



Intego VirusBarrier X5

User's Manual



Intego VirusBarrier X5 for Macintosh

© 2009 Intego. All Rights Reserved

Intego

www.intego.com

This manual was written for use with Intego VirusBarrier X5 software for Macintosh. This manual and the Intego VirusBarrier X5 software described in it are copyrighted, with all rights reserved. This manual and the Intego VirusBarrier X5 software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by Intego, Inc.

The Software is owned by Intego, and its structure, organization and code are the valuable trade secrets of Intego. The Software is protected by United States Copyright Law and International Treaty provisions.



Contents

1- About Intego VirusBarrier X5	5
What is Intego VirusBarrier X5?	6
VirusBarrier X5's Features.....	8
Using this User's Manual.....	10
2 - Introduction to Computer Viruses	11
Why You Need to be Protected	12
What is a Computer Virus?	12
How Computer Viruses Work	13
Different Types of Viruses	15
How do Viruses Spread?	17
How Can You Protect Yourself from Viruses?	18
If You Think You Have a Virus	20
Basic precautions	22
System Requirements.....	23
Installing VirusBarrier X5	23
3 - Quick Start.....	24
Intego VirusBarrier X5's Interface	25
First Things First: Scan Your Entire Hard Drive for Viruses.....	30
4 – Scanning Your Mac with VirusBarrier X5	32
Virus Scanning.....	33
Selecting Files and Running a Manual Scan.....	33
Drag and Drop Scanning	40
Scheduled Scanning.....	41
E-mail Analysis	43
Alerts	44
Trusted Zone.....	46
Quarantine Zone	47
The VirusBarrier X5 Contextual Menu	49
Using the Intego Menu	50
5 – Understanding Scan Results	51
Scan Results	52
VirusBarrier X5 Logs	53
Using VirusBarrier X5 from the Command Line	57
6 –VirusBarrier X5 Settings and Preferences	58
VirusBarrier X5 Preferences.....	59
General Preferences	59
Scanner Preferences	62
Schedule and Events Preferences.....	66
Logs Preferences.....	68
Locking and Unlocking Preferences	69
About Intego VirusBarrier X5	70



7 - Technical support	71
Help Menu.....	72
Technical Support	72
8 - Glossary	73
Glossary	74



1- About Intego VirusBarrier X5



What is Intego VirusBarrier X5?

Intego VirusBarrier X5 is the simple, fast and non-intrusive antivirus solution for Macintosh computers. It offers thorough protection against viruses and malware of all types, coming from infected files or applications, whether on CD-ROMs, DVDs or other removable media, or in files downloaded over the Internet or other types of networks.

VirusBarrier X5 protects your Mac from viruses by constantly examining all the files that your computer reads and writes, as well as watching for suspicious activity that may be the sign of viruses acting on applications or other files. With VirusBarrier X5 on your computer, you can rest assured that your Macintosh has the best protection available against viruses of all kinds.

VirusBarrier X5 works in the background and checks everything that your Mac does, looking for viruses. It knows the unique signatures of all known Macintosh viruses, and whenever a new virus is discovered, Intego's Virus Monitoring Center goes into action to provide updated virus definitions, which you can download using Intego NetUpdate.

When you purchase VirusBarrier X5, you have access to virus definition updates for one year from the date of installation. After this time, additional subscriptions, allowing you to extend your access to virus definition updates, are available from Intego, and can be purchased by using NetUpdate.

VirusBarrier X5 was designed according to specific concepts. The main idea is that an antivirus program should not require the user to do anything once it is installed and configured, unless a virus is detected. The VirusBarrier X5 philosophy can be summed up in three words: **simple**, **fast** and **non-intrusive**.

Simple

VirusBarrier X5 is the easiest to use antivirus program for Macintosh. After you install it, it works in the background, keeping a close eye on your Mac, and verifies your files silently.



Fast

VirusBarrier X5 is fast and efficient. It does not slow down your Mac, and you can work normally while it's active. Each time a file is created, opened or saved, VirusBarrier X5 checks the file to make sure it is safe.

Non-intrusive

VirusBarrier X5 is non-intrusive. It will not constantly ask you about “suspicious” activity, each time you want to install a program, nor will it generate endless false alarms. Once you have installed it, you probably won't notice it's there, unless it detects a virus and alerts you. In addition, you do not need to deactivate VirusBarrier X5 when installing new software, regardless of what the program's installer or manual may say. VirusBarrier X5 can run all the time, in the background, protecting your Mac without you needing to worry about it.

VirusBarrier X5 is compatible with Mac OS X 10.4 or higher (Tiger and Leopard).



VirusBarrier X5's Features

Virus Scanning

VirusBarrier X5 works in several ways. While its Real-Time Scanner constantly watches over your Mac at all times, protecting you from viruses and malware, it can also work in manual mode, and you can use its on-demand scanner to check any file, folder, disk, or volume, including network volumes, and iPhones or iPod touches connected to a Mac.

Automatic Repairs

If VirusBarrier X5 is running its Real-Time Scanner, it can repair any infected files it finds by eliminating the viruses, if possible. In this mode, you can just forget about VirusBarrier X5's activity—you'll only know it is there if it comes across any viruses or suspicious files.

Quarantine Zone

If you don't want to repair files automatically, you can have VirusBarrier X5 put files in a special quarantine zone. When files are quarantined, they can't be opened or read, which ensures that they cannot infect your Mac. This is useful for administrators who want to check files before running VirusBarrier X5's repair functions.

Manual Scan

You can use VirusBarrier X5 to manually scan your files, disks or volumes to ensure that they are virus-free. This is recommended the first time you install the program, to make sure your Mac is safe. You can also scan individual files by dragging and dropping on the program's icon or on its Orb when it is running in the foreground. We also recommend that you manually scan your Mac each time you install new virus definition updates; an option allows you to run this scan automatically after each update.

Turbo Mode

Turbo mode makes scanning much faster. The first time VirusBarrier X5 scans your Mac, it records information about the files it examines. As long as these files are not updated, VirusBarrier X5 will not rescan them, making scans much faster.



Scan Logs

VirusBarrier X5 stores complete logs of all its activity, and especially of any viruses or suspicious files it finds. You can examine these logs to find out if any files or applications are infected, were repaired, or are damaged. With automatic export of logs, you can rotate log files and store them by date.

Icon, Dock and Contextual Menu

You can scan files or folders for viruses just by dragging them on the VirusBarrier X5 icon, either in the Finder or in the Dock. You can also use a contextual menu item to scan any item quickly from the Finder.

Virus Alerts

VirusBarrier X5 allows you to set alert options so you can know if the program detects any viruses while it's running in the background. You can choose to have the program display an alert, play a warning sound, or even send an e-mail message to a specific address. This can be useful if you want to run VirusBarrier X5 on computers connected to a network, and warn a network administrator or the computer's owner if viruses are detected when they are away from their computer.

NetUpdate

VirusBarrier features Intego's NetUpdate program, which allows you to check for program updates or new virus definitions automatically. You can set the update frequency in NetUpdate itself, so the program checks daily, or weekly on a given day. You can also check current update status at any time using the NetUpdate widget that is included with VirusBarrier X5.



Using this User's Manual

This user's manual provides detailed information on installing, using and updating VirusBarrier X5, as well as a glossary of virus terminology.

You should start by reading the introduction to find out how computer viruses work, and then you should follow the Quick Start instructions (chapter 3). Next, you should read the description of VirusBarrier X5's features and how to scan your Mac (chapters 4 and 5), settings and preferences (chapter 6) and, if you want to know more about viruses, you can consult the Glossary (chapter 9).



2 - Introduction to Computer Viruses



Why You Need to be Protected

You know very well that your Mac contains important information and files. If you use it for your work, you are aware how much time and money it would cost if you were to lose these files. Even if you just use your computer at home, you certainly have files you would hate to lose. On top of that, if a virus were to erase all of your files, even if you did not lose anything important, you would have to spend a great deal of time reinstalling your system and all of your programs.

The virus threat is real. More and more viruses are being discovered every day. While the Macintosh is relatively privileged, compared to Windows, there is still the danger of existing viruses or new viruses spreading to your Mac and damaging your files.

What is a Computer Virus?

Nothing can scare a computer user more than suggesting that their computer may have a virus. Computer users have all heard the horror stories about what viruses can do, and, although some of them may be complacent, none remain indifferent when discovering a virus on their computer.

The problem of viruses is widespread, and is exacerbated by people exchanging files regularly. A virus on one user's computer can spread just as quickly as this year's flu epidemic. Yet, what are computer viruses, really? How do they work? Why are they so dangerous?

The term virus was first applied to computers in the early 1980s, when a self-replicating computer program was released "in the wild".

A virus is simply a bit of executable code that is attached to a file or application. Viruses don't get caught just from the air—they need a means of transmission, which could be a CD-ROM or DVD, or a file sent by e-mail or downloaded from the Internet. Like the viruses that invade our bodies, computer viruses attempt to replicate, after infecting a host, and attach themselves to more files and applications. They clone themselves, attack new hosts, and so on.



