includes the Secure Now button, which you click to fix issues associated with your anti-spyware software.

In addition, the Latest Threats section of the Overview tab displays information about the most common and latest known spyware threats.

Quarantine Screen

The Quarantine screen (shown in Figure 8-9) displays a list of spyware that has been quarantined by CA Anti-Spyware and the total number of quarantined items.

Figure 8-9: CA Anti-Spyware Quarantine screen

This screen contains the following items:

- **Quarantine List**

  Identifies spyware that the product has quarantined and provides the following information about each item:

  - **Session:** Displays the session in which the spyware was quarantined.
  - **Infection Name:** Displays the name of the spyware.
  - **Infection Type:** Displays the type of spyware detected.
  - **File Name:** Displays the name of the file.
  - **File Location:** Displays the path of the file.
  - **Date/Time:** Displays the date and time of the scan in which the item was detected.
  - **More Information:** Provides a link to the CA Security Advisor website for more information about the detected spyware.

- **Restore**

  Releases items from the Quarantine List and restores them to their original locations.

- **Delete**

  Deletes the listed items from the Quarantine List and from your computer.

- **Save Report**

  Saves the current Quarantine List as a comma-separated value (CSV) text file.

Options Screen

From the Options screen (shown in Figure 8-10), you can change any settings or preferences related to the anti-spyware component.

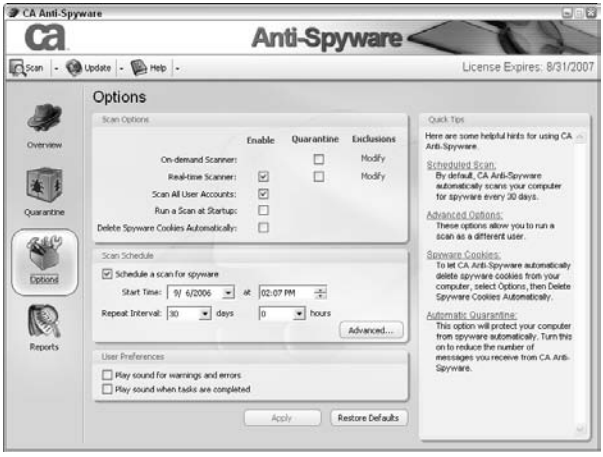

Figure 8-10: CA Anti-Spyware Options screen

This screen contains the following items:

- **Scan Options**

  CA Anti-Spyware provides the following options to help you scan for spyware:

  - **On-Demand Scanner:** You use this option to schedule an on-demand scan or initiate an immediate scan. It enables you to check your local computer for spyware and set options for managing detected files before you run a scan.

Note

This type of scan is enabled by default and cannot be disabled.

- **Real-Time Scanner:** By detecting malicious activity as it occurs, CA Anti-Spyware prevents and removes unwanted ActiveX controls, Browser Helper Objects, and browser toolbars; prevents malicious changes to the Windows Hosts file, Registry, and Startup Programs list; and protects Internet Explorer settings, including your home page, favorites, and search pages. This new functionality builds on existing real-time capabilities to detect and remove tracking cookies and spyware programs running in memory.
- **Scan All User Accounts:** This option, which is enabled by default, scans all the user accounts on your computer.
- **Run A Scan At Startup:** This option is turned off by default. If you enable it, CA Anti-Spyware launches a silent scan each time you start your computer. If spyware is detected during the scan, information about the detected spyware is displayed.
- **Delete Spyware Cookies Automatically:** This option is turned off by default. If you enable it, CA Anti-Spyware automatically scans for and deletes spyware cookies.

- **Scan Schedule**

  You can schedule scans to repeat on a regular basis. By default CA Anti-Spyware automatically runs a scan after installation, and then every 30 days.

- **User Preferences**

  You can configure CA Anti-Spyware to use sounds to alert you when the following conditions occur:

  - Warning and errors
  - Tasks are completed

In addition, the Options screen provides a Quick Tips section that contains information and answers to frequently asked questions about spyware and CA Anti-Spyware.

Reports Screen

The Reports screen (shown in Figure 8-11) displays reporting statistics and lets you view logs to track information about your protection status.

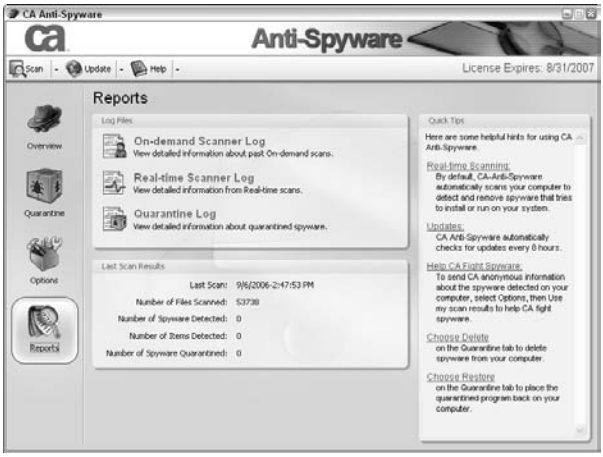

Figure 8-11: CA Anti-Spyware Reports screen

This screen contains the following items:

- **Log Files**

  This section provides access to the following logs:

  - **On-Demand Scanner Log:** Displays the results of past on-demand scans.
  - **Real-Time Scanner Log:** Displays the results of past real-time scans.
  - **Quarantine Log:** Displays information about quarantined spyware.

- **Last Scan Results**

  This section displays the following statistics about your last anti-spyware scan:

  - The date and time of your last scan
  - The number of files scanned in your last scan
  - The number of spyware programs detected by CA Anti-Spyware
  - The number of items detected by CA Anti-Spyware
  - The number of spyware programs quarantined

In addition, the Reports screen provides a Quick Tips section that contains information and answers to frequently asked questions about spyware and CA Anti-Spyware.

Common Tasks

This section provides step-by-step instructions for common tasks relating to the anti-spyware component.

Secure Now

You can use the Secure Now feature in CA Anti-Spyware to fix problems associated with your anti-spyware software:

1. Select the Overview tab on the left side of the CA Anti-Spyware window.

   The Overview window appears.

2. Click Secure Now, as shown in Figure 8-12.

Figure 8-12: Securing CA Anti-Spyware

   The Secure Your System dialog appears and describes the actions CA Anti-Spyware will take to protect your system.

3. Click Continue.

   The product automatically performs tasks depending on the issues that need to be addressed. These tasks can include any or all of the following:

   - Renew your license if it is close to expiring to ensure that your system is continuously protected from spyware.
   - Enable real-time protection to automatically scan your computer and detect and remove spyware that attempts to install or run on your system.

- Update your system with the latest available signature files to ensure that you are protected from the latest spyware threats.
- Scan your computer for spyware if you have not run a scan in the past 30 days.

Perform a Quick Scan

You can quickly scan common locations on your computer for spyware:

1. Select the Overview tab on the left side of the CA Anti-Spyware window.

   The Overview window appears.

2. Click Start a Quick Scan, as shown in Figure 8-13.

Figure 8-13: Starting a Quick Scan

The CA Anti-Spyware Scan window appears, as shown in Figure 8-14, and the scan begins.

As items are detected, they appear in the Scan Results list. The Scanner Status field displays the path name of the object currently being scanned when the scanner is running or a Ready status when the scanner is inactive.

When the scan finishes, a dialog displays the number of items scanned.

Figure 8-14: CA Anti-Spyware Scan dialog

3. Click OK to close this dialog box.

The Spyware Detected and Items Detected fields display the number of suspicious items and spyware detected by the scan.

4. Specify the action that CA Anti-Spyware should take for the spyware and suspicious items detected by the scan. You can move all spyware discovered during a scan to a quarantine location, from which you can either delete or release it after you evaluate it, or you can add individual items discovered during a scan to your Exclusion list to exempt these items from future scans.

To specify the action to take for detected items:

a. Select individual entries from the Scan Results list or select the Select/Deselect All check box to select all of the entries in the list.

b. (Optional) Click Exclude Selected Spyware.

Selected items are added to the On-demand Scanner Exclusion list and are exempted from subsequent on-demand anti-spyware scans.

c. (Optional) Click Quarantine All Spyware.

The items in the Scan Results list are moved to the Quarantine List.

5. Click Close to exit the CA Anti-Spyware Scan window.

Perform a Selective Scan

You can direct CA Anti-Spyware to perform an On-demand scan of specific drives, files and folders:

1. Select the Overview tab on the left side of the CA Anti-Spyware window.

   The Overview window appears.

2. Click Select Files And Folders To Scan, as shown in Figure 8-15.

Figure 8-15: Starting a selective scan

The Select Files and Folders to Scan dialog appears, as shown in Figure 8-16.

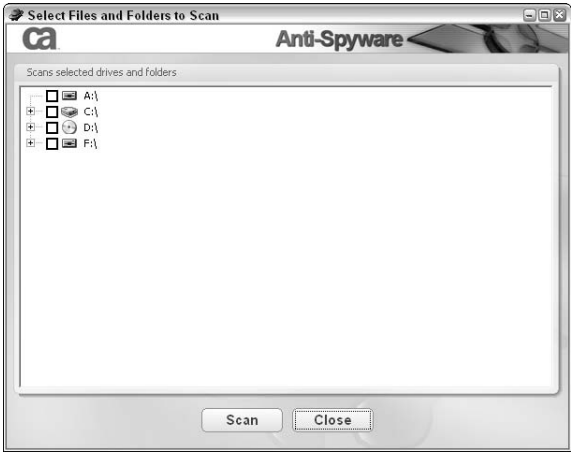

Figure 8-16: Select Files and Folders to Scan dialog

3. Select the check boxes for the drives, files and folders that you want to scan.

Note
When you select a folder, all of its subfolders are also selected.

4. Click Scan.

   The CA Anti-Spyware Scan dialog appears and the scan begins. As items are detected, they appear in the Scan Results list. The Scanner Status field displays the path name of the object currently being scanned when the scanner is running or a Ready status when the scanner is inactive.

   When the scan finishes, a dialog displays the number of items scanned.

5. Click OK to close this dialog box.

   The Spyware Detected and Items Detected fields display the number of suspicious items and spyware detected by the scan.

6. Specify the action to take for the spyware and suspicious items detected by the scan. You can move all spyware discovered during a scan to a quarantine location, from which you can either delete or release it after you evaluate it, or, you can add individual items discovered during a scan to your Exclusion list to exempt these items from future scans.

   To specify the action to take for detected items:

   a. Select individual entries from the Scan Results list or select the Select/Deselect All check box to select all of the entries in the list.

   b. (Optional) Click Exclude Selected Spyware.

      Selected items are added to the On-demand Scanner Exclusion list and are exempt from subsequent on-demand anti-spyware scans.

   c. (Optional) Click Quarantine All Spyware.

      The items in the Scan Results list are moved to the Quarantine List.

7. Click Close.

   The CA Anti-Spyware Scan dialog closes.

8. Click Close again.

   The Scan Files or Folders dialog closes.

Turn Real-Time Protection On or Off

Real-time protection, which is enabled by default, automatically scans your computer to detect and remove spyware that attempts to install itself or run on your system. However, you can enable or disable this real-time protection at any time:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. Continue with the next steps depending upon if you're enabling or disabling:

   To enable the Real-time Scanner:

   a. In the Scan Options area, check the Real-time Scanner check box, as shown in Figure 8-17.

   b. Click Apply.

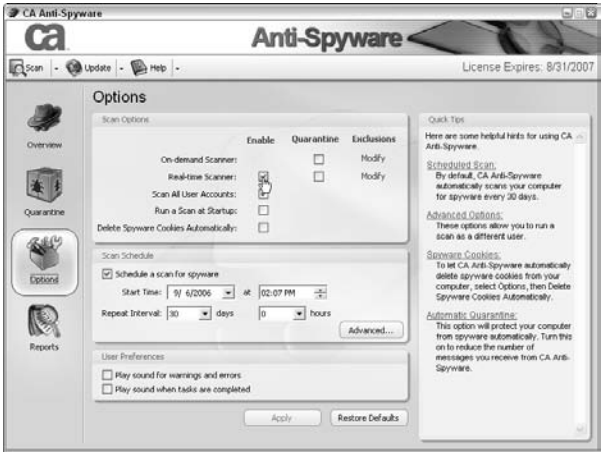

Figure 8-17: Enabling the CA Anti-Spyware real-time scanner

To disable the Real-time Scanner:

a. In the Scan Options area, uncheck the Real-time Scanner check box, as shown in Figure 8-18.

b. Click Apply.

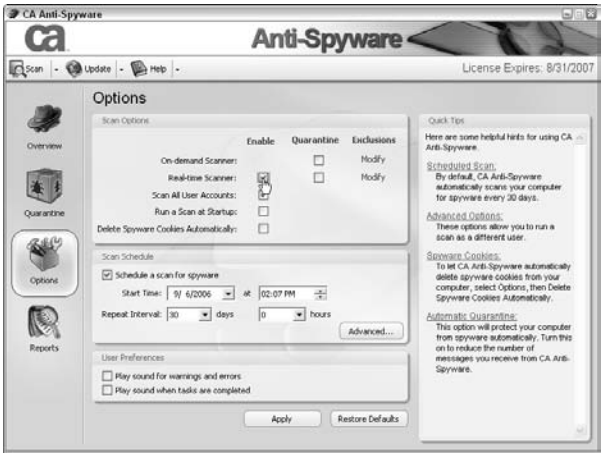

Figure 8-18: Disabling the CA Anti-Spyware real-time scanner

Schedule Automatic Scans

You can schedule spyware scans to repeat on a regular basis:

Note

By default, CA Anti-Spyware runs a scan every 30 days.

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. Check the Schedule A Scan For Spyware box, as shown in Figure 8-19.

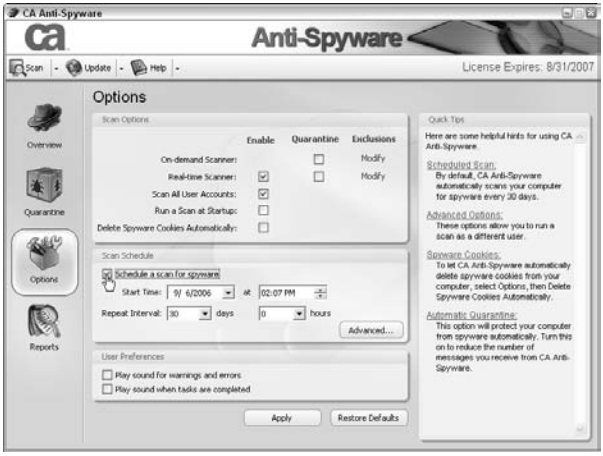

Figure 8-19: Enabling a scheduled scan

The scheduling fields in the Scan Schedule area become active.

3. Select a date and time for the scheduled scans to begin.
4. Select a repeat interval for the scheduled scans.
5. (Optional) Click Advanced to access advanced scheduling options.

   The Advanced Options dialog appears, as shown in Figure 8-20.

Figure 8-20: Advanced Options dialog box

Using the Advanced Options dialog, you can specify the user the scheduled scan applies to. You can specify that the scheduled scan is to run only when the current user or another specific user is logged in.

To specify a user:

a. Click one of the options on the Advanced Options dialog.

   If you clicked The current user, the scheduled scan will run only if the user currently logged in to this machine is logged in.

   If you clicked This user, the scheduled scan will run only if the specified user is logged in.

   The Account and Password fields are enabled.

b. If you clicked This user, enter the user name and password for the user for whom the scheduled scans apply in the Account and Password fields.

c. Click OK to exit the Advanced Options dialog.

Note
To specify that the scheduled scan should run for all users logged into the computer, enable the Scan All User Accounts option in the Scan Options section of the Options tab.

6. Click Apply. Your changes are saved and your specified schedule becomes active.

Advanced Tasks

This section provides step-by-step instructions for CA Anti-Spyware tasks that are less commonly performed.

Specify Scan Options

You can specify settings for your spyware scans:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the Scan Options area (shown in Figure 8-21), select the appropriate check boxes to enable or disable the following:

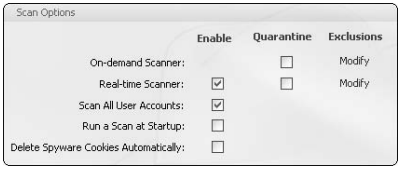

Figure 8-21: Scan options

   - Real-Time Scanner
   - Scan All User Accounts
   - Run A Scan At Startup
   - Delete Spyware Cookies Automatically

Note
The on-demand scanner is enabled by default and cannot be disabled.