Viruses are basically small computer programs—the smaller the better, to hide more easily within files and applications and escape detection. They are written with only one purpose: to reproduce and spread among other computers. While some viruses exist that do no damage, or merely cause a certain text to be displayed on screen, most do indeed harm computers and files. There have been notable cases of viruses written without any malicious intentions, but in most cases, viruses are written with the sole purpose of destroying files, and propagating to other computers. Increasingly, viruses are written to cause economic harm, either by sending personal data to malicious computers, or by hijacking a user's web activity. Viruses, once written by angry teenagers and skillful hackers, are now created by criminals with very clear goals.

Computer viruses can infect any computer, from your home computer to your company's network, unless precautions are taken. The best precaution you can take is to use Intego VirusBarrier X5, and, above all, make sure you keep the program and its virus definitions up to date.

How Computer Viruses Work

In the minds of most computer users, the term “computer virus” includes many types of “malware”, not all of which are actually viruses: Trojan horses and worms, for example, work in different ways, and do not always replicate like viruses do, yet most people tend to include them as part of the virus family. While these programs are malicious, and can seriously damage your computer and your files, they function differently.

A real virus is a small bit of computer code, or programming instructions, that can be executed, or run, on the type of computer it targets. For this reason, viruses written to attack Windows computers have no effect on Macintosh computers, and vice versa. Although if you are running Windows on an Intel-based Macintosh, you will have to consider protecting that operating system as well. Intego's Dual Protection product line offers protection for both your Mac and for your Windows installation.

Viruses do two things when activated on a computer. First, they try and execute their code, in order to do the damage that they were designed for, and then they try to reproduce themselves, by copying this code into other files, applications, disks or network volumes. Here is an example of



what a fictional virus might do on your Macintosh. (Actually, this example presents the actions of a Trojan horse, since it will be easier to understand.)

You receive an infected program from a friend, or colleague, over the Internet. Even though you have been told not to open e-mail attachments that come from people you don't know, this comes from someone you trust, so you open it. Let's assume that it is an application; one of those popular animated greeting cards that people send to each other. You double-click the file, and the application starts running. While it is running, however, it activates its viral code and copies malicious code into your system. At the same time, it spreads across your company's local network, copying itself to other files. After the presentation is finished, you quit the application. Nothing happens to your computer right away, though, since the code is set to truly act only when you restart your computer.

The next morning, when you get to work, and start up your computer, you notice it takes longer than usual to start. When it finally starts, you find that it is running very slowly. When you go to open that urgent report that has to be finished by lunchtime, you notice the file is no longer there. You look through your hard disk, and find that dozens, even hundreds of files are missing. It is then that you realize that you forgot to back up your computer yesterday, and have no copies of any of these files.

In the meantime, you have already sent the animated greeting card to some other friends, but you don't realize that the two are related. It is only several hours later that one of your friends calls, since he realized that the animated greeting card damaged his computer.

As you see, the consequences of this can be very serious. Not only for you, but also for those you are in contact with. One of the biggest problems with viruses today is that computer users are constantly sending files to one another over the Internet, and computers can get infected very quickly. By protecting yourself with Intego VirusBarrier X5, you are also protecting others as well.



Different Types of Viruses

Viruses can be broken down into two different types, according to what they target in your computer. The first type is called system viruses, since these viruses attack system files. The second type, file viruses, infects applications and data files.

Viruses

A computer virus is a small program that acts like a parasite, living in a host file or program, that is capable of infecting files and applications, reproducing itself, and spreading to other computers through infected files and applications. It is no surprise that people use terms originally used for diseases to speak of computer viruses—they work in a very similar manner.

Viruses that attack your system are among the most lethal. The damages they can do are such that you may need to reinstall your system entirely, and even reformat your hard drive and check all your backups to make sure they are disinfected.

File viruses are different from system viruses in that they attach themselves to data files, rather than applications, and their hosts depend on specific programs to do their damage. These viruses often come in attachments to e-mail messages, which, when opened, activate their malicious code.

Some viruses act very quickly, while others are set to go off at a certain time. Some merely content themselves with spreading to other disks and volumes, but all system viruses can potentially cause damage, such as erasing all your files.

Trojan Horses

The name Trojan Horse comes from an episode in the war that opposed the Greeks and the city of Troy, several millennia ago. The Greeks built a huge, hollow wooden horse and gave it to the Trojans, apparently as a gift, before supposedly sailing away and ending the war. While some of the Trojans were skeptical about it, the horse was taken inside their stronghold. That night, Greek warriors emerged from the horse, opened the city gates, and Greek soldiers from outside stormed the city.



It is obvious that the Trojans were never told not to open attachments. The Trojan horses that we are worried about are programs that look innocent and claim to do a certain task, but actually contain malicious code or viruses. In many cases, Trojan horses can be even more dangerous than other viruses. One example is the RSPlug Trojan horse (also known as DNSChanger), which Intego's Virus Monitoring Center discovered in 2007. This malware, disguised as a video codec—software needed to view videos on a web site—changed the DNS server on a Mac to hijack its web traffic.

Worms

Worms are one of the oldest forms of viral programs on computers. They spread by methods other than attaching themselves to files and applications, and can be very difficult to find. They spread over networks, and, once they find new hosts, can carry out malicious actions.

Macro Viruses

Many programs provide the ability to create macro commands. These simple programs use the internal functions of an application or helper program to “record” and “play back” commonly used sequences of commands. Other applications provide a more powerful macro language, which includes both menu commands and a programming language. Programs such as Microsoft Word and Excel, for versions prior to Office 2008, base their macro functions on Visual Basic, which is similar to the Basic programming language. Several thousand macro viruses have been found, most affecting Microsoft Word and Excel.

The real danger of macro viruses is the fact that they are cross-platform viruses. A macro virus that can attack Microsoft Word for Windows can also damage Word on a Mac. One of the reasons that macro virus writers target Microsoft programs is that these applications allow users to embed macros in data files. In the past, one worried only about viruses coming through applications, since, for a virus to act, it has to execute, and only applications could execute. But the Microsoft Visual Basic approach is different—if you wish to use a macro, you can either run it from your template, or add it to a data file. This surprised users at first, since they thought that nothing was “executed” when opening a word processor or spreadsheet file. But these files can indeed contain “programs”, and do things you would never expect.



If the macro language provides the possibility to modify files, a macro virus will be able to copy itself into other files used by the same application. This then allows the virus to spread when you open other files, create new files, or pass files on to someone else.

Macro viruses can do many things: some may simply alter their program's environment, such as changing or removing menus or commands. Others can corrupt or delete files, hide certain application functions, and even more. And, on top of all that, they are cross-platform viruses, which can do damage both to Macs and PCs running Windows, as well as Windows running on a Mac.

It is important to note that macro languages are very powerful tools that can be extremely helpful. Not all macros are viruses. While Microsoft Word and Excel include a preference to alert you if there are macros in any documents you open, this defeats the purpose of having a macro function. The real problem is that the macros are stored in data files, rather than, say, in separate macro files. Users could easily exchange macros, and be certain that the files they open contain only data. Unfortunately, this approach to a macro language leads users to be far too worried about macros, instead of using them for their function-enhancing properties.

VirusBarrier X5 detects all known Word and Excel macro viruses, and is updated when new macro viruses are found.

How do Viruses Spread?

Viruses can spread through infected files on CDs, DVDs or other removable media, or downloaded from the Internet. They can also be sent as attachments via e-mail. Infected files cannot spread their viruses without being opened or read. Merely copying an application cannot cause a virus to spread, but starting up that application can. VirusBarrier X5 protects your computer from these viruses by scanning files on your computer when they are written, used or opened. As soon as you do something with a file, it is scanned immediately, and if VirusBarrier X5 detects a virus, the file or application will be disinfected or rendered inoperable.



How Can You Protect Yourself from Viruses?

There are a few simple ways you can protect yourself from computer viruses. The first, and certainly the most important, is to use VirusBarrier X5 to constantly monitor your computer and automatically check for viruses. VirusBarrier X5 provides the best protection for your Macintosh, and works in the background, to ensure that your computer remains safe.

To ensure that VirusBarrier X5 is always watching out for all known viruses, you must update the program regularly. Intego NetUpdate makes this easy to do, even automatic, if you choose. You should check for updates at least once a week. If any major new viruses are discovered, we will post information on our web site (www.intego.com) as soon as possible, as well as on Intego's Mac Security Blog (<http://blog.intego.com>). Intego's Virus Monitoring Center is ready 24/7, and will react on the first signs of any new viruses.

If you think you have caught a new virus, see chapter 7, Technical Support, for instructions on how to contact Intego.

To protect yourself as much as possible, you should only use software that comes from reputable sources. Pirated software may contain viruses, or may be an unexpected Trojan horse. Only install software if you are sure of where it comes from.

In addition to this, you should be very wary of attachments or other files sent by e-mail or over the Internet. We have seen how the oldest recorded case of nonchalantly opening an attachment led to disastrous consequences (when the Trojans "opened" the horse given to them by the Greeks). People used to say that you should never open attachments from people you don't know, but many viruses have spread because they were in attachments that came from friends and co-workers. VirusBarrier X5 protects you by scanning every file as you open it, and eliminating all known viruses automatically. If you are on a network, and VirusBarrier X5 detects a virus in an attachment, make sure you contact your network administrator immediately, so they can remove the infected file from your company's mail server.

In spite of all the antivirus protection provided by VirusBarrier X5, there still remains one additional thing you should do to protect your data: back up your files regularly. Not only should



you back up important files every day, but you should also make multiple backups of them. The media you use for backups could get damaged or corrupted, and, in this case, your backups won't be of much use. Intego Personal Backup X5 provides a complete backup solution, and it can even run backups automatically, so you can be sure to always have a safe copy of your data in case your Mac does get a virus.

A good way to work is the following: you should have two different backups of your data. Think of this as insurance. Not only does this ensure that you have clean copies of your files if you find a virus on your computer, but it also protects your data from any other types of problems, such as hard disk crashes, etc. Given the relatively low cost of removable media, or even writable CDs, DVDs or external hard disks, you should also back up your System and applications as well. Remember, if, for some reason, your computer gets corrupted, it will take you a long time to reinstall your system and applications. If you back up your entire Mac, you will be able to do this in just a few minutes. Intego Personal Backup X5 offers a full range of backup features, including incremental backups, bootable system backups, and synchronizations. With a coherent backup policy, you can make sure that even if you do have problems, you'll be back to work quickly.



If You Think You Have a Virus

Some Symptoms of Infection

While the presence of these symptoms does not necessarily mean that a virus has attacked your computer, they could be signs of a viral attack:

- You see unexpected error messages,
- Your Macintosh crashes inexplicably,
- Applications quit unexpectedly,
- Your system seems to be running unusually slowly,
- You discover new user accounts that you have not created,
- Your disk space seems to have reduced significantly, even though you have not added many files.

If your Mac starts showing any of the above symptoms, there are several things you can do to check if the problem comes from a virus or from other software problems.

First, you should run Intego NetUpdate and check that you have the latest virus definitions for VirusBarrier X5. You can then scan your Mac to make sure you are free of malware.

Next, if this doesn't solve the problem, it is more likely that you have disk corruption. You can run Apple's Disk Utility program. This program is designed to diagnose problems that you may have with your computer's hard disk, and repair most of them. It is installed by default in the Utilities folder of your Applications folder. If Disk Utility finds problems that it cannot repair, you will need a commercial disk maintenance program.

If this does not solve your problem, you should think about any recently installed software. Most problems with computers come from software conflicts. If you have recently installed any new software, try uninstalling the software, and see if the problem persists.



Your problem may come from other hardware, such as external drives, any USB hardware you may have connected to your computer, your printer driver, etc. Again, see if the problem continues when these devices and their drivers are activated.

For more help, you can go to the Support section of the Apple web site (www.apple.com) to see if there is a solution for your problem.

Finally, if you think that you have an infected file, you can send a copy of the file to the Intego Virus Monitoring Center. For information on this, see chapter 7, Technical Support.



Basic precautions

Even though VirusBarrier X5 is now keeping a close eye on your Macintosh, you should still get into the habit of respecting a few basic principles to make sure that your files will always be protected.

- Make regular backups of your files. Use Intego Personal Backup X5 to run automatic backups of your users files and to create bootable backups of your entire Mac.
- Make several copies of your most important files.
- When your removable media “travel” to other computers, or if you lend them to other people, make sure they are write-protected by sliding the write-protection tabs (if possible). Use VirusBarrier X5 to scan any external hard disks, USB key drives or flash memory cards that others lend you to transfer files.
- Do not deactivate VirusBarrier X5 unless you absolutely must: you do not need to deactivate VirusBarrier X5 to install new applications, even though some installation programs may request this.
- Do not use pirated software: not only is it against the law, but these programs may also carry viruses.
- With this in mind, only install programs if you are sure that the original packaging has not been tampered with.
- Think about using NetUpdate to verify that your version of VirusBarrier X5 is up-to-date, and do this regularly, to make sure you have the latest version.

To ensure that there is no incompatibility, use only VirusBarrier X5 to protect your computer against viruses.



System Requirements

- Any officially-supported Mac OS X compatible computer
- Mac OS X 10.4 or higher, or Mac OS X Server 10.4 or higher

Installing VirusBarrier X5

For information on installing and serializing VirusBarrier X5, see the Intego Getting Started manual, included with your copy of the program. If you purchased VirusBarrier X5 by download from the Intego web site, this manual will be in the disk image you downloaded that contains the software. If you purchased VirusBarrier X5 on a CD or a DVD, you'll find this manual on the disc.



3 - Quick Start



Intego VirusBarrier X5's Interface

When you install Intego VirusBarrier X5 and restart your Macintosh, you must launch the program once and enter your serial number for the program to start watching over your Mac. VirusBarrier X5 is designed to be simple and non-intrusive, and it fully protects your computer without your doing anything at all.

Once VirusBarrier X5 is installed, you can just let it run on its own. However, it is recommended that you either set NetUpdate to make automatic checks to find if the program has been updated, or that you make manual checks at least once a week.

To open VirusBarrier X5, and change any of the settings, or run a manual scan, either:

- Double-click the VirusBarrier X5 icon in the Applications folder, or
- Choose Intego Menu > VirusBarrier X5 > Open VirusBarrier X5...

The VirusBarrier X5 application contains the Orb, the Scan button, and several other instruments that display information or let you change settings. To access any of these features, click on one of the small arrow buttons on the interface.



The Intego VirusBarrier X5 Orb, the large green area in the center of the window, gives you information about the current operation. Around the Orb are six “instruments”, gauges and displays, and beneath the Orb is the Scan button.



The Scan button below the VirusBarrier X5 Orb changes according to the function it can have, such as Scan, Pause, Stop, etc. By default it is a Scan button: if you click it, VirusBarrier X5 will scan your Mac for viruses and other malware. If it finds any, an alert window will ask you what to do. But when you press the Option key, the Scan button turns into a Repair button, which means that VirusBarrier X5 will automatically repair any files containing viruses or malware it finds without asking for your intervention. If you press the Option (Alt) key during a scan, the button displays Pause; click the button to pause your scan.



The Select button above the Scan button lets you select volumes, folders or files to scan for viruses. See Selecting Files and Running a Manual Scan in Chapter 4, “Scanning and Repairing Your Mac with VirusBarrier X5” for more about selecting items to scan. If you press the Option (Alt) key, the Select button becomes Browse, and you can click this to browse your Mac to scan files or folders.

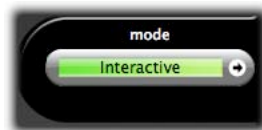


The Schedules instrument shows you how many scans are scheduled, and allows you to set a schedule of fixed times when you want to run scans. If any scans are currently running, the number of active scans will display in parentheses in the Schedules instrument following the total number of scheduled scans. If you click the arrow button, you can set schedules; see Scheduled Scanning in Chapter 4, “Scanning and Repairing Your Mac with VirusBarrier X5” to learn how to set schedules.



The Mode instrument shows you in which mode VirusBarrier X5 is working. This can be:

- Interactive mode, where the program will display an alert asking you what to do when it finds infected files,
- Repair mode, where the program will automatically repair infected files, or
- Quarantine mode, where VirusBarrier X5 will place infected files in its quarantine zone.



If you click the arrow button, you can change the mode; see Scanner Preferences in Chapter 6, “VirusBarrier X5 Settings and Preferences” to learn more about choosing modes.

The Malware Quarantine instrument shows how many files are in VirusBarrier X5’s quarantine zone, and its gauges react when new files are added. If you click the arrow button, you will go to the quarantine zone; see the Quarantine Zone section in Chapter 4, “Scanning and Repairing Your Mac with VirusBarrier X5” to learn about using the quarantine zone.



Three instruments provide visual representations of how fast VirusBarrier X5 is:

The Velocity Monitor shows how hard your Mac's processor (or processors) is working.



The Turbo Mode instrument shows how efficient VirusBarrier X5's Turbo Mode is. When VirusBarrier X5 scans your files, it remembers which ones it has scanned, and adds these files to a database. The next time it scans your Mac, VirusBarrier X5 doesn't need to rescan all files, but only those that have been opened or changed since the last scan. However, when you install new virus definitions, VirusBarrier X5 rescans *all* files, and resets the Turbo Mode database; this is to ensure that all files are checked against new virus definitions.

The Turbo Mode instrument shows the percentage of files, during a scan, that are in the Turbo Mode database. When the needle is toward green, VirusBarrier X5 is saving time by using Turbo Mode. When it is toward red, VirusBarrier X5 is scanning files for the first time, or is scanning files that have changed since the last scan.