3. Select the Quarantine check box next to On-demand Scanner or Real-time Scanner to specify that items detected during these types of scans are automatically held in quarantine until you review and approve them.
4. Click the Modify link next to On-demand Scanner or Real-time Scanner to create Exclusion lists for these scan types, or to add or remove files, directories, or drives from the Exclusion list.
5. When you have specified all of your settings, click Apply.

Exclude Files or Folders from On-Demand Spyware Scanning

When necessary, you can exclude certain files or folders from being scanned by the on-demand scanner, or exclude certain spyware from the scans (such as files that trigger a false detection).

Add Files or Folders to the Excluded Files/Folders List

Follow these steps to exclude files and/or folders from being scanned for spyware by the on-demand scanner:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.
2. In the Scan Options section, click the Modify link next to On-demand Scanner, as shown in Figure 8-22.

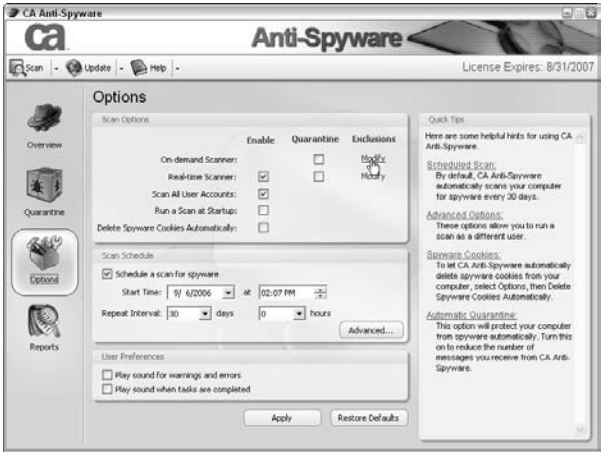

Figure 8-22: Accessing the Excluded Files/Folders and Spyware lists

The Modify Exclusions dialog appears. The Modify Exclusions dialog provides a list of spyware and a list of files or folders that are currently excluded from scans.

3. Click Browse.

   The Please select a file dialog appears, listing all files and folders.

4. Select the items to be excluded from scans (see Figure 8-23 for an example), and then click OK.

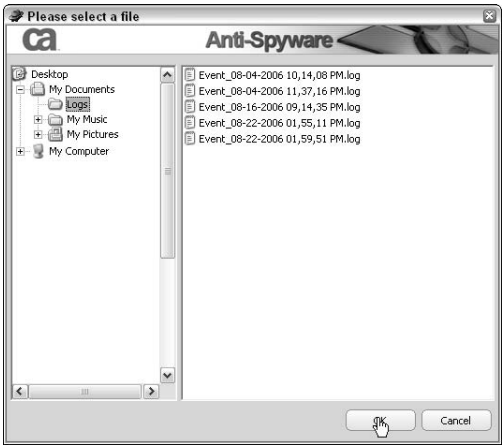

Figure 8-23: Adding files or folders to the Excluded Files/Folders list

   The Please select a file dialog closes and the selected files or folders are added to the Exclusion list.

5. Click the Close button to apply your changes and exit the Modify Exclusions dialog box.

Remove Items from the Excluded Files/Folders or Spyware List

You can modify the Excluded Files/Folders List (for the On-demand Scanner) by following these steps:

1. Select the Options tab on the left side of the CA Anti-Spyware window. The Options window appears.

2. In the Scan Options section, click the Modify link next to On-Demand Scanner, as shown in Figure 8-24.

   The Modify Exclusions dialog appears. The Modify Exclusions dialog provides a list of spyware and a list of files or folders to be excluded from scans.

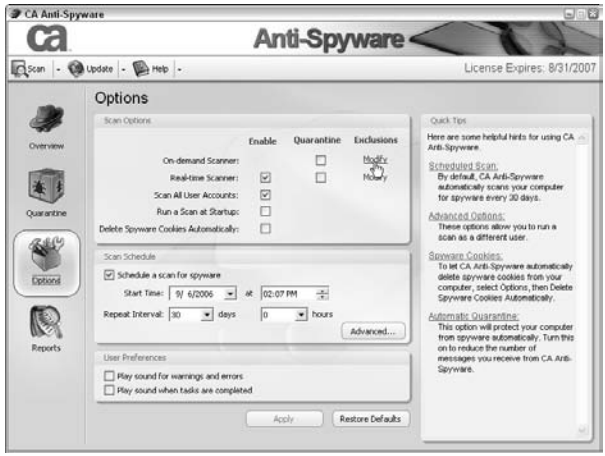

Figure 8-24: Accessing the Excluded Files/Folders and Spyware lists

3. Select the items to be removed from the exclusion list.

Note

You can click Select/Deselect All to select all of the items from the list.

4. Click Remove Selected Exclusions to indicate that these items should now be included in scans. See Figure 8-25 for an example.

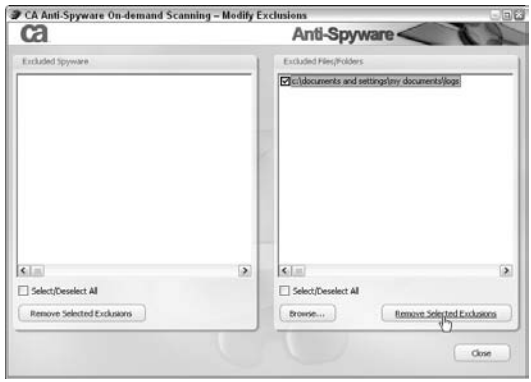

Figure 8-25: Removing items from the Excluded Files/Folders or Spyware lists

5. Click Close to apply your changes and exit the Modify Exclusions dialog box.

Exclude Files or Folders from Real-Time Spyware Scanning

When necessary, you can exclude certain files or folders from being scanned by the real-time scanner, or to exclude certain spyware from the scans (for example, if problems arise in certain files that trigger an unwanted detection).

Add Files or Folders to the Excluded Files/Folders List

Follow these steps to exclude files and/or folders from being scanned for spyware by the real-time scanner:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the Scan Options section, click the Modify link next to Real-Time Scanner, as shown in Figure 8-26.

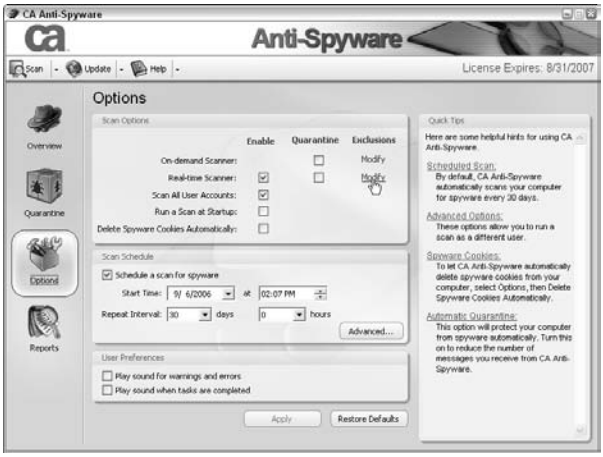

Figure 8-26: Accessing the Excluded Files/Folders and Spyware lists

   The Modify Exclusions dialog appears. The Modify Exclusions dialog provides a list of spyware and a list of files or folders to be excluded from scans.

3. Click Browse.

   The Please select a file dialog appears, listing all files and folders.

4. Select the items to be excluded from scans (see the example in Figure 8-27) and click OK.

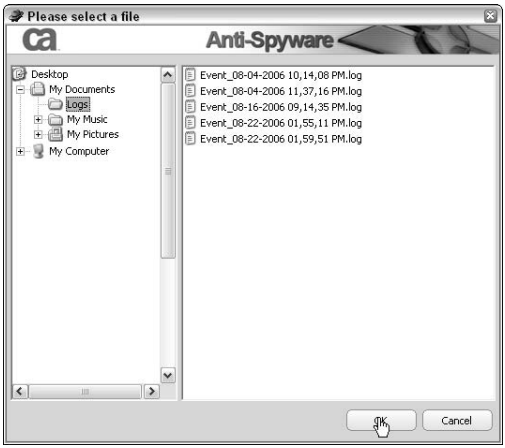

Figure 8-27: Adding files or folders to the Excluded Files/Folders list

The Please select a file dialog closes and the selected files or folders are added to the Exclusion list.

5. Click Close to apply your changes and exit the Modify Exclusions dialog box.

Remove Items from the Excluded Files/Folders List or Spyware List

Follow these steps to modify the Excluded Files/Folders list for the real-time scanner:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the Scan Options section, click the Modify link next to Real-Time Scanner, as shown in Figure 8-28.

   The Modify Exclusions dialog appears. The Modify Exclusions dialog provides a list of spyware and a list of files or folders to be excluded from scans.

Figure 8-28: Accessing the Excluded Files/Folders and Spyware lists

3. Select the items to be removed from the Exclusion list.

Note

You can click Select/Deselect All to select all of the items from the list.

4. Click Remove Selected Exclusions to indicate that these items should now be included in scans. See Figure 8-29 for an example.

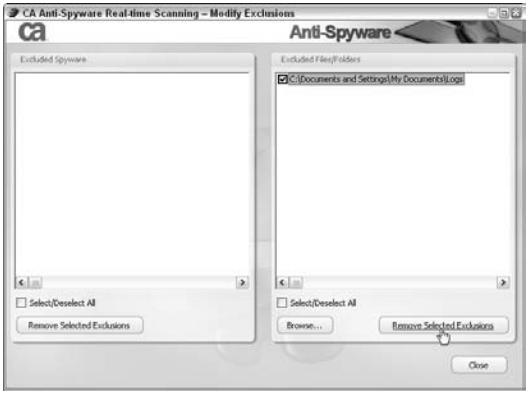

Figure 8-29: Removing items from the Excluded Files/Folders or Spyware list

5. Click Close to apply your changes and exit the Modify Exclusions dialog box.

Exclude Specific Spyware from Spyware Scans

When necessary, you can exclude certain spyware from trigger alerts or detection, such as when problems arise in certain files that trigger a false or unwanted detection. Excluding spyware from scanning can only be done just after a completed spyware scan or detection.

For On-Demand Scanning Exclusion

1. Perform a spyware scan.
2. After the scan has completed, check the spyware that you would like to exclude from scanning in the CA Anti-Spyware Scan window and click Exclude Selected Spyware. See Figure 8-30 for an example.

Figure 8-30: Excluding selected spyware

For Real-Time Scanning Exclusion

1. From the Real-time Spyware Detection Dialog click Exclude, as Figure 8-31 shows.

Figure 8-31: Excluding selected spyware

Working with Quarantined Items

This section discusses the common tasks relating to quarantined items.

View Quarantined Items

To display files that have been quarantined, you can view your quarantined items list:

1. Select the Quarantine tab on the left side of the CA Anti-Spyware window.

   The Quarantine window appears and shows your quarantined items, as seen in Figure 8-32.

Figure 8-32: Quarantine window

Note

For more information about the details of quarantined items see the "Quarantine Screen" section earlier in this chapter.

Delete Items

Follow these steps to remove unwanted quarantined items from your computer:

Note

When you restore or delete quarantined files, all files quarantined during that session (and all subsequent sessions) are also restored or deleted. You cannot restore or delete individual items from scans, only groups of items found during the same scan and all subsequent scans.

1. Select the Quarantine tab on the left side of the CA Anti-Spyware window.

   The Quarantine window appears, listing your quarantined items.

2. Select the scan session that you want to delete from the Quarantine List (as shown in the example in Figure 8-33), and then click Delete.

   The items detected during that session (and all subsequent sessions) are removed from the list and from your computer.

Figure 8-33: Removing items from the Quarantine List

Restore Items

To revert the quarantining of selected items, you can restore selected quarantined items to their original location:

Note

When you restore or delete quarantined files, all files quarantined during that session (and all subsequent sessions) are also restored or deleted. You cannot restore or delete individual items from scans, only groups of items found during the same scan and all subsequent scans.

1. Select the Quarantine tab on the left side of the CA Anti-Spyware window.

   The Quarantine window appears, listing your quarantined items.

2. Select the scan session that you want to restore from the Quarantine List (see Figure 8-34 for an example), and then click Restore.

Figure 8-34: Restoring items from the Quarantine List

The items are removed from the Quarantine List and restored to their original locations.

Enable or Disable Automatic Quarantine

If it becomes necessary, you can enable or disable the automatic quarantine of detected infections, for each type of scanning method:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the Scan Options area, check or uncheck the Quarantine box for either the On-Demand and/or Real-Time Scanner rows (see Figure 8-35).

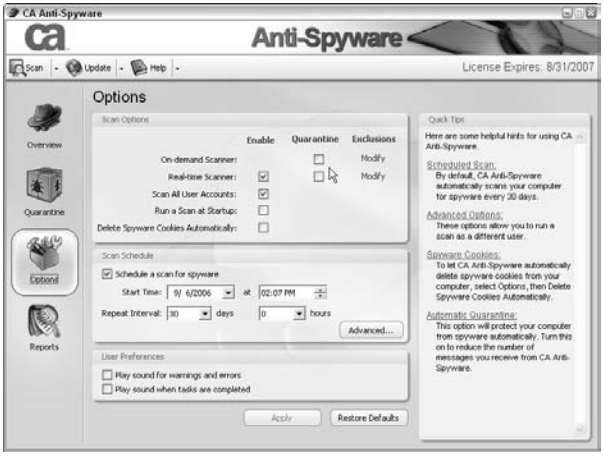

Figure 8-35: On-Demand and Real-Time Scanner Quarantine check boxes

3. Click Apply.

Scanning Multiple User Accounts

If you have multiple user accounts on your computer, you can configure CA Anti-Spyware to include all of these accounts during scans:

Note
This option is enabled by default.

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the Scan Options area, check or uncheck the Scan All User Accounts check box (see Figure 8-36), depending on whether you want the feature enabled or disabled.

3. Click Apply.

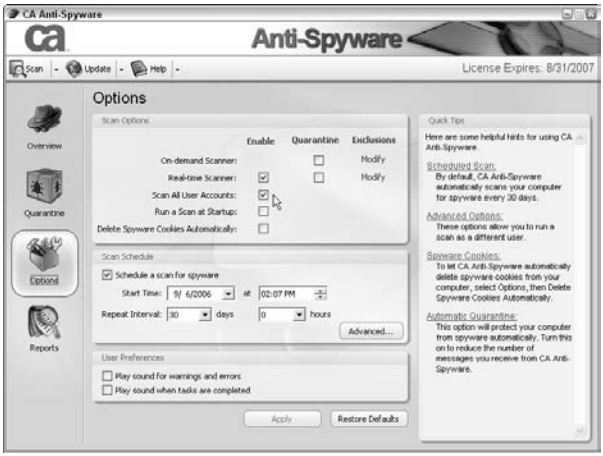

Figure 8-36: Scan All User Accounts check box

Note
This setting applies to all scans, including scheduled scans.

Configure Alert Sounds

You can configure CA Anti-Spyware to use sounds to alert you when a task is complete or to indicate warnings or errors:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. In the User Preferences section (shown in Figure 8-37), check or uncheck the following options:

   - Play sound for warnings and errors
   - Play sound when tasks are completed

Figure 8-37: User Preferences section

3. Click Apply.

   CA Anti-Spyware will alert you with a sound when the specified condition exists.

Restore Scan Settings Defaults

You can use the Restore Defaults feature to reset your scan options to the default settings:

1. Select the Options tab on the left side of the CA Anti-Spyware window.

   The Options window appears.

2. Click Restore Defaults, as shown Figure 8-38.

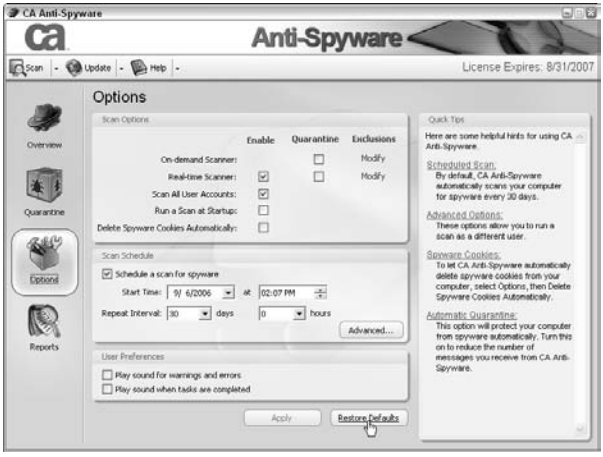

Figure 8-38: Restoring scan settings to defaults

   All settings, including any schedules you have set, are restored to the default settings.

3. Click Apply.

   Your changes are saved.

Submit Files to CA Research

You can participate in CA's ongoing spyware research by submitting your scan results to their research department. No personal data is sent with your scan results, and you can discontinue your participation at any time.

Note

By default, this option is disabled. You must enable it to participate in the research.

1. Select the Overview tab on the left side of the CA Anti-Spyware window.

   The Overview window appears.

2. Click Help CA Fight Spyware, as shown in Figure 8-39.

Figure 8-39: Helping CA fight spyware

   The Help CA Fight Spyware dialog appears.

3. Check the Use my scan results to help CA fight spyware option, as shown in Figure 8-40.

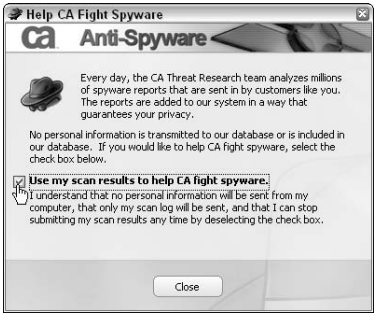

Figure 8-40: Help CA Fight Spyware option

4. Click Close.

   Scan results from future scans will be sent anonymously to the CA Threat Research team for analysis.

9

BLOCKING SPAM

The anti-spam component of CA Internet Security Suite (CA Anti-Spam) helps reduce or eliminate the spam you receive. It is an effective and easy-to-use spam filter that delivers messages from approved senders to your Inbox and automatically quarantines all other messages for later review.

This chapter is organized into these main sections:

- **Setting Up CA Anti-Spam**

  This section discusses the setup wizard, which helps you specify the initial settings of CA Anti-Spam.

- **CA Anti-Spam Introduction**

  This section takes you through all the menus of CA Anti-Spam and lets you know where everything is located and what each option does.

- **Common Tasks**

  This section provides step-by-step instructions for common CA Anti-Spam tasks.

- **Advanced Tasks**

  This section provides step-by-step instructions for CA Anti-Spam tasks performed less often.

Setup CA Anti-Spam

The setup wizard runs the first time you open Microsoft Outlook or Microsoft Outlook Express after you install CA Internet Security Suite. This wizard helps you to set the initial options for CA Anti-Spam.

Note

If you don't use the setup wizard (for example, if you've already opened Microsoft Outlook and canceled the wizard, and it won't appear again), you can still use CA Anti-Spam by enabling it in the Options menu, as discussed in the Accessing the CA Anti-Spam Toolbar Menu section later in this chapter.

1. Open Microsoft Outlook or Microsoft Outlook Express.

   The CA Anti-Spam Welcome page appears, identifying the features you can enable:

   - **CA Anti-Spam and Anti-Fraud:** Enable this feature to protect your computer against spam, phishing scams, and fraud.
   - **CA Anti-Spam Email Search:** Select this to enable the Search feature that indexes your saved mail, contacts, appointments, tasks, and notes for search purposes.

2. Select the features you want to set up and click Next.

Note

Click the Learn More link next to each feature to access a website with more information about the feature. It's recommend that you enable both features.

   CA Anti-Spam scans your email messages to compile a list of approved senders.

3. Click Next until the scan finishes.

   During the scan, CA Anti-Spam also installs the necessary libraries to support the search features and adds the CA Anti-Spam toolbar to Microsoft Outlook or Microsoft Outlook Express.

Note

You are prompted to click Next and page through several screens during the course of the scan. These pages provide information about CA Anti-Spam and the setup process.

4. Click Build Index to create an index of your email, contacts, appointments, tasks, and notes to enable you to use the Search feature.

When the setup process finishes (it might take a considerable amount of time to build the index, depending on the size of your Inbox), a Welcome screen appears, providing access to support information and a list of frequently asked questions related to the use of CA Anti-Spam.

CA Anti-Spam Introduction

The Anti-Spam component doesn't have an interface like the other components. You access all CA Anti-Spam settings and preferences from a toolbar menu in Microsoft Outlook or Microsoft Outlook Express. The CA Security Center, however, does display the component status information for CA Anti-Spam, as shown in Figure 9-1.

Figure 9-1: CA Anti-Spam component area in CA Security Center

The following sections discuss the screens of CA Anti-Spam, which are accessed from the toolbar menu in Microsoft Outlook or Microsoft Outlook Express.

Accessing the CA Anti-Spam Toolbar Menu

Follow these steps to access the CA Anti-Spam toolbar menu, which is the only interface to configure the component settings and preferences:

1. Open Microsoft Outlook or Microsoft Outlook Express.
2. On the toolbar, click the CA Anti-Spam drop-down menu, as shown in Figure 9-2.

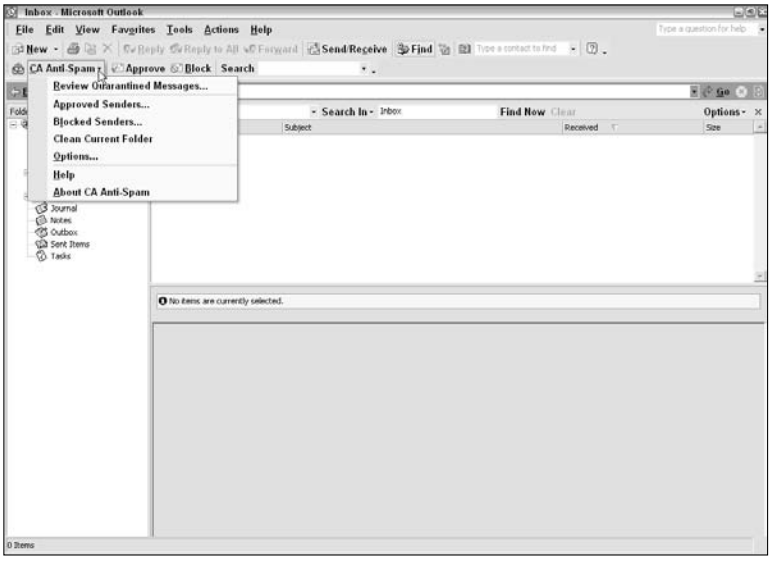

Figure 9-2: Accessing the CA Anti-Spam menu

If you can't find the CA Anti-Spam menu on the toolbar, right-click somewhere on the toolbar and select the CA Anti-Spam option, as shown in Figure 9-3.

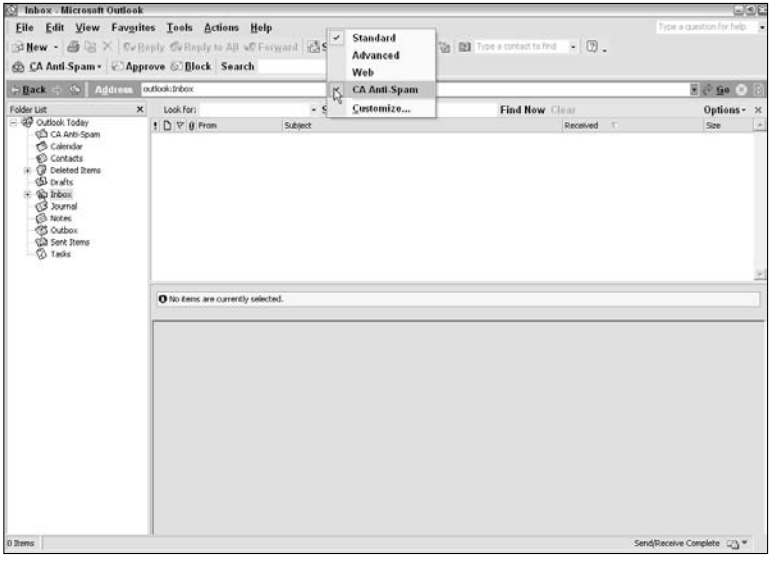

Figure 9-3: Enabling the CA Anti-Spam toolbar

If this toolbar isn't available in Microsoft Outlook or Microsoft Outlook Express, then CA Anti-Spam may not be properly installed. Refer to the CA Security Center for more information.

Note

If you didn't set up CA Anti-Spam using the setup wizard that appears the first time you start Microsoft Outlook or Microsoft Outlook Express after you installed CA Anti-Spam, and you want to use CA Anti-Spam, you'll need to enable it from the Start menu:

Start ➔ Programs (or All Programs) ➔ CA ➔ CA Internet Security Suite ➔ CA Anti-Spam

Then select Enable or Disable CA Anti-Spam.

Review Quarantined Messages Screen

The Unreviewed Quarantined Messages screen displays the quarantined messages that you have not yet opened, as shown in Figure 9-4. Here you can approve messages to move them from the Quarantined Messages list to your Inbox.

Figure 9-4: CA Anti-Spam Unreviewed Quarantined Messages screen

Approved Senders Screen

The CA Anti-Spam Approved Senders screen (shown in Figure 9-5) lets you view the list of senders you have approved to contact you through email. Here you can add and remove entries from the list and scan folders for new approved senders.

Figure 9-5: CA Anti-Spam Approved Senders screen

Blocked Senders Screen

From CA Anti-Spam Blocked Senders screen (shown in Figure 9-6), you can view the list of blocked senders whose messages are automatically quarantined upon receipt.

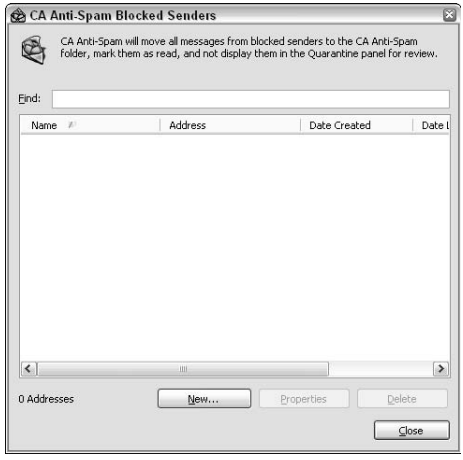

Figure 9-6: CA Anti-Spam Blocked Senders screen

Clean Current Folder Screen

This feature, which is accessible from the CA Anti-Spam drop-down menu (see Figure 9-7), moves all email that did not come from an approved sender from the folder you are currently using into quarantine.

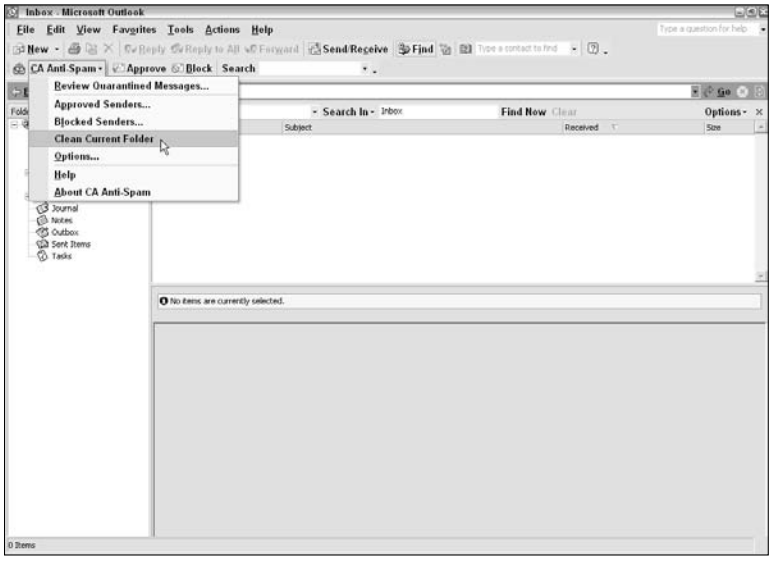

Figure 9-7: CA Anti-Spam Clean Current Folder screen

Options Screen

The CA Anti-Spam Options screen (shown in Figure 9-8) is where you configure all options for CA Anti-Spam, such as quarantine parameters, reminder schedules, spam scoring, search indexing, and the folders to be monitored for spam.

Figure 9-8: CA Anti-Spam Options screen

Quarantine Tab

The Quarantine tab (shown in Figure 9-9) lets you set parameters for your Quarantine folder. (This is the same screen as shown in Figure 9-8 because the Options screen and Quarantine tab are on the same screen.)

Figure 9-9: Options Screen Quarantine tab

- **Messages**
  - **Mark quarantined messages as read:** You can have CA Anti-Spam automatically mark quarantined messages as having been read. Therefore, the new message indicator in Microsoft Outlook will only alert you when you have messages from approved senders. New messages from unknown senders are added to your CA Anti-Spam folder without any visual indicators from Microsoft Outlook or Microsoft Outlook Express.
  - **Number of days to save quarantined messages:** You can specify the number of days that you want to retain quarantined messages in your CA Anti-Spam folder before CA Anti-Spam automatically and permanently deletes them. This feature ensures that you do not accidentally delete or lose important messages.

Note

Do not set a retention period of less than 7 days.

- **Reminders**
  - **Show quarantined message reminder:** You can configure CA Anti-Spam to remind you to review quarantined messages. This feature enables alerts to appear in the Windows system tray when quarantined messages are available for review or to set a schedule for these reminders.
  - **Show new quarantined messages when CA Anti-Spam folder is selected:** You can configure CA Anti-Spam to display the Unreviewed Quarantined Messages window automatically if you have unreviewed messages when you open the CA Anti-Spam folder in Microsoft Outlook.

Senders Tab

The Senders tab (shown in Figure 9-10) lets you specify whether CA Anti-Spam should automatically verify sender domains to test the authenticity of email messages.

Figure 9-10: Options Screen Senders tab

For example, when this feature is enabled, the following things occur:

- If a message is sent by a mail server known to be used by the sender of the message, a stamp indicates the domain from which the message was received.

- If a message was sent by a mail server that is not known to the sender of the message, a stamp warns you that the message was not verified.

Note

The Not Verified stamp indicates that messages may be fraudulent. Handle them with caution.

You should also note that not all email messages contain a stamp. For example, if the mail server doesn't support this verification process, no stamp will be placed on the message.

Spam Score Tab

The Spam Score tab (shown in Figure 9-11) lets you manage messages based on the likelihood that they are spam.

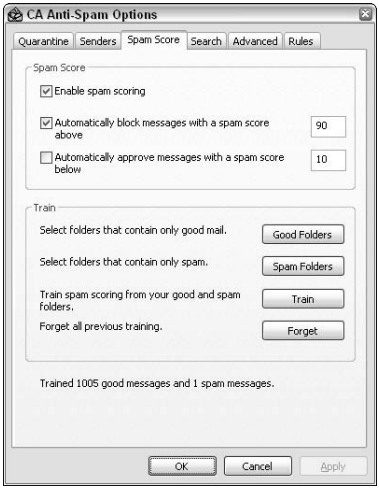

Figure 9-11: Options Screen Spam Score tab

- **Spam Score**

  You can enable automatic scoring of your incoming messages to identify the messages most likely to be spam.

  Spam scoring assigns the content of each quarantined message a score between 0 and 100, indicating the likelihood that the message is spam. The higher the spam score, the more likely the message is to be spam. A score of 100 indicates that CA Anti-Spam definitely identifies the message as spam.

- **Enable spam scoring:** This enables the use of the spam scoring and the training feature.
- **Automatically block messages with a spam score above:** You can indicate a specific spam score at which messages are automatically blocked and hidden from the list of quarantined messages shown in the Unreviewed Quarantined Messages window.
- **Automatically approve messages with a spam score below:** You can indicate a specific spam score at which messages are automatically approved and delivered to your Inbox.

Note

CA Anti-Spam does not automatically add the senders of these messages to your Approved Senders list.

- **Train**

  You can train CA Anti-Spam to identify good messages or spam to speed up the learning process by which CA Anti-Spam scores quarantined messages.

  Training is optional. If you do not use training, CA Anti-Spam automatically learns which messages are more likely to be spam by analyzing the quarantined messages that you approve over time.

  You can train CA Anti-Spam using folders that contain known good messages or known spam messages, or you can train CA Anti-Spam using both good and spam folders.

  - **Good Folders button:** Click this button to identify folders containing messages known to be good for training purposes.
  - **Spam Folders button:** Click this button to identify folders containing messages known to be spam for training purposes.
  - **Train button:** After you have selected at least one folder, containing good or spam emails, clicking this button will train CA Anti-Spam to score messages based on your specified entries.
  - **Forget button:** You can reset your CA Anti-Spam training by clicking this button to delete the previous training data, and then you can train CA Anti-Spam to recognize spam according to different criteria.

Search Tab

The Search tab, shown in Figure 9-12, contains indexing and searching options.