You can reset the Turbo Mode database by clicking the Reset button in the Turbo Mode instrument. If you do this, VirusBarrier X5 will start from scratch the next time you run a manual scan, checking all your files.



Note: when you use VirusBarrier X5's Turbo Mode, the program will write invisible files, named .vbt5, at the root level of every writeable volume it scans.



The Real-Time Scanner instrument shows the activity level of VirusBarrier X5's Real-Time Scanner, as well as the number of files scanned since the last time you restarted your Mac.

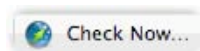


Two additional buttons appear at the top and bottom of the window.

The Log button in the lower-right corner opens a list of logs that show you the dates and times of any manual scans and any infected or damaged files found.



The NetUpdate button, labeled “Check Now...”, lets you check for updates to VirusBarrier X5. The NetUpdate button displays in the NetUpdate Status Bar; if you don't see this bar, choose View > Show NetUpdate Status Bar. For more information about NetUpdate, see the Getting Started manual.



First Things First: Scan Your Entire Hard Drive for Viruses

VirusBarrier X5 has numerous features that protect your Mac from viruses whenever they appear. But before you do anything else, you should run a full scan of your Mac to identify and eliminate any viruses that are already there. Here's how.

If your Mac just has one hard drive, or if you want to scan all the drives connected to your Mac, simply click the Scan button.

If you have several drives and only want to scan some of them, do the following:

1. Click the Select button.



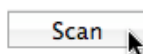
2. Click the Hard Drives button.



3. Click each hard drive that you want to scan.



4. Click the Scan button.



In either case, VirusBarrier X5 will first count all the files on your Mac, then will check each one to ensure that it's virus-free. Because this process can involve hundreds of thousands of files, it could take several minutes or even hours. You can still use your Mac while VirusBarrier X5 runs this scan; however, you may wish to wait until you're not actively using your computer for other purposes before running this initial check, and ensure that your computer is plugged in instead of running on battery power.

For details on what to do if VirusBarrier X5 finds a problem, see Alerts in Chapter 4, "Scanning Your Mac with VirusBarrier X5".



4 – Scanning Your Mac with VirusBarrier X5



Virus Scanning

VirusBarrier X5 works in several ways. Its Real-Time Scanner constantly watches over your Mac, protecting you from viruses, and automatically checking all files when they are opened or saved. You can also use VirusBarrier X5's on-demand scanner to check any file, folder, disk, or volume on your Mac.

The Real-Time scanner ensures that your Mac is protected at all times by scanning every file that is created, copied, modified or saved. It does not, however, scan other files. This is why we suggest you run a full scan of all your files when you install VirusBarrier X5 and after each update to the program's virus definitions.

Selecting Files and Running a Manual Scan

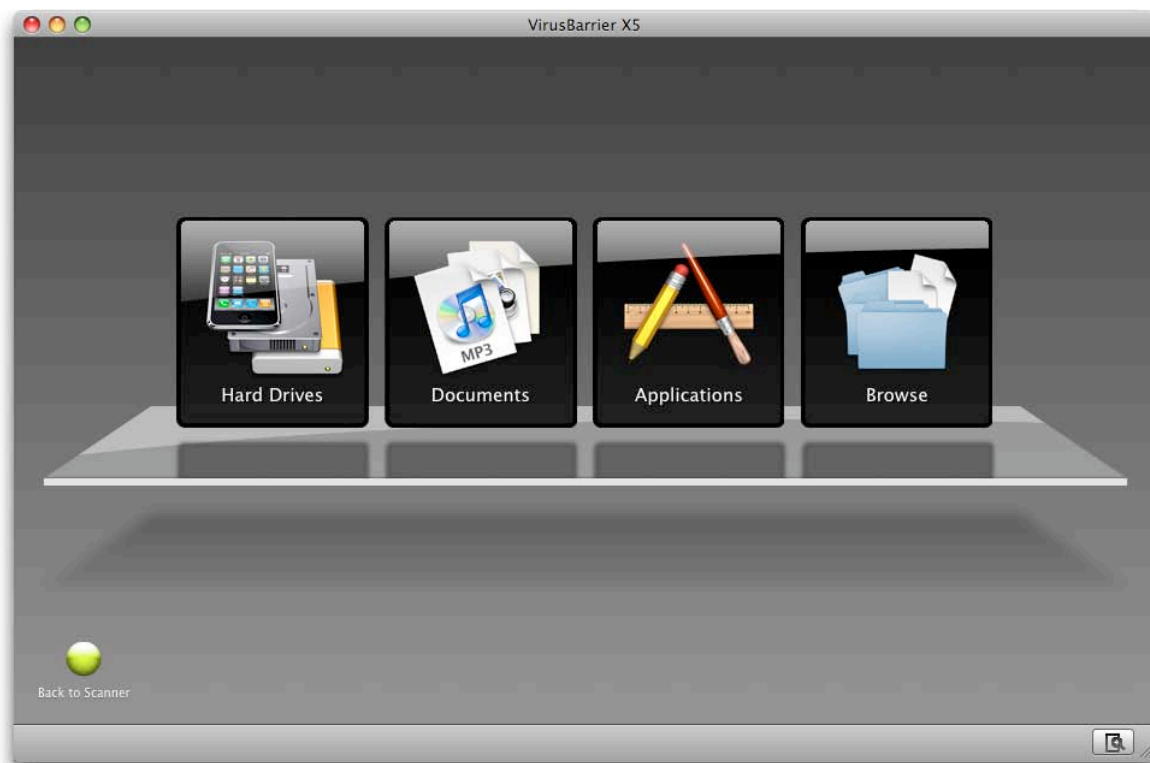
Once VirusBarrier X5 is installed, it watches over your files ensuring that they are safe from viruses. But VirusBarrier X5 also checks files as they are opened and saved. This is a unique feature of VirusBarrier X5 that reduces the time required to scan files, making it truly non-intrusive.

You can run a manual scan any time you want. You should do this immediately after installation to ensure that you don't have any infected files. After that, VirusBarrier X5 makes sure that any new files are safe.

If you did not choose to run a manual scan after installation, to run a manual scan at any time, open VirusBarrier X5 by double-clicking its icon in the Applications folder. You can also choose to do a manual scan of any individual files or folders by simply dragging and dropping them either onto the program's icon in the Finder or in the Dock, or onto the Orb when VirusBarrier X5 is in the foreground.

Click the Select button to see four ways to select items to scan.



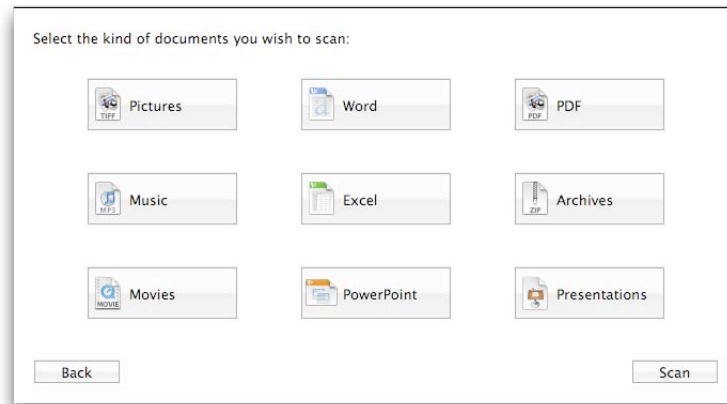


The **Hard Drives** button shows a list of all the hard drives connected to your Mac, as well as any iPhone or iPod touch connected. In this case there's only one, named "Macintosh HD". As with all four selection screens, click the item you wish to scan to highlight it. To deselect an item, click it again. Click Scan to begin the scanning process, or click Back to return to the selection screen.

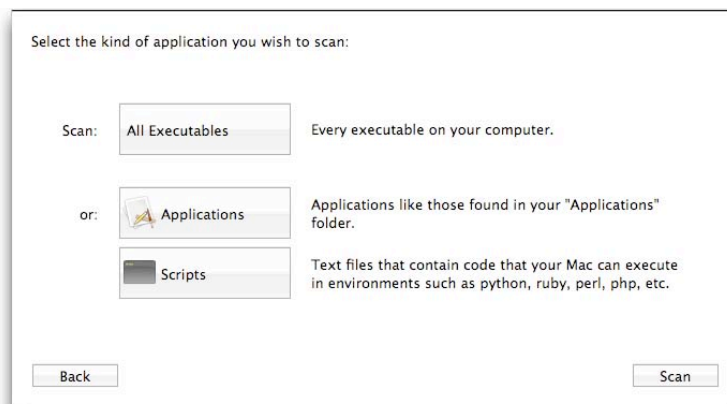


The **Documents** button allows you to select the items you'd like to scan by several common document file types, such as PDF, Microsoft Word, or movie files. As described above, click those you wish to scan.