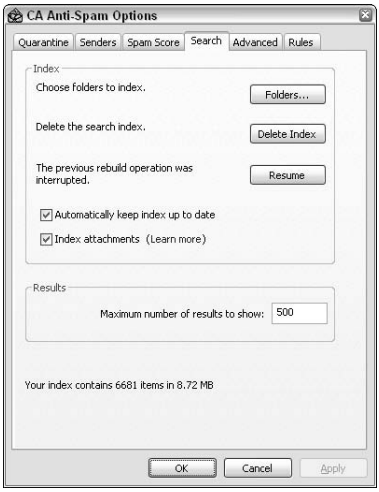

Figure 9-12: Options Screen Search tab

- **Index**

  Indexing organizes your email messages, contacts, appointments, tasks, and notes to enable quick searches using the Search feature. The Index area contains the following options:

  - **Folders button:** This button allows you to identify specific folders for CA Anti-Spam to index for search purposes. Use this feature to shorten the search time by confining searches to the folders most likely to contain the searched-for items.
  - **Delete Index button:** Clicking this button removes your existing search index, enabling you to re-index your messages to accommodate changes and improve the efficiency of the search feature.

Note

If you delete your search index, you cannot use the search feature until CA Anti-Spam rebuilds a search index of your saved messages, contacts, appointments, tasks, and notes.

- **Build Index button:** If CA Anti-Spam Search is enabled and you have not yet created a search index, if you've added folders to be indexed, or if you deleted an existing search index, you can click this button to build a search index.
- **Automatically keep index up to date:** You can configure CA Anti-Spam to update your search index automatically.
- **Index attachments:** You can configure CA Anti-Spam to include message attachments (for example, TXT files, HTML files, Microsoft Office documents, or PDF files) in your search index.

- **Results**
  - **Maximum number of results to show:** You can specify the maximum number of results to be displayed when you use the Search feature.

Advanced Tab

You can set advanced CA Anti-Spam options from the Advanced tab, as shown in Figure 9-13.

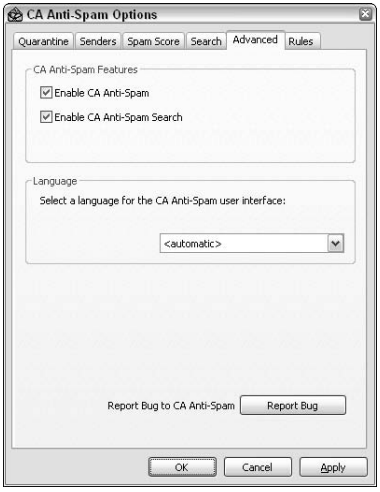

Figure 9-13: Options Screen Advanced tab

- **CA Anti-Spam Features**
  - **Enable CA Anti-Spam:** You can enable or disable CA Anti-Spam.
  - **Enable CA Anti-Spam Search:** You can enable or disable the Search feature of CA Anti-Spam.
- **Language**

  You can select a language to be used for CA Anti-Spam messages, panels, windows, and dialog boxes from the drop-down list.
- **Report Bug to CA Anti-Spam**

  You can open a technical support issue to report a problem with a product feature to CA. Reporting problems in this way provides CA with valuable product configuration information that can be used to identify and resolve product problems quickly.

Rules Tab

You can use the Rules tab (shown in Figure 9-14) to identify the folders that CA Anti-Spam should monitor for spam.

Figure 9-14: Options Screen Rules tab

Monitored folders work with Microsoft Outlook Rules to let you to create policies to deliver messages to folders other than the Inbox.

For example, if you create a rule that moves all mail sent to my-address@isp.com to the ISP-mail folder, you can direct CA Anti-Spam to monitor the ISP-mail folder and quarantine any new messages that arrive from unknown senders.

Note
This feature is not supported for Microsoft Outlook Express.

Menu Buttons

The following buttons, as shown in Figure 9-15, are available on CA Anti-Spam toolbar menu:

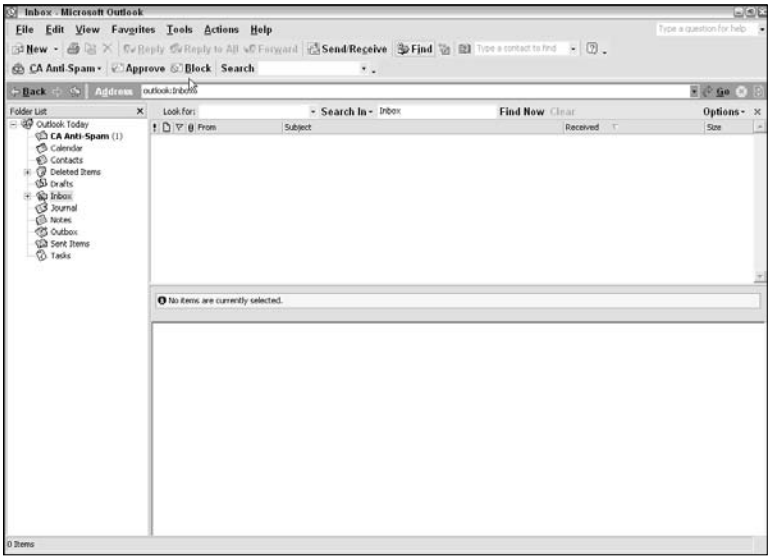

Figure 9-15: CA Anti-Spam toolbar buttons

- **Approve**

  Click this button to approve an email that's currently open, which will add the sender and all recipients of the message to the list of approved senders.

- **Block**

  Click this button to identify the currently open message as spam and move it to the CA Anti-Spam folder. Any messages received from that sender in the future are automatically quarantined and marked as read.

- **Search**

  When Search is enabled, this field appears on the toolbar. You can click this button or enter one or more keywords in the field to open the Search dialog box and generate a list of messages, contacts, tasks, notes, or appointments in which the keywords appear in the body or any of the attachments. Alternatively, you can click Search to open the Search window and access search options. In addition, you can use the down arrow to the right of the Search field to view keywords entered for previous searches.

Common Tasks

This section provides step-by-step instructions for common CA Anti-Spam tasks.

Review Quarantined Messages

CA Anti-Spam periodically alerts you to new messages that it has quarantined. After being alerted or at any time you can view new quarantined messages as follows:

1. Open the Review Quarantined Messages window using one of the following methods:
   a. Click the envelope icon next CA Anti-Spam in the toolbar menu, as shown in Figure 9-16.
   b. Select Review Quarantined Messages from the CA Anti-Spam toolbar menu, as shown in Figure 9-17.

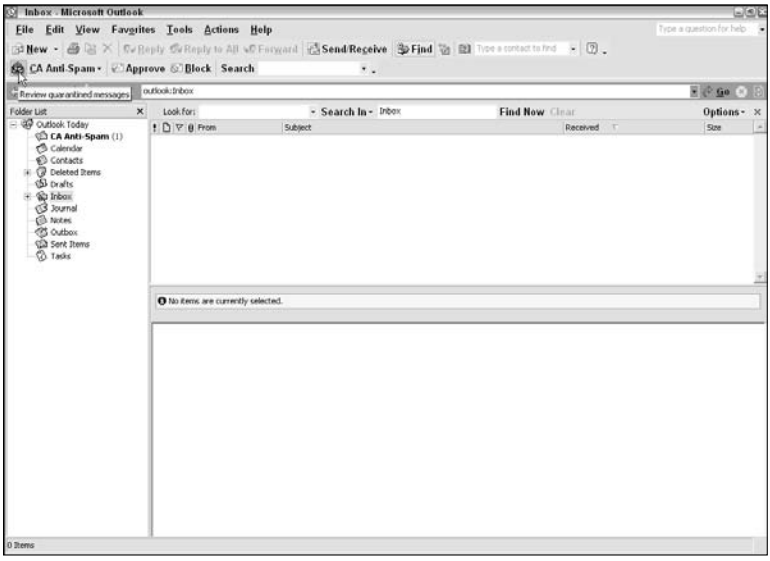

Figure 9-16: Opening the window with the Envelope icon

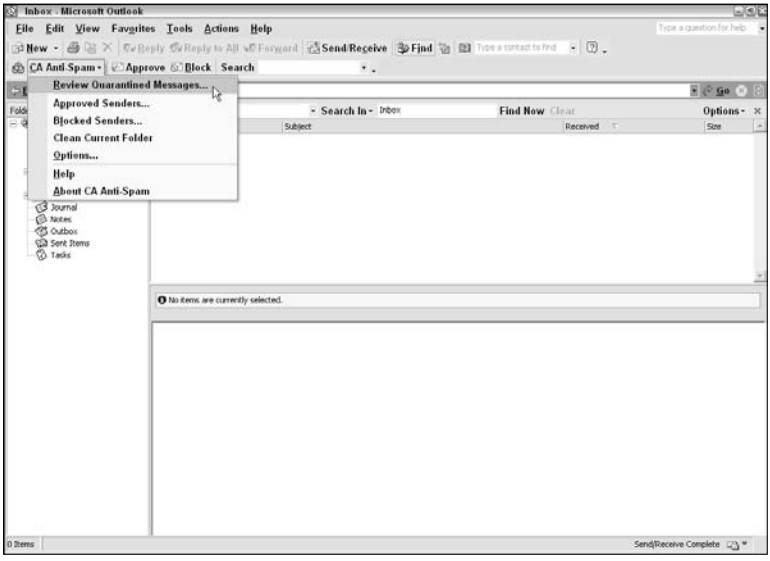

Figure 9-17: Opening the window using the toolbar menu list

c. Click the CA Anti-Spam folder in the Folder List, as shown in Figure 9-18.

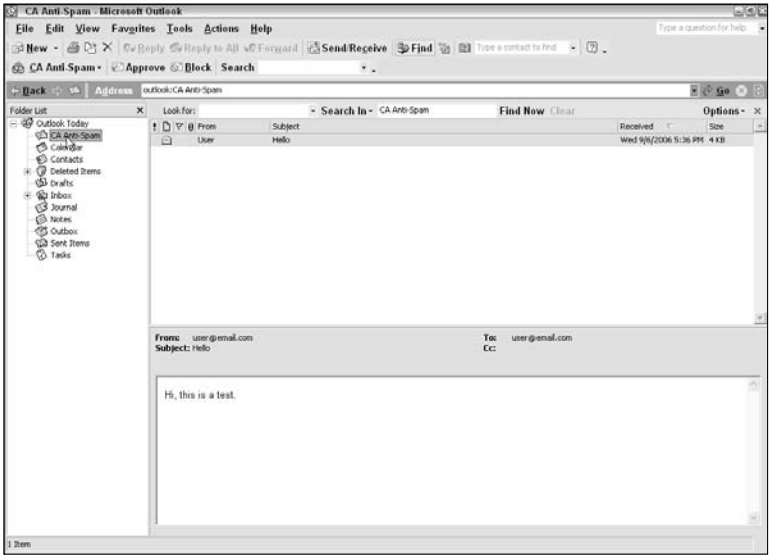

Figure 9-18: Opening the window from the CA Anti-Spam folder

Note

When you click the CA Anti-Spam folder, the Unreviewed Quarantined Messages window will be displayed only if there are new unreviewed messages.

The Unreviewed Quarantined Messages screen appears. It displays a list of messages that have not yet been reviewed and includes the sender of the message, the address from which it was sent, the subject of the message, the date and time received, and the spam score. In addition, the screen displays the number of new quarantined messages and the number of messages quarantined since installation.

2. (Optional) Select a message or messages you want to approve and click OK.

Note

To view the contents of the quarantined messages, hover your mouse over the envelope icon on the left-hand side of the screen.

The messages are moved to your Inbox and the sender's addresses in the messages are added to your Approved Senders list. Any remaining messages are left in the quarantine folder and marked as having been reviewed.

Note

You can specify the length of time quarantined messages are allowed to age before they are deleted on the Quarantine tab of the CA Anti-Spam Options.

Approve Messages and Senders

You can approve emails as you review them, and add the sender and all recipients of the message to the list of approved senders:

1. Select an email message, as shown in Figure 9-19.

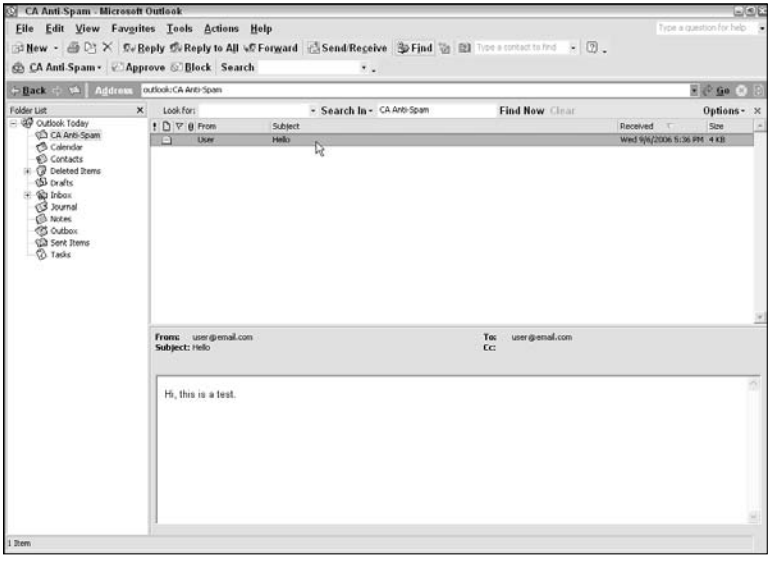

Figure 9-19: Selecting an email message

2. Click Approve on the CA Anti-Spam toolbar, as shown in Figure 9-20.

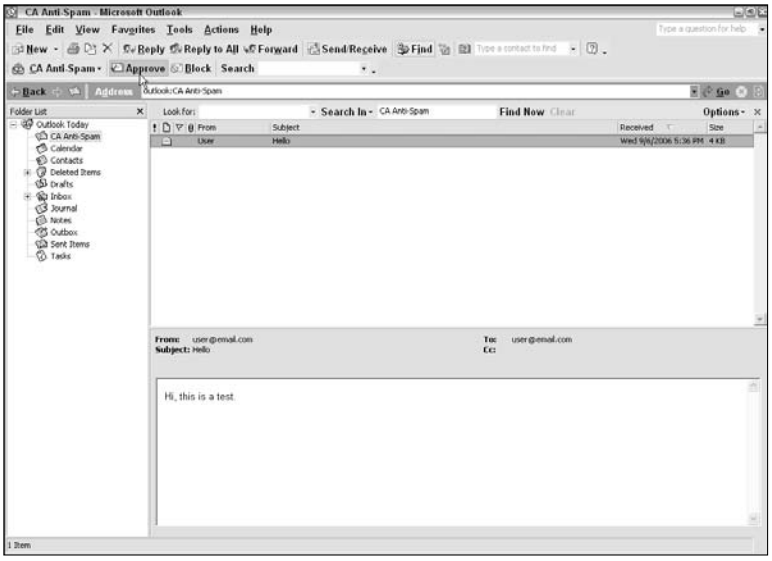

Figure 9-20: Approving an email message

The sender and all other recipients of the message are added to your Approved Senders list.

Block Messages and Senders

You can identify a currently open message as spam, move it to the CA Anti-Spam folder, and add the sender to your Blocked Senders list:

1. Select an email message, as shown in Figure 9-21.
2. Click Block on the CA Anti-Spam toolbar, as shown in Figure 9-22.

   The sender is added to the Blocked Senders list and the message is moved to your CA Anti-Spam quarantine folder and marked as read.

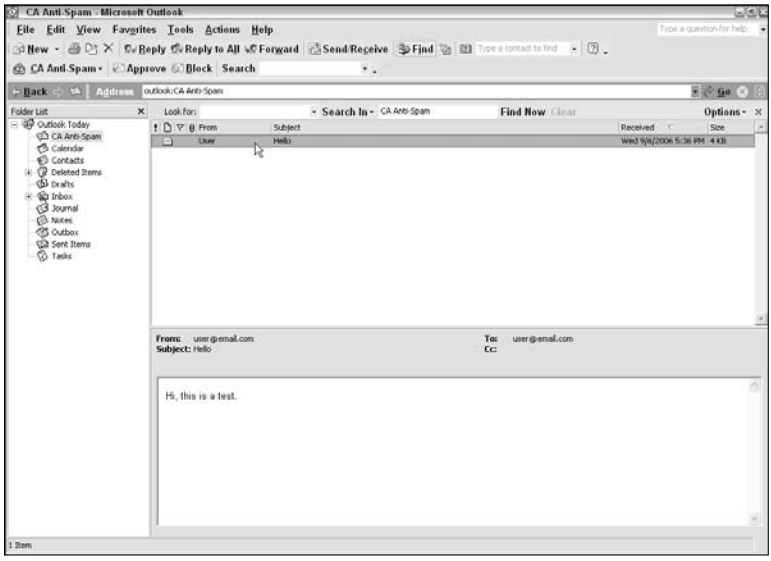

Figure 9-21: Selecting an email message

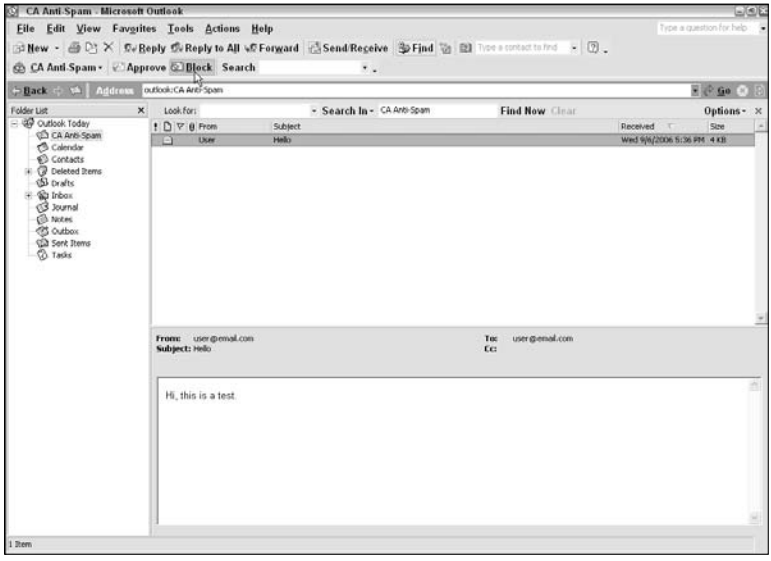

Figure 9-22: Blocking an email message

Search for Email Messages

When the Search feature is enabled, the Search field appears on the toolbar. Follow these steps to use this field to identify the criteria for your search:

1. In the Search field of the CA Anti-Spam toolbar, enter a keyword or keywords for your search, as shown in Figure 9-23.

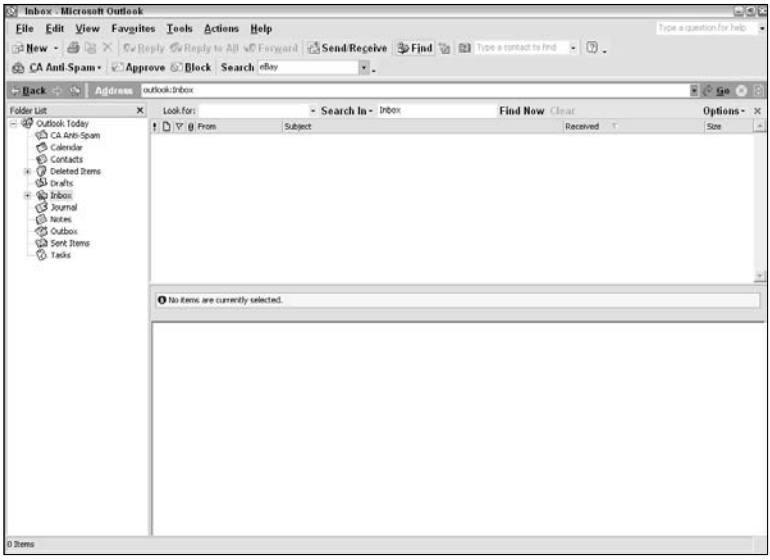

Figure 9-23: Entering search terms

You can click the down arrow to the right of the Search field to view and select keywords entered for previous searches.

Alternatively, you can click the word Search in the toolbar to open the Search window and enter your search criteria.

2. Click Search to begin searching.

CA Anti-Spam scans the items that match your search criteria to find the words or phrases you specified.

When the search is complete, the Search dialog appears, as shown in Figure 9-24, listing the results.

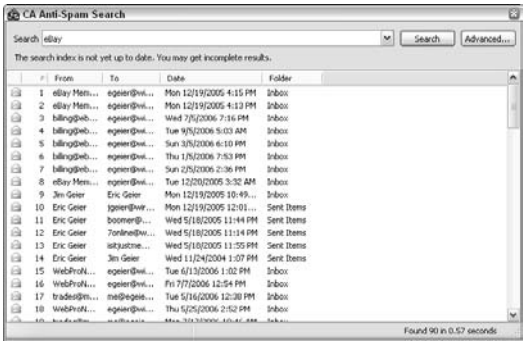

Figure 9-24: Search results example

The Search dialog displays a list of messages, contacts, tasks, notes, or appointments in which the keywords appear in the body or any of the attachments.

3. Scroll through the list to view the results.

   To view the contents of the items listed in the Search dialog, hover your mouse over the envelope icon on the left-hand side of the screen.

Approved Senders List

The Approved Senders list provides information about the listed senders, including the name and email address of the sender, the date the sender was added to the list, and the date of the last message from the sender.

The following sections cover tasks relating to the Approved Senders list.

View Approved Senders

You can monitor the Approved Senders list and ensure that it accurately reflects the senders approved to contact you through email:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-25.

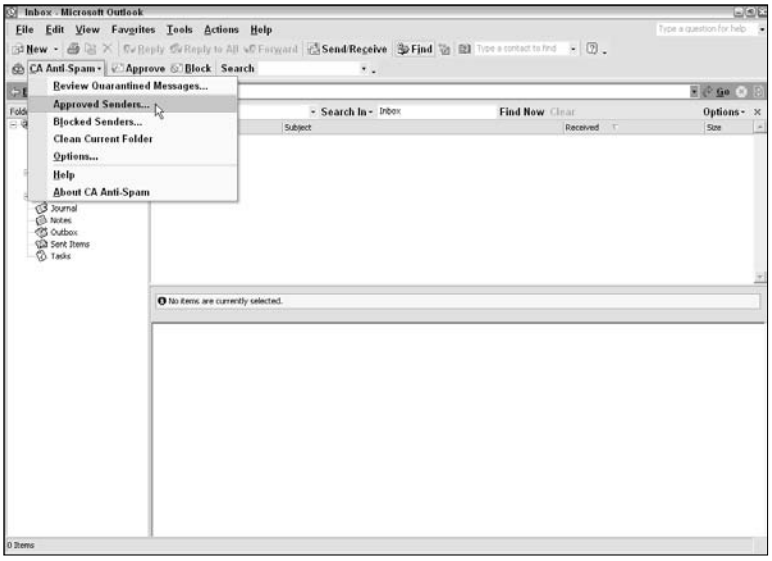

Figure 9-25: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Use the Find field on the Approved Senders screen to locate a specific sender or scroll down to review all of the senders in the list.

3. To review information about a particular sender, as shown in Figure 9-26, select a sender and click Properties or double-click on the sender.

Figure 9-26: Reviewing sender information example

4. Click Close to exit the Approved Senders screen.

Add Senders to Your Approved Senders List

You can use the Approved Senders screen to manually add to the list of senders who are approved to contact you. Follow these steps:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-27.

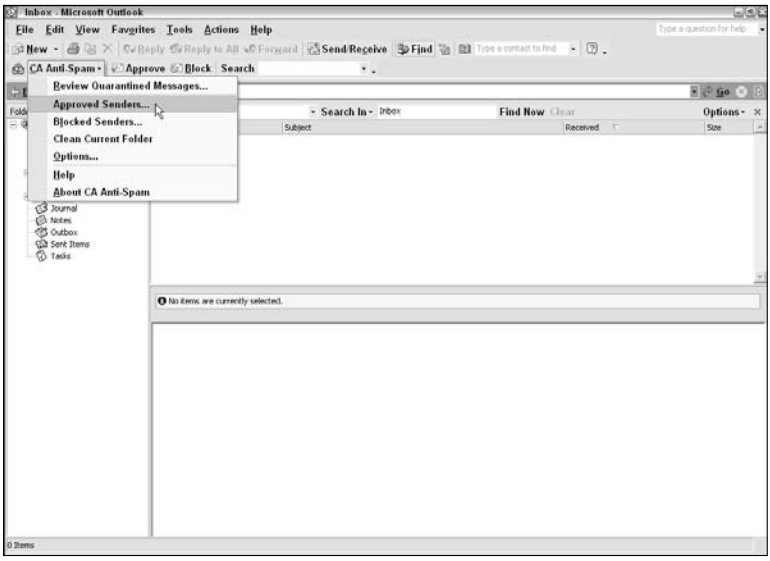

Figure 9-27: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Click New.

The New Address window appears.

3. Enter the name and email address of the sender in the appropriate fields, as shown in Figure 9-28.

Figure 9-28: Adding a sender

4. Specify options for this sender.

   You can specify that a valid digital signature or a matching name is required for messages from this address.

5. Click OK.

   The sender is added to the list of approved senders and all messages from this sender are automatically approved.

Add Domains to Your Approved Senders List

To ensure that multiple users from the same location (such as a specific company) can contact you through email, you can add the associated domain to your Approved Senders list:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-29.

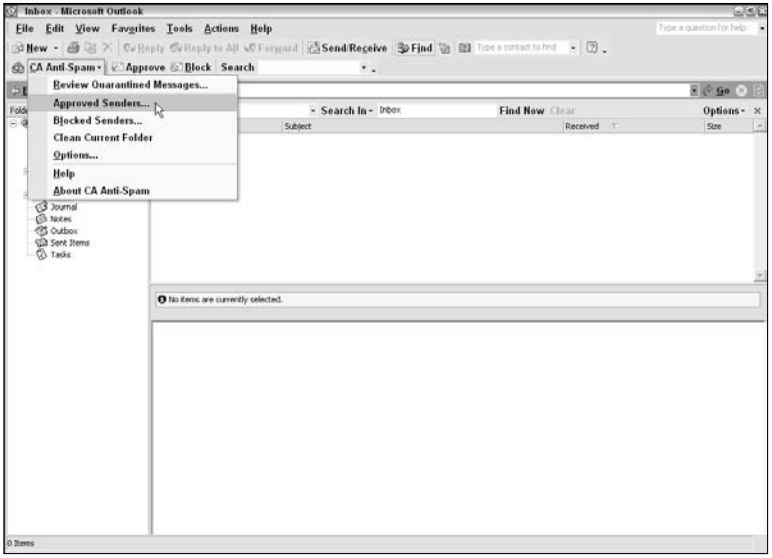

Figure 9-29: Accessing the Approved Senders screen

   The Approved Senders window appears.

2. Click New.

   The New Address window appears.

3. Enter the domain name in the Address field, as shown in Figure 9-30.

Figure 9-30: Adding a domain

4. Specify options for this domain.

   You can specify that a valid digital signature or a matching name is required for messages from this domain.

5. Click OK.

   The domain is added to the Approved Senders list and all messages from any address in the domain are automatically approved.

Delete Senders from Your Approved Senders List

You can delete entries from your Approved Senders list:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-31.

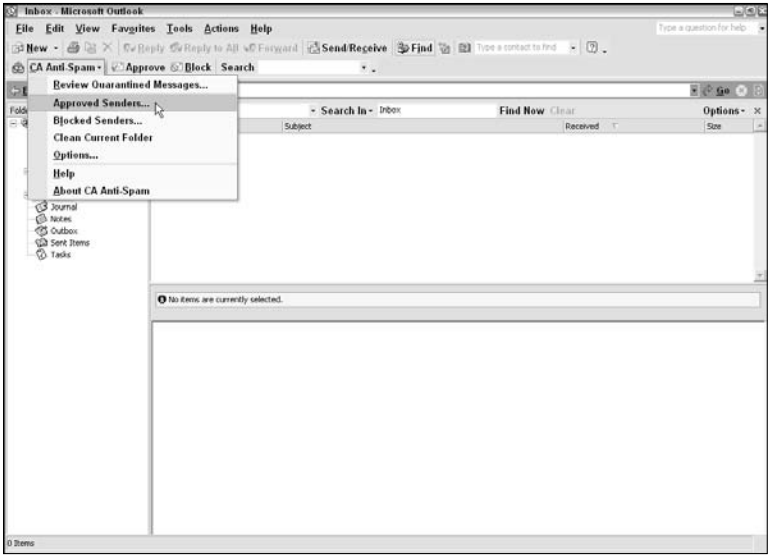

Figure 9-31: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Select the sender you want to delete from the list.
3. Click Delete (see Figure 9-32), and then click Yes to confirm the deletion.

Figure 9-32: Deleting a sender

The sender is removed from the list.

Note

When you delete senders from the Approved Senders list, the senders are not automatically added to the Blocked Senders list. To actively block a sender that you have removed from your Approved Senders list, you must manually add the sender to your Blocked Senders list.

Build Your Approved Senders List Automatically

You can use the Approved Senders screen to automatically build or add to your Approved Senders list from information in Microsoft Outlook or Microsoft Outlook Express folders.

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-33.

   The Approved Senders window appears.

2. Click Scan in the Tools section.

   The scan begins. CA Anti-Spam scans your saved mail, sent mail, and contacts. A progress bar tracks the progress of the scan.

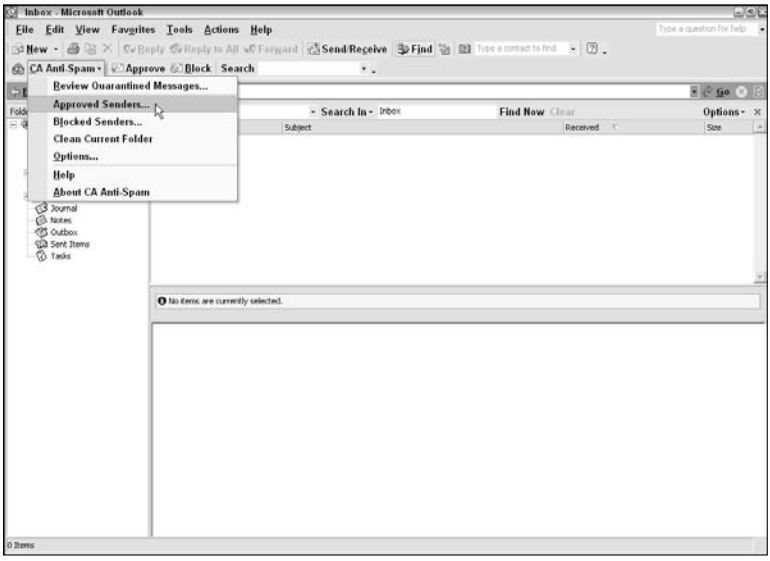

Figure 9-33: Accessing the Approved Senders screen

Note

Because CA Anti-Spam scans your email folders, make sure all spam is deleted and not present in your saved or sent mail folders.

When the scan finishes, CA Anti-Spam identifies the number of addresses added to your Approved Senders list.

3. Click OK to close the window.

Blocked Senders List

The Blocked Senders List lets you manage who can and cannot contact you through email. Messages from senders on the Blocked Senders list are automatically moved to the CA Anti-Spam folder and marked as read. These messages do not appear in the Quarantine list.

The following sections cover tasks relating to the Blocked Senders list.

View Blocked Senders

You can monitor the Blocked Senders list and ensure that the list accurately reflects the senders approved to contact you through email:

1. Select Blocked Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-34.

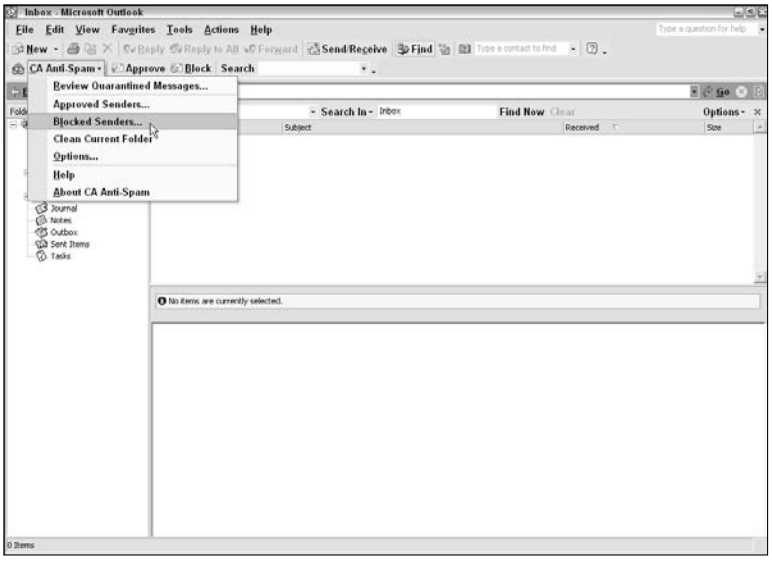

Figure 9-34: Accessing the Blocked Senders screen

The Blocked Senders window appears.

2. Use the Find field to locate a specific sender, or scroll down to review all of the senders in the list.

3. To review information about a particular sender, as shown in Figure 9-35, select a sender and click Properties or double-click on the sender.