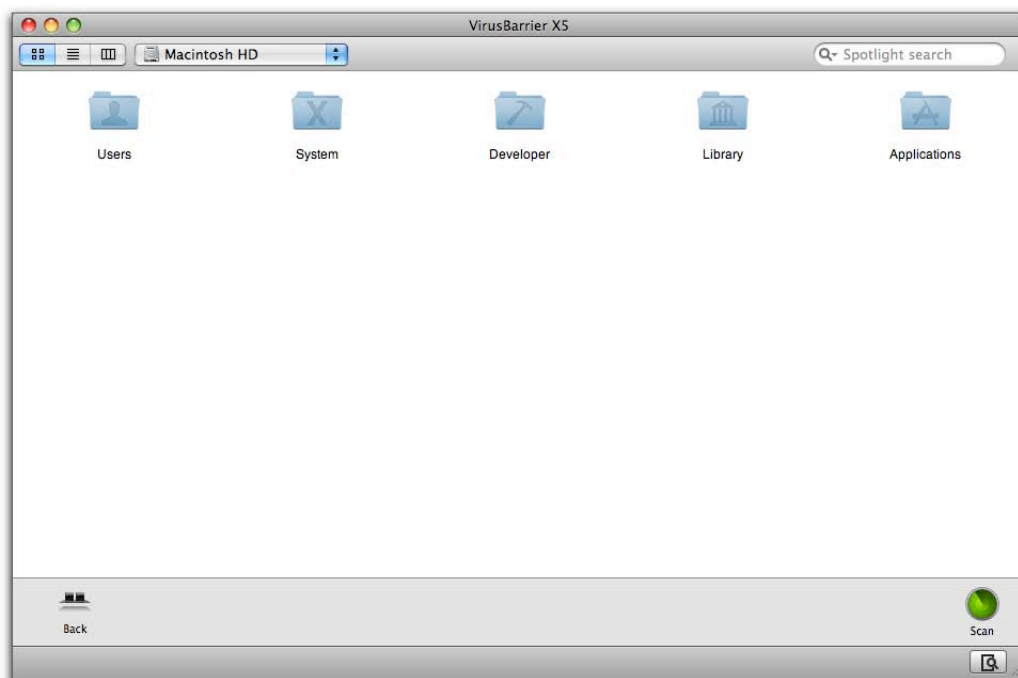


The **Applications** button gives you three options to scan executable files, commonly known as applications or programs. These files especially carry potential danger, as viruses that have “piggybacked” on applications, or that masquerade as applications themselves, could gain access to all the system resources of the application itself. Your options are to scan All Executables that VirusBarrier X5 finds, only those contained in your Applications folder, or executable scripts contained in innocuous-seeming text files (as is commonly found in programs written in some languages such as Perl and Python).

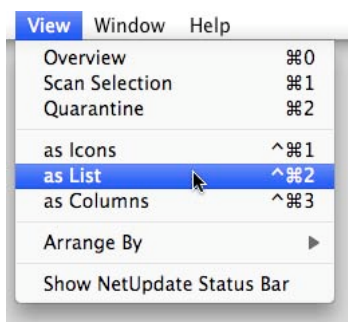


Finally, the **Browse** button allows you to select any group of files and/or folders you’d like to scan, regardless of location or file type. Clicking this button shows you files on your Mac as icons in a Finder-like view.



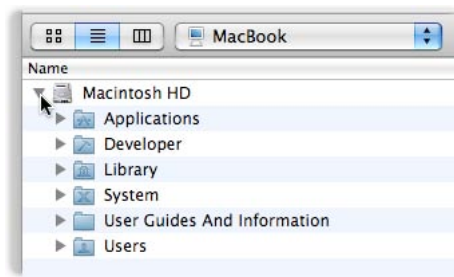


As in the Finder, you can change the view to see your files as a simple list or in a file browser by clicking on the view buttons in the window's upper-left corner. You can also change the view by choosing the desired selection under the View menu ("as Icons", "as List" or "as Columns") or by pressing the appropriate keyboard shortcut (Control-Command-1 for Icons, Control-Command-2 for the list view, and Control-Command-3 for the columnar browser view).

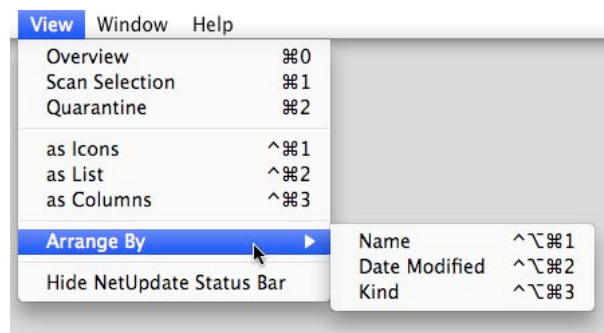


When the list view is visible, you can display files inside a folder by clicking on its disclosure triangle, to the left of the folder's name.

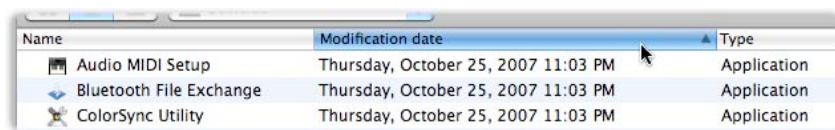




In both Icon and List view are options that let you change the order in which items appear, under the View > Arrange By menu: either select the order you prefer, or press the appropriate keyboard shortcut (Control-Option-Command-1 to sort by name, Control-Option-Command-2 to sort by the date the file was last modified, Control-Option-Command-3 to sort by file type, or “Kind”).



In List view, you can also change the view order by clicking on a column’s header to sort by that column’s criterion. Here we’re sorting by the Modification date, ascending. To sort a column in descending order, click the column header again.



Regardless of how you’ve chosen to view your files, you can select multiple items by making them visible, then holding down the Command key as you click on each one in turn. When you’ve made your selection, click Scan to begin the process.



You can also scan any individual volumes, files or folders by simply dragging and dropping them either onto the program icon when it is running in the background, or onto the Orb when VirusBarrier X5 is in the foreground.

If you have selected Count files before scan in the Preferences, VirusBarrier X5 counts how many files are to be scanned, then displays the number of files scanned and the percentage of the scan completed. Additionally, the Orb's rim changes to visually indicate how close the scan is to completion.



VirusBarrier X5 can scan files contained in compressed archives. When scanning archives, the Orb's display changes to show that it's working on an archive, and gives you an opportunity to skip scanning of that archive, if it is very large and you are sure it is secure.



If you press the Option key when an archive is displayed in the Orb, the Skip button changes to Reveal, so you can see where the archive is located.



When scanning an iPhone or iPod touch, VirusBarrier X5 copies all the files contained on the device to the user's startup volume in order to verify their security. If any malware or infected files are found, VirusBarrier X5 alerts the user and offers to repair or delete the infected files.

You can stop the scan at any time by clicking the Stop button. If you wish to pause the scan, hold down the Option key on your keyboard, and you will notice that the Stop button now displays Pause. Click this button, and scanning will pause.



To resume scanning, click this button, which will now show Resume.



Drag and Drop Scanning

You can scan any volume, folder or file by dragging it onto the Orb. You may need to enter an administrator's password if you do not have the appropriate permissions to access files contained in the item you drag on the Orb.



You can also do this by dragging and dropping the volume, folder or file onto the VirusBarrier X5 program icon in the Finder.



Finally, you can drag and drop items to scan onto VirusBarrier X5's Dock icon.

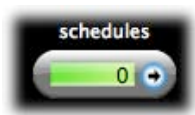


Once you release the item to be scanned, Intego VirusBarrier X5 will start scanning it, the same as for any other manual scan.

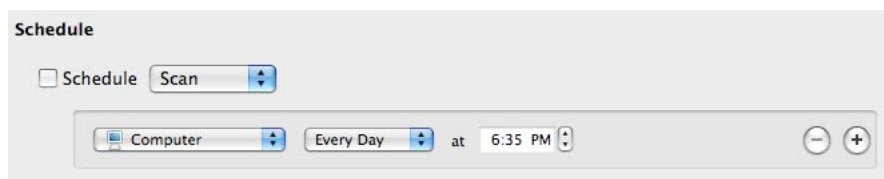


Scheduled Scanning

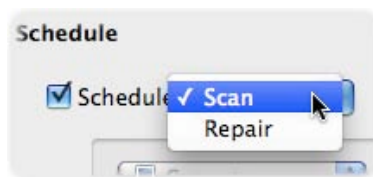
VirusBarrier X5 can also be set to run automatically at pre-arranged times. Click the arrow on the Schedules instrument to open the Schedules and Events Preferences.



The settings at the top of this window control several functions that we'll discuss in chapter 6, "VirusBarrier X5 Settings and Preferences". For now, we'll just look at the Schedule section at the bottom of the window.