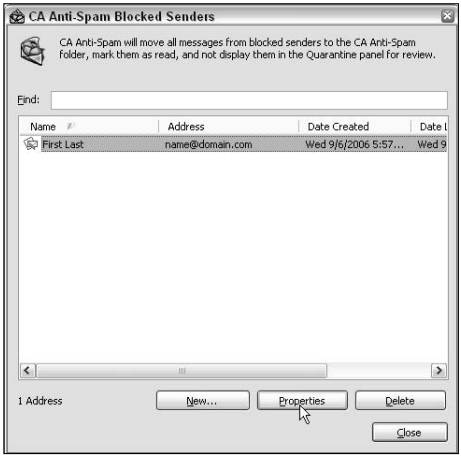

Figure 9-35: Reviewing sender information

4. Click Close to exit the Blocked Senders screen.

Add Senders to Your Blocked Senders List

You can use the Blocked Senders screen to add to the list of blocked senders:

1. Select Blocked Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-36.

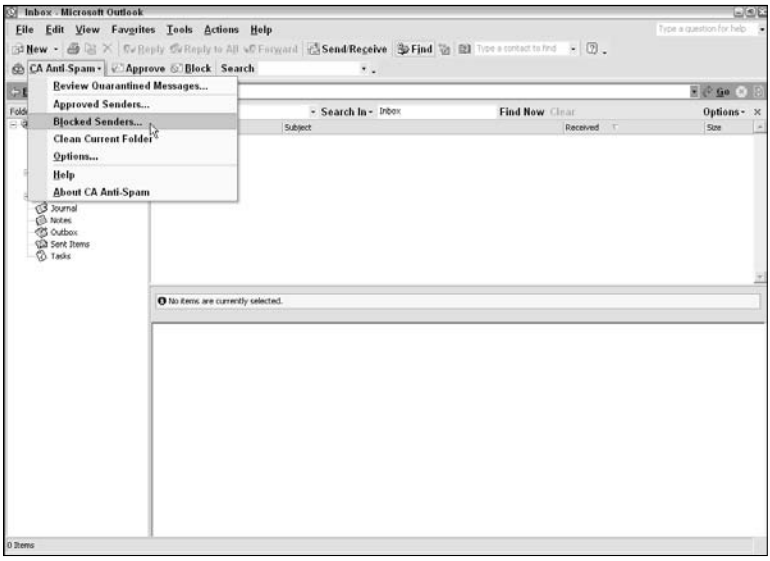

Figure 9-36: Accessing the Blocked Senders screen

The Blocked Senders window appears.

2. Click New.

The New Address window appears.

3. Enter the name and email address of the sender you want to block, as shown in Figure 9-37.

Figure 9-37: Adding a sender

4. Click OK.

The sender is added to the list of blocked senders and all messages from this sender are automatically marked as read and placed in the CA Anti-Spam folder.

Add Domains to Your Blocked Senders List

To block mail from an entire domain, you can add the associated domain to your Blocked Senders list:

1. Select Blocked Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-38.

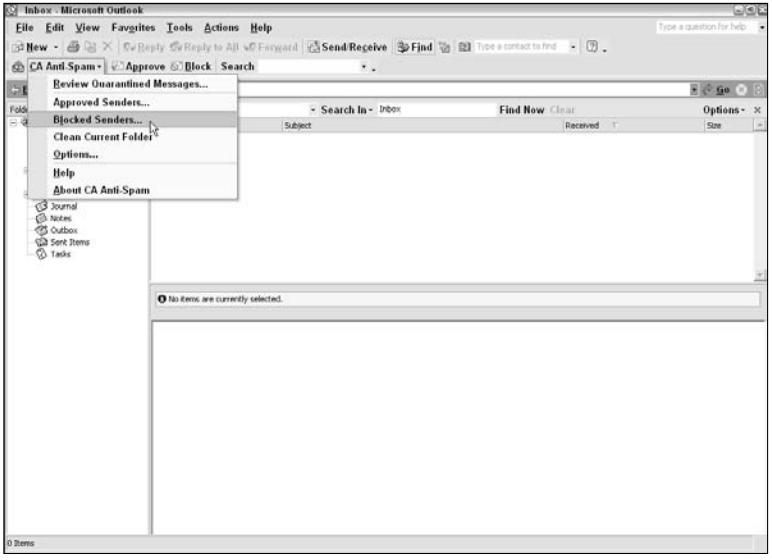

Figure 9-38: Accessing the Blocked Senders screen

The Blocked Senders window appears.

2. Click New.

The New Address window appears.

3. Enter the domain name you want to block email from, as shown in Figure 9-39.

Figure 9-39: Adding a domain

4. Click OK.

   The domain is added to the Blocked Senders list and all messages from the domain are automatically marked as read and placed in the CA Anti-Spam folder, unless a specific email address is already added to the Approved Senders list. An approved sender will overwrite a blocked domain.

Delete Senders from Your Blocked Senders List

You can delete entries from your Blocked Senders list:

1. Select Blocked Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-40.

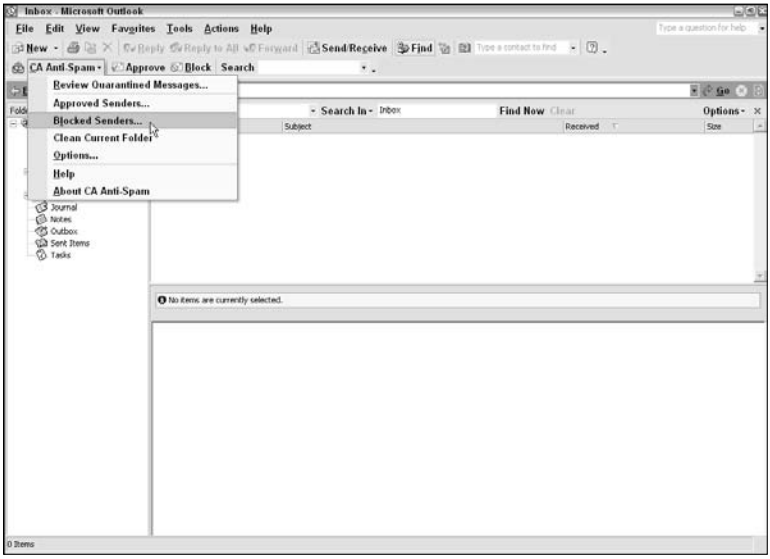

Figure 9-40: Accessing the Blocked Senders screen

   The Blocked Senders window appears.

2. Select the sender you want to delete from the list.
3. Click Delete (see Figure 9-41), and then click Yes to confirm the deletion.

   The sender is removed from the list.

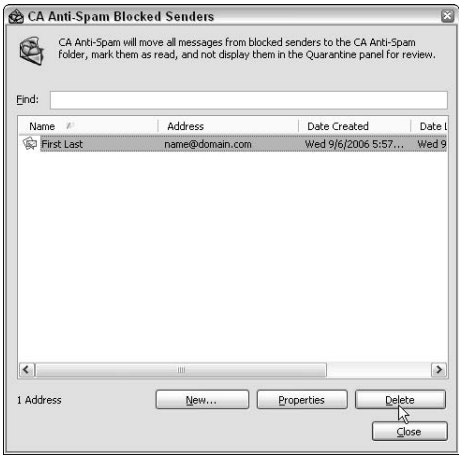

Figure 9-41: Deleting a sender

Advanced Tasks

This section provides step-by-step instructions for CA Anti-Spam tasks that are less commonly performed.

Setting Options

1. Select Options from the CA Anti-Spam toolbar menu list, as shown in Figure 9-42.

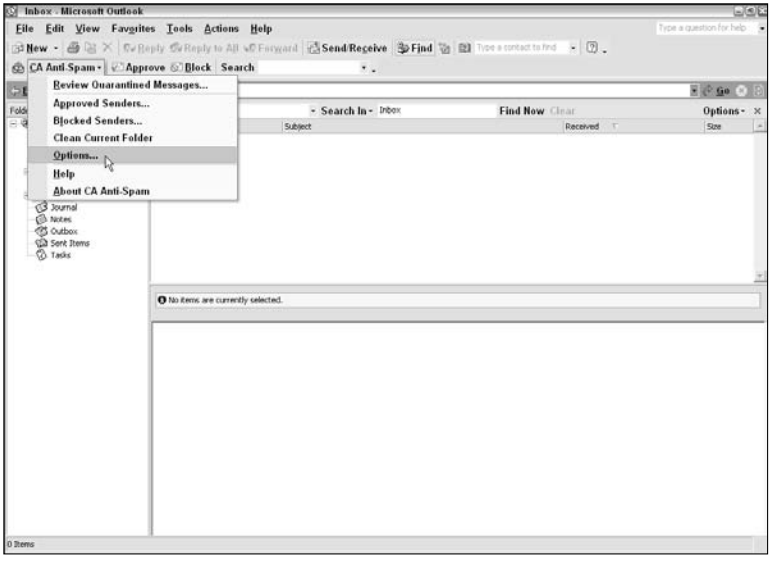

Figure 9-42: Accessing the Options screen

The CA Options window appears.

2. Click through the Options tabs and make any desired changes.
3. When you're all done, click OK to exit the Options screen.

Export Approved Senders Lists

You can export your Approved Senders list as an XML file. This is a good way to back up your list in case your computer crashes and you lose your CA Anti-Spam settings, or to share your approved senders with another computer.

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-43.

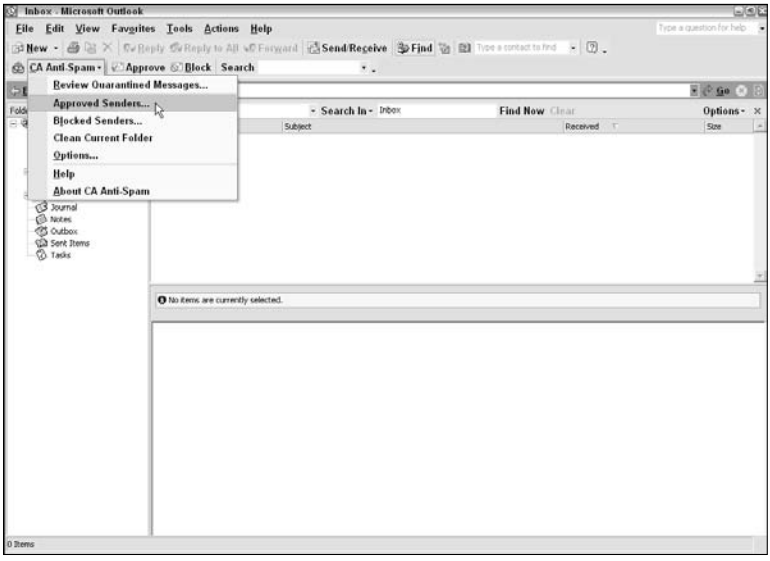

Figure 9-43: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Click the Export button, as shown in Figure 9-44.

The Save As dialog appears.

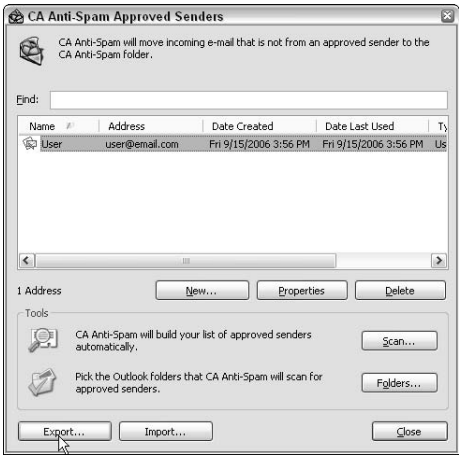

Figure 9-44: Exporting Approved Senders lists

3. In the Save As dialog box, enter the name of the Approved Senders list and click OK.

   CA Anti-Spam saves the list to the specified folder as an XML file.

4. Click Close to exit the Approved Senders screen.

Import Approved Senders Lists

You can import Approved Senders lists from the XML files you've created using the CA Anti-Spam import feature:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-45.

   The Approved Senders window appears.

2. Click the Import button on the Approved Senders screen.

   The Open dialog appears, as Figure 9-46 shows.

3. Select the list you want to import and click Open.

   CA Anti-Spam imports the list into your Approved Senders list. When the import process is complete, you are prompted with the number of addresses added to your Approved Senders list.

4. Click OK and then click Close to exit the Approved Senders screen.

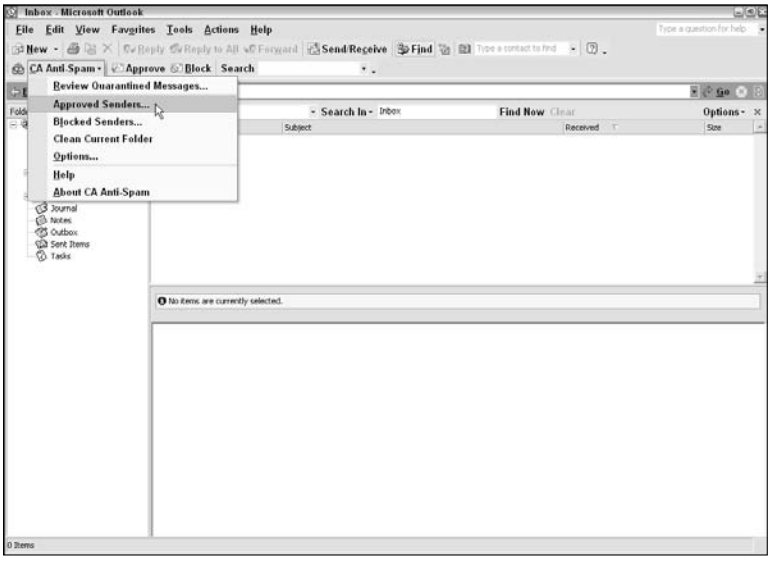

Figure 9-45: Accessing the Approved Senders screen

Figure 9-46: Importing Approved Senders lists

Require Valid Digital Signatures

You can set an extra layer of security for your email by specifying that a valid digital signature is required for messages from a specific sender or domain:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-47.

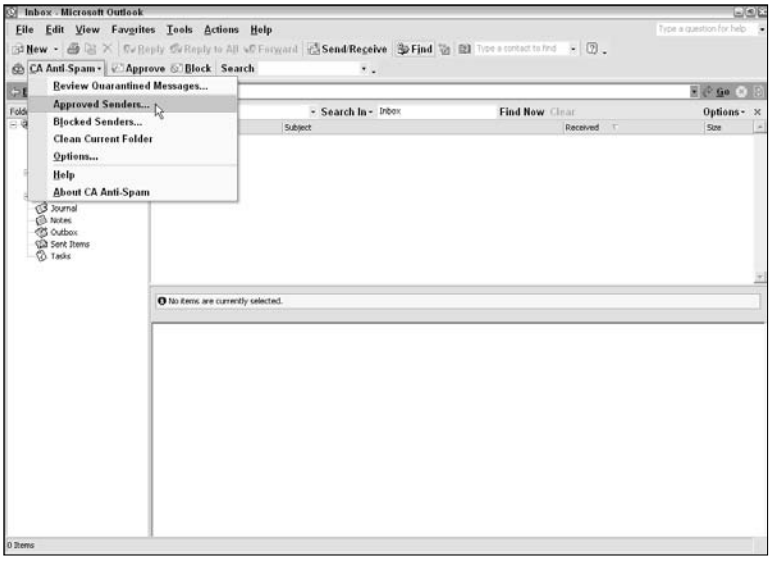

Figure 9-47: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Select a specific sender or domain from the Approved Senders list, and then click Properties.

   The Properties dialog appears.

3. Check the option to require a valid digital signature for messages from this address, as shown in Figure 9-48.

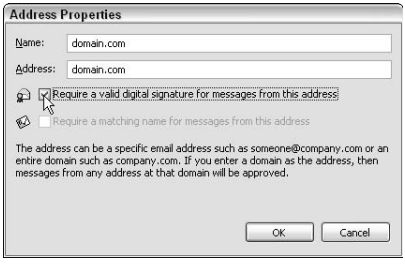

Figure 9-48: Requiring valid digital signatures

4. Click OK.

Require Matching Names from Senders

You can set yet another layer of security for your email by specifying that a matching name is required for messages from a specific sender or domain:

1. Select Approved Senders from the CA Anti-Spam toolbar menu list, as shown in Figure 9-49.

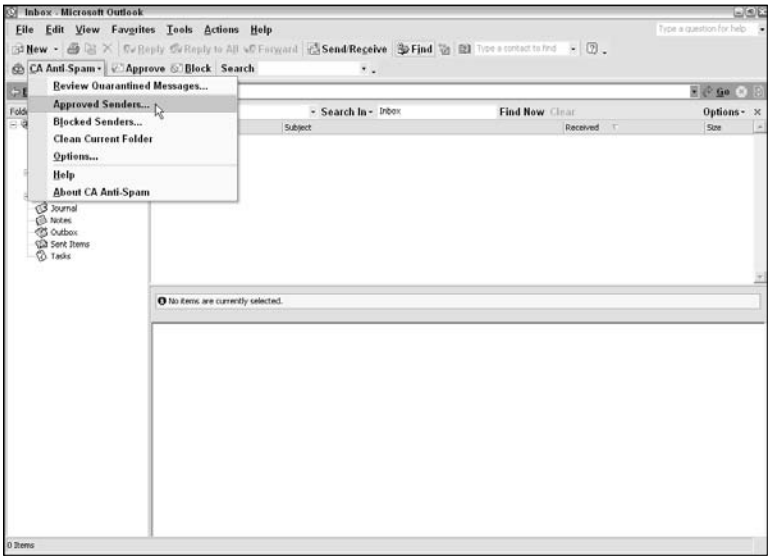

Figure 9-49: Accessing the Approved Senders screen

The Approved Senders window appears.

2. Select a specific sender or domain from the Approved Senders list, and then click Properties.

The Properties dialog appears.

3. Check the option to require a matching name for messages from this address, as shown in Figure 9-50.

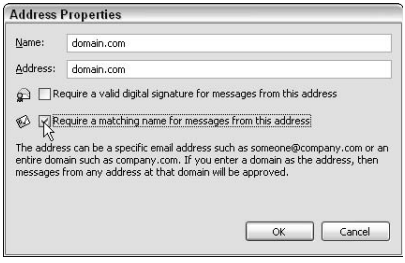

Figure 9-50: Requiring matching names from senders

4. Click OK.

10

BLOCKING OFFENSIVE WEBSITES

Included with CA Internet Security Suite is Blue Coat K9 Web Protection, which protects your family from web content that may be inappropriate for your younger PC users.

This chapter is organized into these main sections:

- **Web Content Filtering Methods**

  This section introduces the filtering methods used in Blue Coat K9 Web Protection.

- **Blue Coat K9 Web Protection Introduction**

  This section takes you through all the administration screens of Blue Coat K9 Web Protection and tells you where each option is located and what it does.

- **Tasks**

  This section provides step-by-step instructions for Blue Coat K9 Web Protection tasks.

Web Content Filtering Methods

Blue Coat K9 Web Protection software goes through a process (shown in Figure 10-1) every time someone tries to visit a website that ensures that only websites (or categories of websites) that have been approved by the administrator are shown to the users. Those that aren't approved won't be displayed and the user is redirected to an alert page, shown in Figure 10-2.

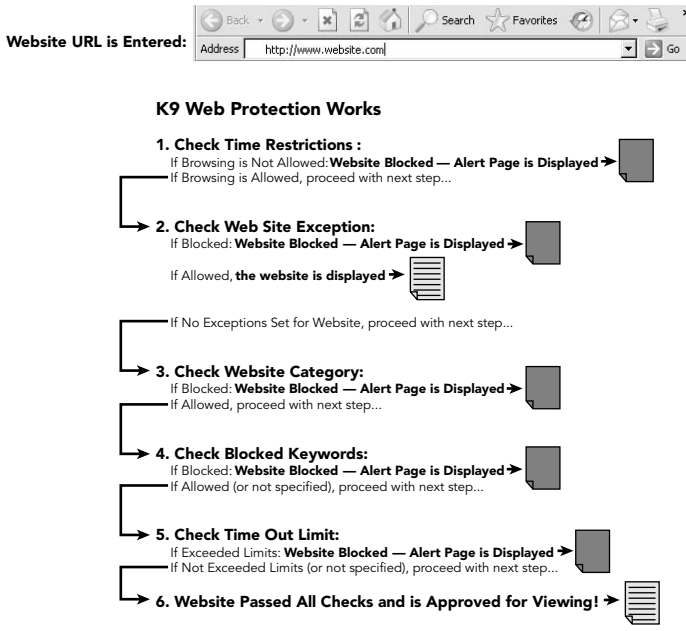

Figure 10-1: Example of the Blue Coat K9 Web Protection filtering process

Figure 10-2: Example of a blocked page alert

Blue Coat K9 Web Protection Introduction

As soon as you install Blue Coat K9 Web Protection and reboot your computer, it's actively working. To customize the filtering settings and to perform any other tasks relating to the software, you can access the Blue Coat K9 Web Protection Administration tool, shown in Figure 10-3. This tool has two main sections: View Internet Activity and Setup.

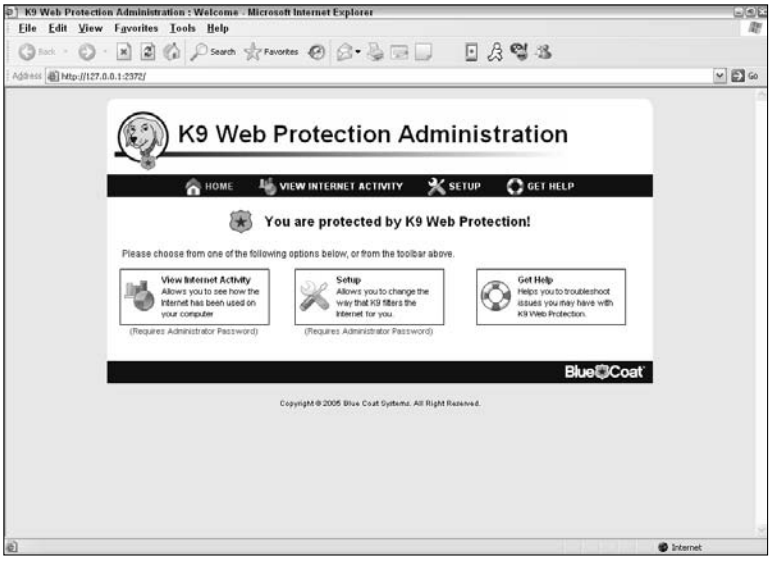

Figure 10-3: Blue Coat K9 Web Protection Administration tool

The following sections discuss the main pages and screens of the Blue Coat K9 Web Protection Administration tool.

Open Blue Coat K9 Web Protection Administration

There are a few ways to open Blue Coat K9 Web Protection Administration:

- **Start Menu**

  Browse to the following path on your Start menu:

  Programs (or All Programs) ➔ Blue Coat K9 Web Protection

  Then click on Blue Coat K9 Web Protection Admin, as shown in Figure 10-4.

- **Desktop Icon**

  If you chose to create a desktop icon for Blue Coat K9 Web Protection Administration during installation, then you can simply double-click on that icon, as shown in Figure 10-5.

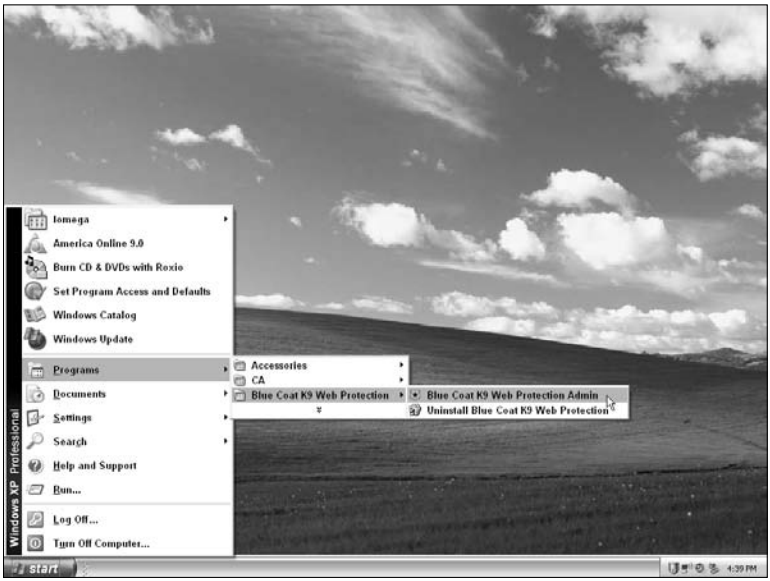

Figure 10-4: Opening Blue Coat K9 Web Protection Administration from the Start menu

Figure 10-5: Opening Blue Coat K9 Web Protection Administration with the desktop icon

- **Quick Launch**

  If you chose to install an icon on the quick launch bar for Blue Coat K9 Web Protection Administration during installation, then you can simply click on that icon, as shown in Figure 10-6.

Figure 10-6: Opening Blue Coat K9 Web Protection Administration with the Quick Launch icon

Administrator Login

After opening Blue Coat K9 Web Protection Administration, you'll see a page like the one shown in Figure 10-7.

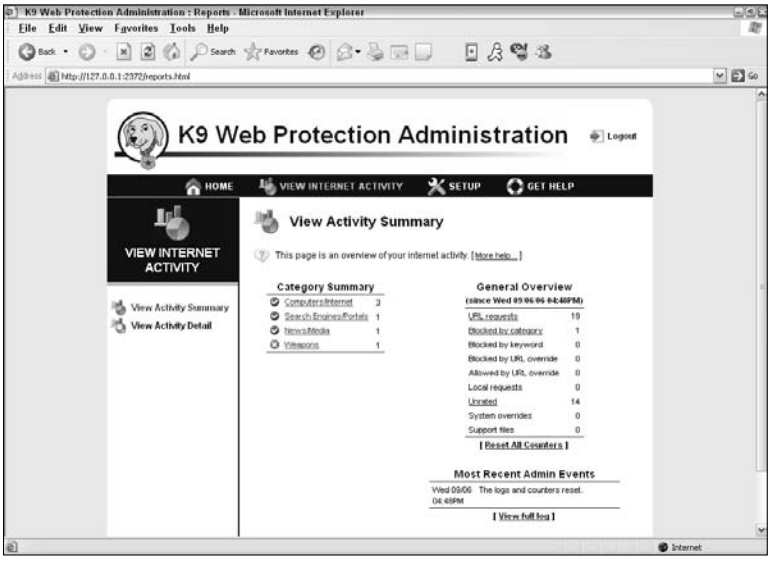

Figure 10-7: Blue Coat K9 Web Protection Administration

You can access the View Internet Activity and Setup sections with the administrator password you selected during the installation process.

View Internet Activity

After opening Blue Coat K9 Web Protection Administration, you can access the View Internet Activity section from the main page, as shown in Figure 10-8.

Figure 10-8: View Internet Activity section

After logging into the View Internet Activity section, you can access its pages from the menu on the left side of the main page. The following sections discuss each of the pages in this section.

Note

The administrator login times-out after 5 minutes of nonactivity to ensure that, should the administrator fail to log out, other users cannot change filtering or administrative settings.

View Activity Summary

This page contains the following items:

- **Category Summary**

  Lists all categories relevant to the active Blue Coat K9 Web Protection filtering policy. Categories shown in green are allowed. Categories listed in red are blocked by the active filtering policy. Categories in orange have changed status during the reporting period.

  The Category Summary also provides access to statistics about recent Internet activity by category.

You can click on a category for a detailed view of website requests in that category. For example, to view a list of which sites within the Weapons category that someone attempted to access, click on the link for Weapons. A detailed report similar to the Figure 10-9 shows will appear.

Figure 10-9: Viewing a detailed report about a specific category

- **General Overview**

  Displays a general breakdown of recent Internet activity, including the number of web pages visited, requests allowed, and requests blocked.

  You can click on any statistic for a detailed view, as Figure 10-10 shows.

Figure 10-10: Viewing detailed information about general Internet activity

- **Most Recent Admin Events**

  Shows recent changes to the web filtering policy (such as overrides, keyword blocking additions, and login failures) and other administrative changes made using the administrator password.

Note

The statistics tracked in this window begin upon installation of the software and continue to increment indefinitely. If you would like to purge the log and restart the statistics, you can click the Reset All Counters button at the bottom of the General Overview table.

View Activity Detail

This page displays a detailed view of all Internet activity, including all websites visited and blocked since the last log purge, the category ratings of these sites (if rated), and the actual URL of the sites visited. Figure 10-11 shows an example of an activity detail page.

Figure 10-11: Viewing activity details

Setup

After opening the administration tool, you can access the Setup section of Blue Coat K9 Web Protection Administration from the main page, as shown in Figure 10-12.

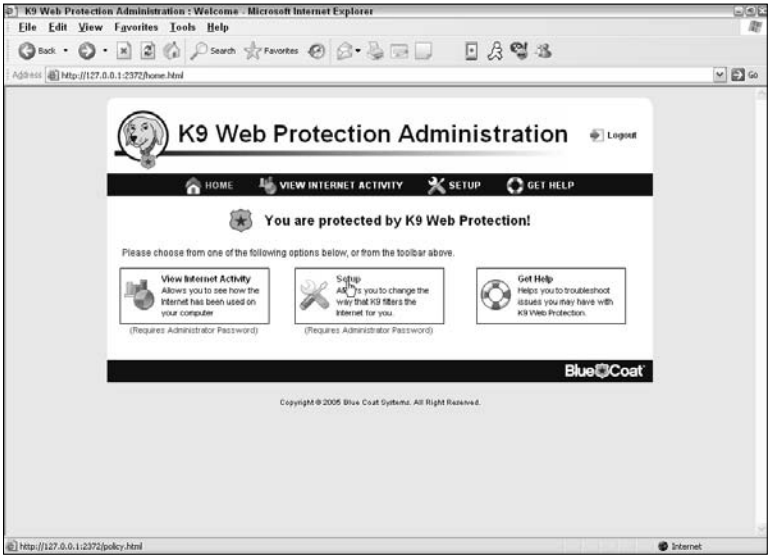

Figure 10-12: Blue Coat K9 Web Protection Administration

After logging into the Setup section, you can access its pages from the menu on the left side of the main page. The following sections discuss each of the pages in the Setup section.

Note

The administrator login times-out after 5 minutes of nonactivity to ensure that, should the administrator fail to log out, other users cannot change filtering or administrative settings.

Web Categories to Block Page

This page, as shown in Figure 10-13, allows you to set your desired Protection Level from the following choices:

Figure 10-13: Blue Coat K9 Web Protection Setup — Web Categories to Block page

- **High**

  Blocks the most commonly blocked categories, as well as Abortion, Gay/Lesbian, and Unrated sites.

- **Default**

  Blocks the most commonly blocked categories, but allows Unrated sites.

- **Moderate**

  Blocks the Adult/Mature Content, Pornography, Nudity, and Spyware categories.

- **Minimal**

  Blocks the Pornography and Spyware categories.

- **Monitor**

  Allows all categories — it only logs traffic.

- **Custom**

  You can select your own set of categories to block. Figure 10-14 shows an example of the customization screen and the available categories.

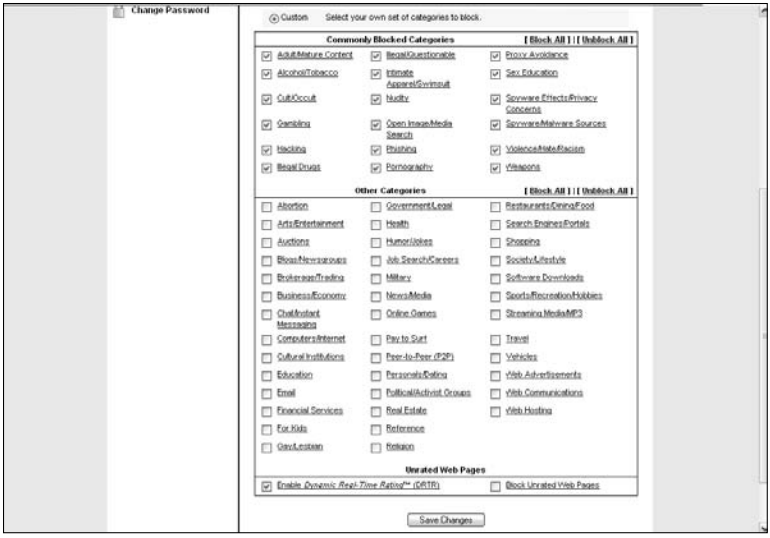

Figure 10-14: Customization screen

Web Site Exceptions Page

From the Web Site Exceptions page (shown in Figure 10-15), you can explicitly block or allow access to specific websites.

Figure 10-15: Blue Coat K9 Web Protection Setup — Web Site Exceptions page

Web Search Options Page

The Web Search Options page (shown in Figure 10-16) lets you specify whether Google SafeSearch is used. Google SafeSearch diminishes the amount of adult material that might be returned as a result of an Internet search when using the Google search engine at `www.google.com`.