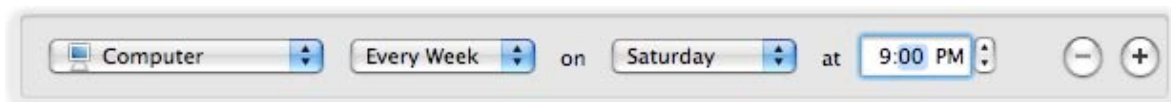
To turn on scheduling, click the Schedule checkbox. In the popup menu next to it, you can select whether VirusBarrier X5 will simply scan your files at the appointed time, or also make any repairs it can if it finds any infected files.



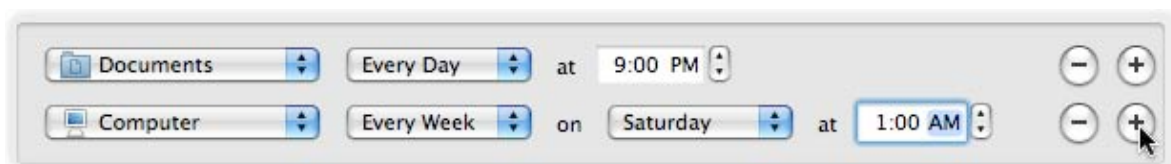
Below these settings is a scheduling selector, where you can say which folder should be examined, and when. The first popup menu lists the folders you are most likely to want to scan, including your home folder and your Documents folder. The default choice, Computer, directs VirusBarrier X5 to scan all folders for all users on your Mac.



The second popup menu lets you choose whether you want to perform the operation every day or every week. If you select Every Day, you'll be able to choose the time you prefer; select Every Week, and you'll also choose your preferred day.



You can create multi-part schedules, for example to scan your Documents folder every night, and your entire computer once a week. To do so, click the + button to the right of the schedule item: another schedule item will appear beneath it. Make changes in that schedule item as you like. You can add as many schedule items as you like this way; to remove one of them, click the – button next to it.



The order of schedule items is not important; if you've scheduled two scans to run at the same time, they will occur simultaneously.

When you're done, the number of pending schedule items appears in the Schedules instrument on VirusBarrier X5's main window. To turn off all pending schedules, return to the Schedules and Events Preferences screen and uncheck the Schedule button.



E-mail Analysis

Another useful feature of VirusBarrier X5 is that it scans and analyses both incoming and outgoing e-mail. This means that any attachments which are infected are picked up and identified on arrival, before they have the chance to do anything destructive to a recipient who may still be occupied looking over other incoming e-mails. Messages are also scanned when sent, ensuring that you do not infect any other computers.

VirusBarrier X5 also scans and analyses outgoing e-mail and attachments, thus making sure that you are not passing on any viruses to your correspondents either.

VirusBarrier X5 can only scan e-mail messages from programs that store their messages as individual files, such as Apple's Mail. However, when you open or save attachments, VirusBarrier X5 scans all files, regardless of what program they come from.



Alerts

While VirusBarrier X5 can be used to run manual scans, as seen above, most users set it to work in the background. It has several ways of alerting you if it finds any infected files.

If VirusBarrier X5 detects any infected files, and you have set it to scan, and not automatically repair infected files, it will display an alert.



If you scan items by dragging them on the VirusBarrier X5 Orb, the alert is different:



Clicking Reveal In Finder will show the location of the file on your hard disk. If you want VirusBarrier X5 to repair the file, click Repair; to put it in the Quarantine Zone, click Put in Quarantine. (See the Quarantine Zone section later in this chapter for more about using the Quarantine Zone.) If you don't want to do anything, click Ignore, and the file will not be repaired.



WARNING: Ignoring virus warnings can be dangerous! Only select to not repair files if you are sure of what you're doing.

If you don't respond to an alert within one minute, VirusBarrier X5 places the file in the Quarantine Zone. You can check files later in the Quarantine Zone to decide what to do with them. See the Quarantine Zone section later in this chapter.

For more on setting Alert preferences, see **chapter 6, Intego VirusBarrier X5 Settings and Preferences**.



Trusted Zone

VirusBarrier X5 offers the option to add files, folders or volumes to a Trusted Zone. VirusBarrier X5 will trust all files you add to this zone, and will not scan them. You should only use this for safe files that have already been scanned by VirusBarrier X5.

To add items to the Trusted Zone, open VirusBarrier X5's preferences and click the Scanner icon. In the Trusted Zone section, you can define files, folders or volumes that VirusBarrier X5's Real-Time scanner will not check. However, VirusBarrier X5 will check these files when you run manual scans of your Mac.



To add an item to the Trusted Zone, click the + button, browse to an item, then click Choose. You can also drag files or folders from the Finder to this field. Note that adding a folder or volume tells VirusBarrier X5 to trust *all* files contained in the selected item and any subfolders it contains. To remove an item from the Trusted Zone, click it to select it, then click the – button.

You can also use the Contextual Menu to add items to the Trusted Zone. See the following section of this manual for more information.



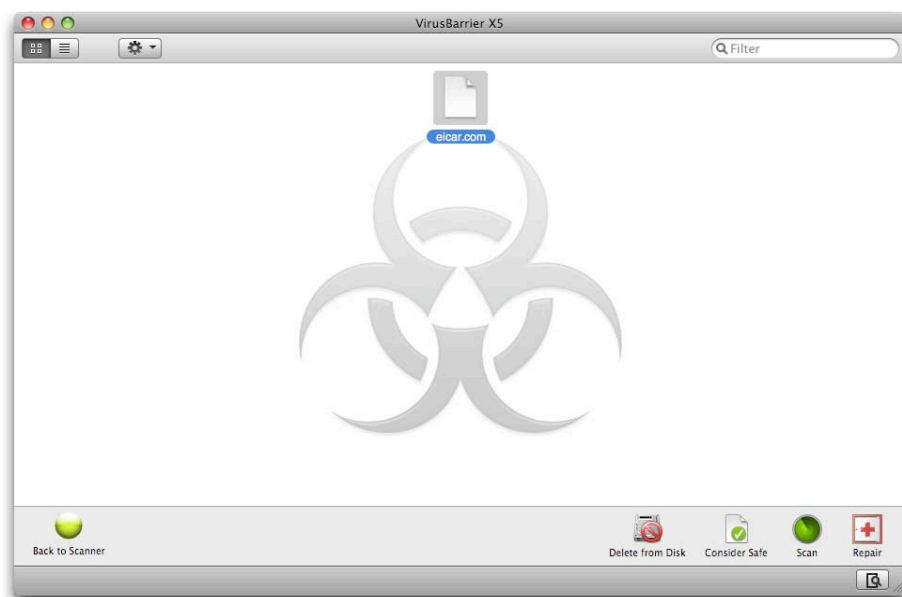
Quarantine Zone

If you don't want to repair files automatically, you can have VirusBarrier X5 put them in a special quarantine zone. When files are quarantined, they can't be opened or read, ensuring that they cannot infect your Mac. This is useful for administrators who want to check files before running VirusBarrier X5's repair functions.

As mentioned above when discussing alerts, VirusBarrier X5 places files in the Quarantine Zone if you don't respond to an alert within one minute. You can then check these files and decide what to do. The Malware Quarantine instrument shows you how many files are in the Quarantine Zone.



To view the contents of the Quarantine Zone, click the arrow button on this instrument. You'll see a display that shows which files are in the Quarantine Zone, as well as a group of buttons allowing you to act on those files.



You can choose to view files in the Quarantine Zone in either Icon view or List view; click one of the view buttons at the top left of the window to change this.

To act on any of the files, select a file, then click on one of the four buttons at the bottom right of the window.



You can do the following:

- **Delete from disk** removes the file from your Mac.
- **Consider safe** tells VirusBarrier X5 that you think this file is not infected. This may occur for false positives. However, be *very careful* in clicking this button; only do so if you are sure that the file is safe. If not, it may infect your entire Mac.
- **Scan** tells VirusBarrier X5 to scan the file again. You may want to do this if you have files that were automatically added to the Quarantine Zone and you want to know what they are infected with.
- **Repair** tells VirusBarrier X5 to repair the file, removing the virus.

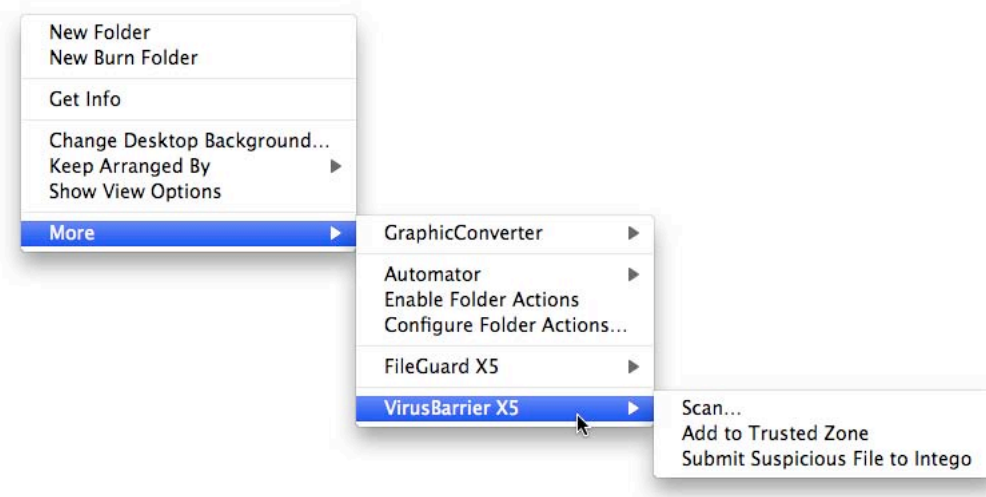
If you display the Quarantine Zone in list mode, a Virus column will tell you which virus your files are infected by.