Time Restrictions Page

Blue Coat K9 Web Protection offers the ability to impose time restrictions on Internet usage, such as blocking all website access after 10 P.M. to ensure that your children won't be doing any late-night web browsing. This feature can be set up on the Time Restrictions page and is shown in Figure 10-17.

Figure 10-16: Blue Coat K9 Web Protection Setup — Web Search Options page

Figure 10-17: Blue Coat K9 Web Protection Setup — Time Restrictions page

Blocking Effects Page

From the Blocking Effects page (shown in Figure 10-18), you can specify what happens when a page is blocked by Blue Coat K9 Web Protection, such as playing an audible alert.

Figure 10-18: Blue Coat K9 Web Protection Setup — Blocking Effects page

URL Keywords Page

The URL Keywords page (shown in Figure 10-19) allows you to block access to web pages based on keywords in the web page URL. You can, for example, block any web page that has the word "sex" in the URL.

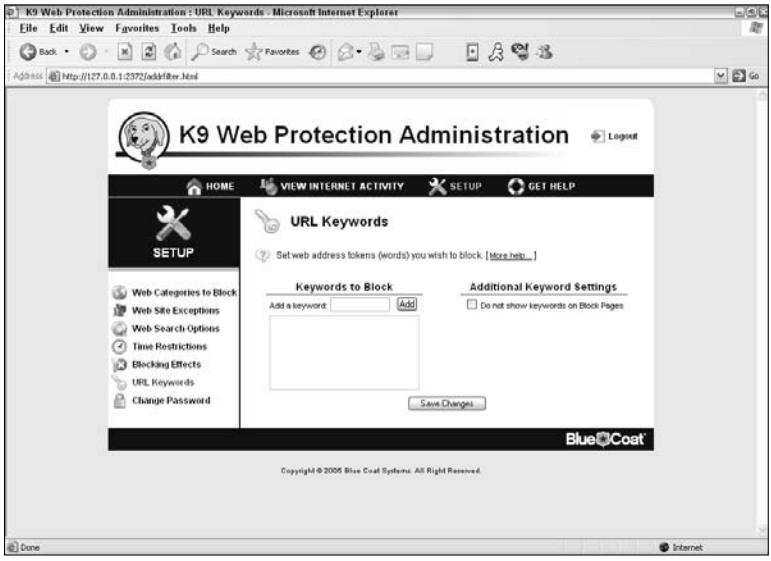

Figure 10-19: Blue Coat K9 Web Protection Setup — URL Keywords page

Change Password Page

This page (shown in Figure 10-20) allows you to change your administration password.

Figure 10-20: Blue Coat K9 Web Protection Setup — Change Password page

Tasks

This section provides step-by-step instructions for Blue Coat K9 Web Protection tasks.

Unblock or Block Websites

You can unblock or block specific websites on the Web Site Exceptions page:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Web Site Exceptions, as shown in Figure 10-21.

Figure 10-21: Accessing the Web Site Exceptions page

3. Enter the URL of the website in either the Sites To Always Block or the Sites To Always Allow field.
4. Click Add.
5. Click Save Changes.

Note

You can also unblock currently blocked websites on the Blocked Page Alert page in the Administrator Override Options section, as shown in Figure 10-22, after visiting a blocked page.

From there you can also allow browsing on that particular website for 15 minutes or permanently.

Figure 10-22: Administrator Override Options section on a Blocked Alert page

Enable or Disable Google SafeSearch

You can enable or disable Google SafeSearch:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Web Search Options, as shown in Figure 10-23.

Figure 10-23: Accessing the Web Search Options page

3. Check or uncheck the Use Google SafeSearch option (shown in Figure 10-24).

Figure 10-24: Use Google SafeSearch option

Configure Time Restrictions

You can specify when and when not to allow web browsing:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Time Restrictions, as shown in Figure 10-25.

Figure 10-25: Accessing the Time Restrictions page

3. Hover over the time diagram, select a region of time with the target cursor, and then click Allow or Deny. See Figure 10-26 for an example.

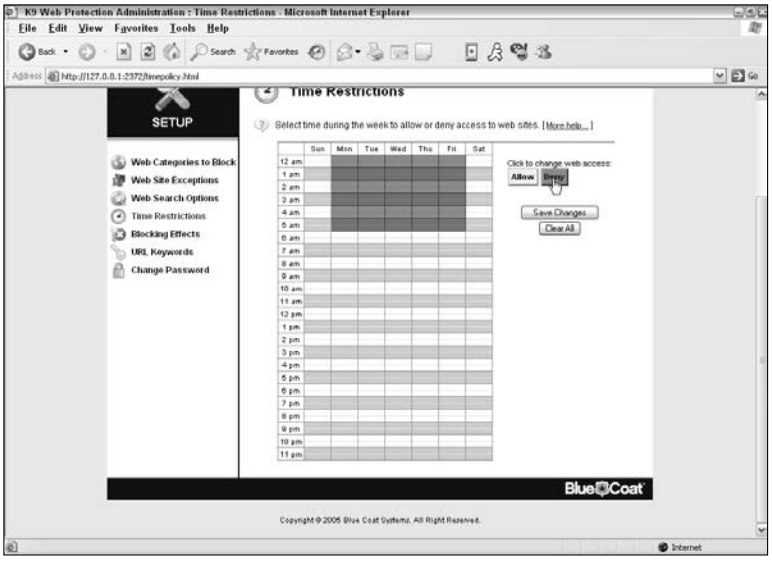

Figure 10-26: Configuring time restrictions

You can repeat this process until you've set your desired time restrictions.

4. When you're done, click Save Changes.

Hide or Show Admin Options on Block Page Alerts

You can remove or add the Administrator Override Options section on the Block pages:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Blocking Effects, as shown in Figure 10-27.

Figure 10-27: Accessing the Blocking Effects page

3. Check or uncheck the Show Admin Options On Block Pages option, as pointed out in Figure 10-28.

Figure 10-28: Show Admin Options On Block Pages option

Hide or Show Blocked URL Keywords on Block Page Alerts

You can remove or add the list of URL keywords you've specified to block:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click URL Keywords, as shown in Figure 10-29.

Figure 10-29: Accessing the URL Keywords page

3. Check or uncheck the Do Not Show Keywords On Block Pages option, as pointed out in Figure 10-30.

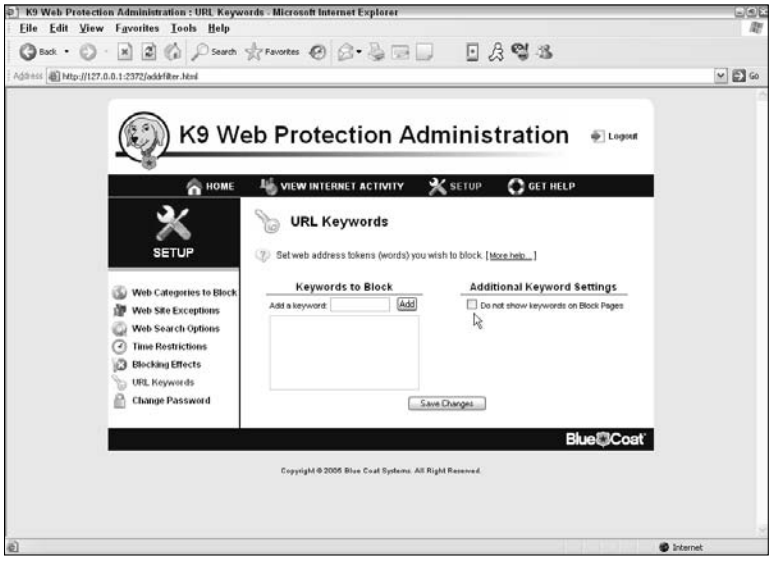

Figure 10-30: Do Not Show Keywords On Block Pages option

Change the Administration Password

You can change the administration password if necessary:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Change Password, as shown in Figure 10-31.

Figure 10-31: Accessing the Change Password page

3. Enter your current password and enter the new password twice in the corresponding fields.
4. Click Change Password to save changes.

Configure Audible Bark on Blocked Alert

You can enable or disable the "barking dog" sound that is activated when someone visits a blocked website:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Blocking Effects, as shown in Figure 10-32.

Figure 10-32: Accessing the Blocking Effects page

3. Check or uncheck the Bark When Blocked option, as pointed out in Figure 10-33.

Figure 10-33: Bark When blocked option

Configure Time Out Settings

You can configure what happens when someone tries to repeatedly visit blocked websites:

1. Open Blue Coat K9 Web Protection Administration and log into Setup.
2. Click Blocking Effects, as shown in Figure 10-34.

Figure 10-34: Accessing the Blocking Effects page

3. Continue with one of the following:

To enable/change the Time Out feature:

a. Check the Enable Time Out Settings option, as pointed out in Figure 10-35.

Figure 10-35: Enable Time Out Settings option

b. Specify your desired time out settings.

c. Click Save Changes.

To disable the Time Out feature:

a. Uncheck the Enable Time Out Settings option, shown in Figure 10-35.

b. Click Save Changes.

11

ENSURING UP-TO-DATE PROTECTION

Don't compromise your PC — make sure you keep CA Internet Security Suite up to date with product updates. This will help to ensure that you're properly protected from the latest Internet threats, as new viruses, spyware, and security holes that are found every day.

Update CA Internet Security Suite

You can quickly update all of the installed components of CA Internet Security Suite manually by following these steps:

Note

By default, CA Internet Security Suite is set to automatically update upon reboot and every 8 hours thereafter.

1. Open the Update Product window using one of the following methods:
    a. On the CA Security Center screen, click the Update button, as shown in Figure 11-1.
    b. On any component screen, click the Update button, as shown in Figure 11-2.

Figure 11-1: Opening the Update Product window in CA Security Center

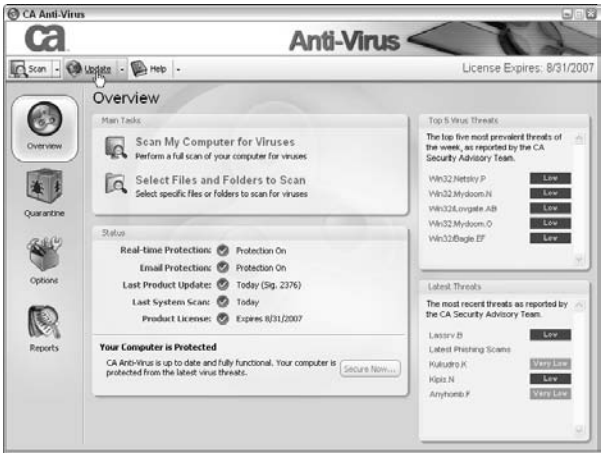

Figure 11-2: Opening the Update Product window in a component screen

c. Right-click the CA Security Center system tray icon and click Update Product, as shown in Figure 11-3.

The Product Update window appears and should begin downloading and installing any available updates. If it does not, click the Update button to begin the process.

The Product Update window provides information about the current versions installed for each listed component. In addition, it displays a status bar and progress bar to provide information about the update process as the downloading and installation takes place.

Figure 11-3: Opening the Update Product window from the System Tray icon

After the updates are downloaded and installed, you are prompted that the update has finished successfully or prompted to restart your computer to complete the update process.

2. Click Close.

   The Product Update window closes. Restart your computer if necessary.

Configure Proxy Settings

If you are using a proxy server, you can configure CA Internet Security Suite with the proxy information so it can properly connect to the Internet. If you aren't using a proxy, don't worry about this section.

1. Click the arrow next to the Update button in the upper left of the CA Security Center or any other component screen and select Configure Proxy Settings, as shown in Figure 11-4.

Figure 11-4: Accessing the Proxy Settings

The Configure Proxy Settings window appears.

2. Use one of the following two methods to configure the proxy settings:

Note

The automatic method should work if you've set up the proxy information within the Internet Explorer Internet Options. Otherwise, you'll need to manually specify the proxy settings in the CA software.

- **Automatic detection:** Select the Automatically Detect Proxy Server Settings option in the Configure Proxy Settings window, as shown in Figure 11-5.

Figure 11-5: Enabling automatic detection of proxy settings

- **Manual setup:** Enter your proxy server name and port number into the Proxy Server and Port fields, as shown in Figure 11-6.

Figure 11-6: Manually specifying proxy settings

3. If your proxy server requires authentication, check the My Proxy Server Requires Authentication option and specify the username and password, as shown in Figure 11-7; otherwise you can ignore this step.

Figure 11-7: Specifying proxy server authentication information

4. Click OK to save changes.

Note

For further help determining your proxy server details, contact your Internet service provider or network administrator.

Configure Automatic Update Options

You can set the following options for how you receive product updates:

- **Update automatically**

  You can configure CA Internet Security Suite to download and install product updates automatically and notify you when the installation is complete.

- **Do not update automatically**

  You can configure CA Internet Security Suite to notify you before downloading any product updates. This option lets you decide whether to download and install updates as necessary.

- **Update according to a schedule**

  You can set a scheduled time to download and install updates automatically.

Note

By default, CA Internet Security Suite is set to automatically update after initial reboot and every 8 hours thereafter.

Follow these steps to change your automatic update options:

1. Click the arrow next to the Update button in the upper left of the CA Security Center or any other component screen and select Schedule Updates, as shown in Figure 11-8.

Figure 11-8: Accessing the Schedule Updates window

The Schedule Updates window appears.

2. Select one of the following options, based on the previous descriptions:

Update automatically:

a. Check this option as shown in Figure 11-9.

b. Click OK.

Updates will now be downloaded and installed automatically and you are notified when they are complete.

Figure 11-9: Setting automatic updates

Do not update automatically:

a. Check the Do not update automatically option as shown in Figure 11-10.

b. Click OK.

Now you will not be notified of updates, and you will have to update by clicking the Update button yourself.

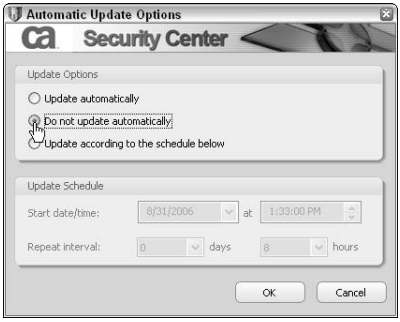

Figure 11-10: Specifying not to update automatically

Update according to a schedule:

a. Check the Update according to the schedule below option as shown in Figure 11-11.

The fields in the Update Schedule area are enabled.

b. Specify a date and time to start downloading updates and the number of days and hours between scheduled updates in the appropriate fields (see Figure 11-12 for an example).

c. Click OK.

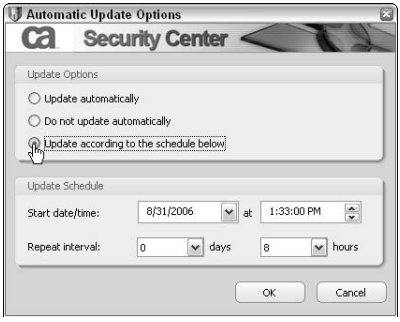

Figure 11-11: Specifying to update according to a defined schedule

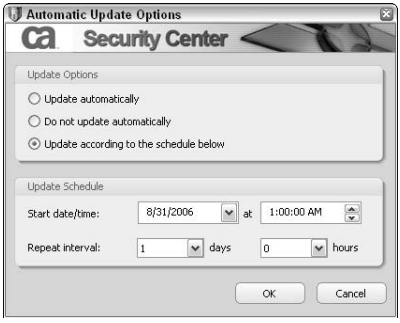

Figure 11-12: Specifying the update schedule

View the Update Log

You can view information about past product updates (to ensure updates are actually taking place, for example) by viewing the Product Update Log (shown in Figure 11-13).

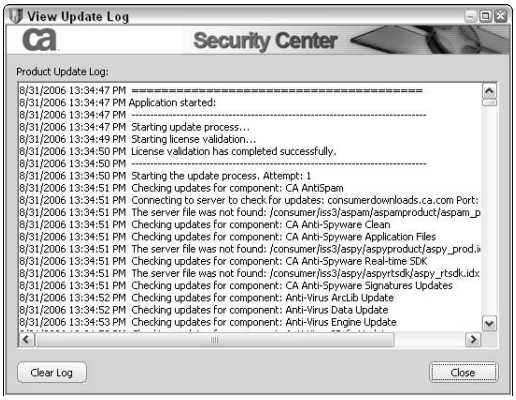

Figure 11-13: Product Update Log

To view the Product Update Log, click the arrow next to the Update button in the upper left of the CA Security Center or any other component screen, and then select View Update Log (see Figure 11-14).

Figure 11-14: Accessing the Update Log

INDEX

A

B

C

D

Continued

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

Continued

U

V

W

Z