The VirusBarrier X5 Contextual Menu

VirusBarrier X5 also offers an option to run directly from the Finder under Mac OS X, using a Contextual Menu.

To do so, just Control-click or right-click on any item—a file, folder or volume— and a contextual menu will open. In Mac OS X 10.5, Leopard, the VirusBarrier X5 menu appears under a “More” menu, while earlier versions of Mac OS X show the VirusBarrier X5 menu immediately.



The contextual menu lets you do the following:

- You can scan the selected item (and repair it if your settings allow).
- You can add the item to the Trusted Zone (exceptions to scans, where data is known to be so safe that no scans are run).
- You can submit a copy of the item to Intego by selecting Submit Suspicious File to Intego. You will need to configure e-mail settings to do this. If you have not done so in VirusBarrier X5's Log preferences, a dialog will ask you for the appropriate information. This is especially useful if you have files that you suspect are infected with new or unrecognized viruses. If you choose this option, Intego's virus experts can examine the file and produce the virus definitions you and other users will need to protect their systems.

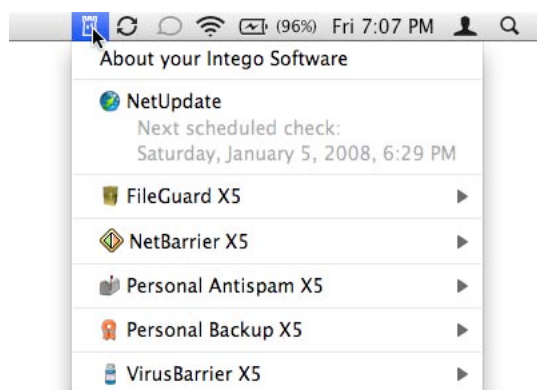


Using the Intego Menu

VirusBarrier X5, like all other Intego programs, installs a menu in the menu bar, called the Intego menu. Its icon is a small tower, as in the Intego logo.



Click the Intego menu icon to display a menu that shows all your Intego software:



You can start and stop the Real-Time Scanner, or open VirusBarrier X5 from the Intego menu.



For more details on using this menu, see the Getting Started manual.



5 – Understanding Scan Results



Scan Results

When you run a manual scan, VirusBarrier X5 informs you if it finds files infected by any known viruses. If any infected files are found, the VirusBarrier X5 Orb will turn red. If VirusBarrier X5 discovers any corrupted files, the Orb will turn orange. If both infected and corrupted files are found, the orb will blink red and orange. VirusBarrier X5 will also alert you according to the alert options you have set in the Preferences. For more on alert options, see chapter 6, **VirusBarrier X5 Settings and Preferences**.



You can discover more about scan results by checking the VirusBarrier X5 logs.



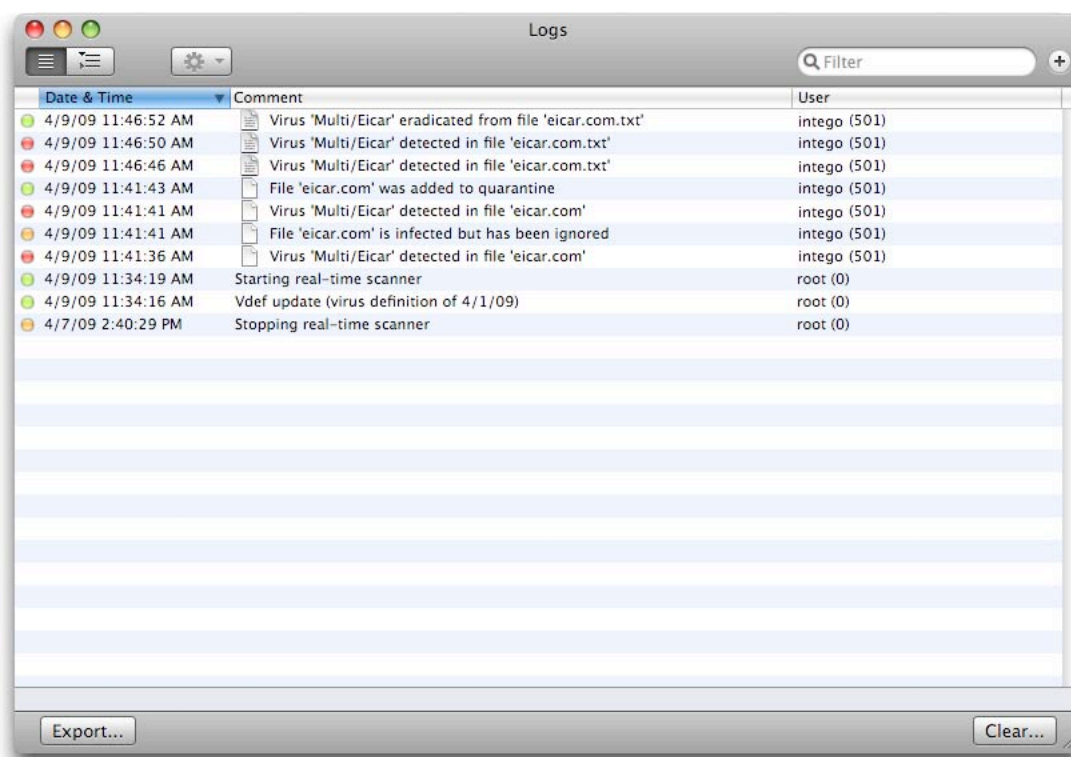
VirusBarrier X5 Logs

To see what operations VirusBarrier X5 has performed since it was first installed, click the icon in the lower-right corner of the main window to reveal the Logs window.

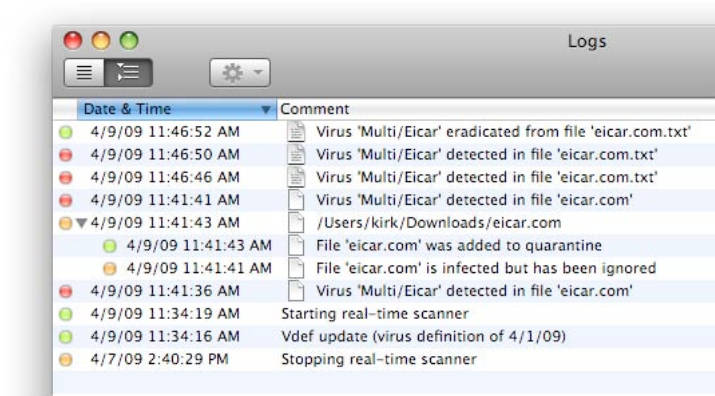


The Log will also appear automatically if VirusBarrier X5 finds any infected files, and you've selected that option in the Logs Preferences (See chapter 6, "VirusBarrier X5 Settings and Preferences"). You can also open the log by choosing the Intego menu > VirusBarrier X5 > Open Logs.

The log looks as follows, although of course your log will show different entries from this one.



There are two ways you can display log information. In the example above, log entries are shown in linear order, each one taking up one line. You can click the second button at the top-left of the window and display log entries in hierarchical order, where disclosure triangles group related entries:

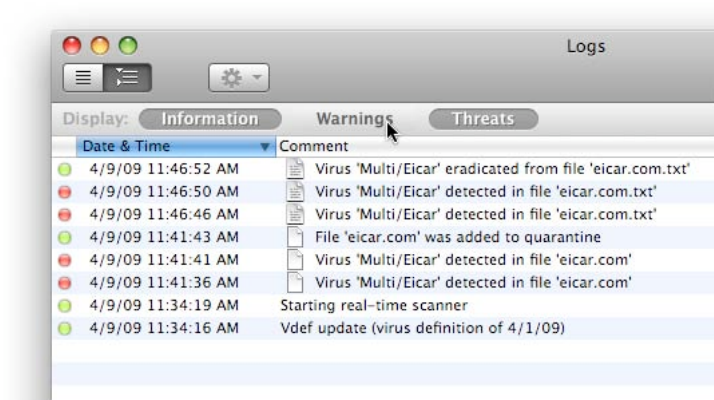


The Log shows every time that:

- You start a scan
- You cancel a scan in mid-process
- Start or stop the real-time scanner
- VirusBarrier X5 finishes a scan, with its results
- VirusBarrier X5 discovers a virus
- VirusBarrier X5 discovers a corrupted file
- VirusBarrier X5 repairs an infected file
- Files are added to or removed from the Quarantine Zone
- Virus definitions are updated

The colored dots in the leftmost column give you a sign of what types of entries are in the log. Green dots indicate information, such as starting the real-time scanner or updating virus definitions. Orange dots are for warnings, such as stopping the real-time scanner. Red dots indicate threats, such as when infected or corrupted files are found. The files, folders or volumes selected for each scan are named, as are all problems found. You can choose to only display certain types of information by clicking the + icon at the right of the log window, then clicking one of the three log type buttons to hide or display their entries.



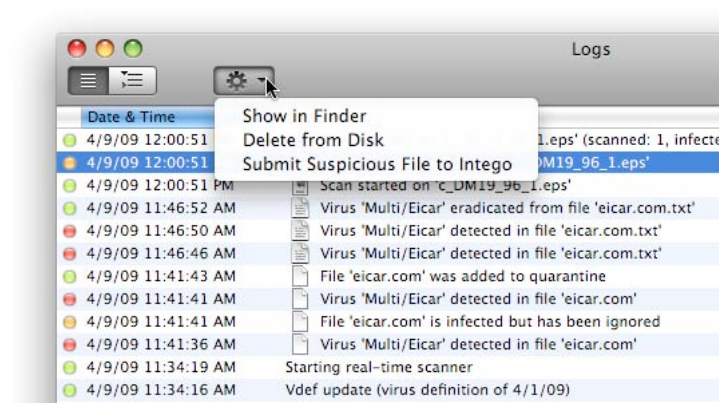


If malware is found, they will be listed in the log in one of four categories:

- Virus
- Backdoor
- Trojan horse
- Exploit

Some lines in the Log are quite long, and therefore aren't completely visible in the window. To see more, drag the bottom-right corner of the window to make it wider, or click and drag the column headers to show more text. To sort by a column's contents click its header once; a second click toggles that column's sort between ascending (1, 2, 3) and descending (3, 2, 1) orders.

You can perform actions on some log entries by selecting them and clicking on the Action button in the log window toolbar, or by Control-clicking or right-clicking. You'll see a contextual menu that offers three options:



- **Show in Finder:** this opens a Finder window with the selected file highlighted so you can see where it is and either delete it or perform other actions on it.
- **Delete from Disk:** this option is only available for corrupted files; if you choose it will delete a corrupted file from your disk
- **Submit Suspicious File to Intego:** choose this to send any suspicious files to Intego for us to examine

You can also filter search results by entering text in the search field in the window's toolbar. As you type text, the results will narrow down, showing only those log entries that contain the text you have typed.

You can copy any log items by selecting them and pressing Command-C; you can then paste them into another application, if needed.

You can remove any log items by selecting them and pressing Delete. You can clear the entire log by clicking the Clear... button.



Using VirusBarrier X5 from the Command Line

VirusBarrier X5 also gives you the option of scanning files and volumes from the command line.

The following describes the use of this command.

```
/Library/Intego/virusbarrier.bundle/Contents/Resources/virusbarriers  
[-rtcCaz] <pathname_to_scan> [<current_directory_pathname>]
```

The following options are available:

```
-r:    Repairs infected files.  
-t:    Uses Turbo Mode; scans only those files that have not been modified  
        since the previous scan.  
-c:    Counts files before scanning.  
-C:    Counts files, but do not scan.  
-a:    Scans all files, including those symlinked to other volumes  
        (or other mount points in /Volumes)  
-z:    Scans compressed archives (including those in e-mail attachments)
```

<pathname_to_scan>: This is required; it can be a relative or absolute path.

[<current_directory_pathname>]: This is optional; it is the current working directory if a relative path is used as the first argument.

Example:

```
/Library/Intego/virusbarrier.bundle/Contents/Resources/virusbarriers  
-tacz /
```

This scans all volumes for which the user has read permission, scanning archives and counting the number of files to scan before beginning. If you run the command preceded by `sudo`, and authenticate, you can scan all files.

You can also define aliases to simplify the use of this command.

For bash:

```
alias vbscan=/Library/Intego/virusbarrier.bundle/Contents/Resources/  
virusbarriers
```

For tcsh:

```
alias vbscan /Library/Intego/virusbarrier.bundle/Contents/Resources/  
virusbarriers
```

This allows you to run the same command as follows:

```
vbscan -tacz /
```



6 –VirusBarrier X5 Settings and Preferences

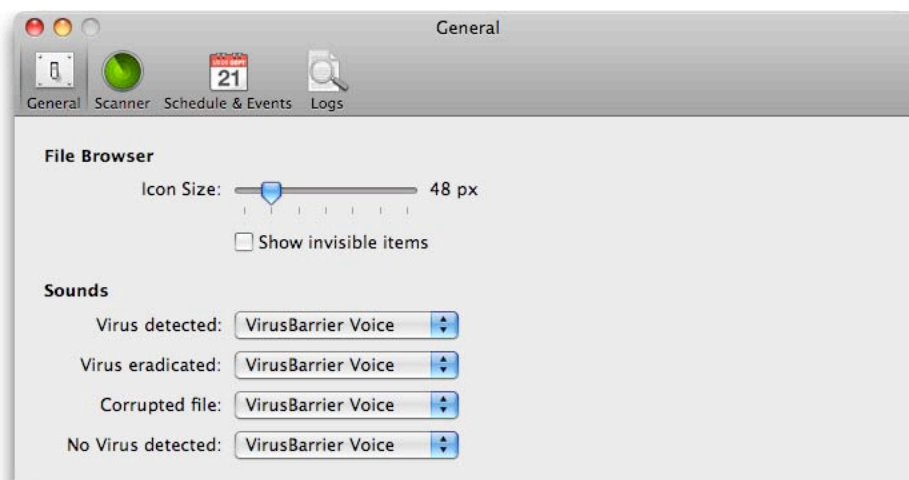


VirusBarrier X5 Preferences

VirusBarrier X5 is designed to work unobtrusively in the background once it's installed. However, it has numerous options to let you control which files it scans, how it scans them, and how you see the results when it's done. You can set the program's options in its Preferences window, which you reach either by choosing VirusBarrier X5 > Preferences... or by pressing Command-comma.

The Preferences window is divided into four panes: General, Scanner, Schedule and Events, and Logs.

General Preferences



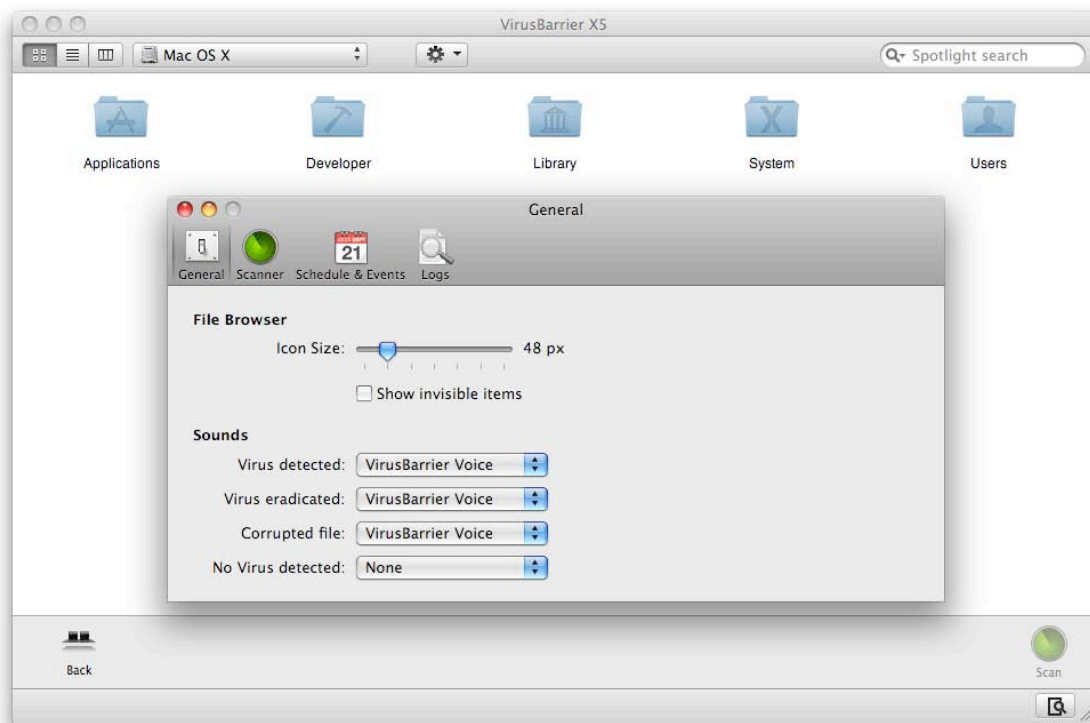
The top section of the General Preferences pane controls how the program looks to you; the bottom, how it sounds. Here's an explanation of each option.

The **Icon size** slider lets you choose how big you want icons to appear when browsing using Icon view (View > as Icons). (Changes to this setting have no effect when viewing items in the List or Column view.)

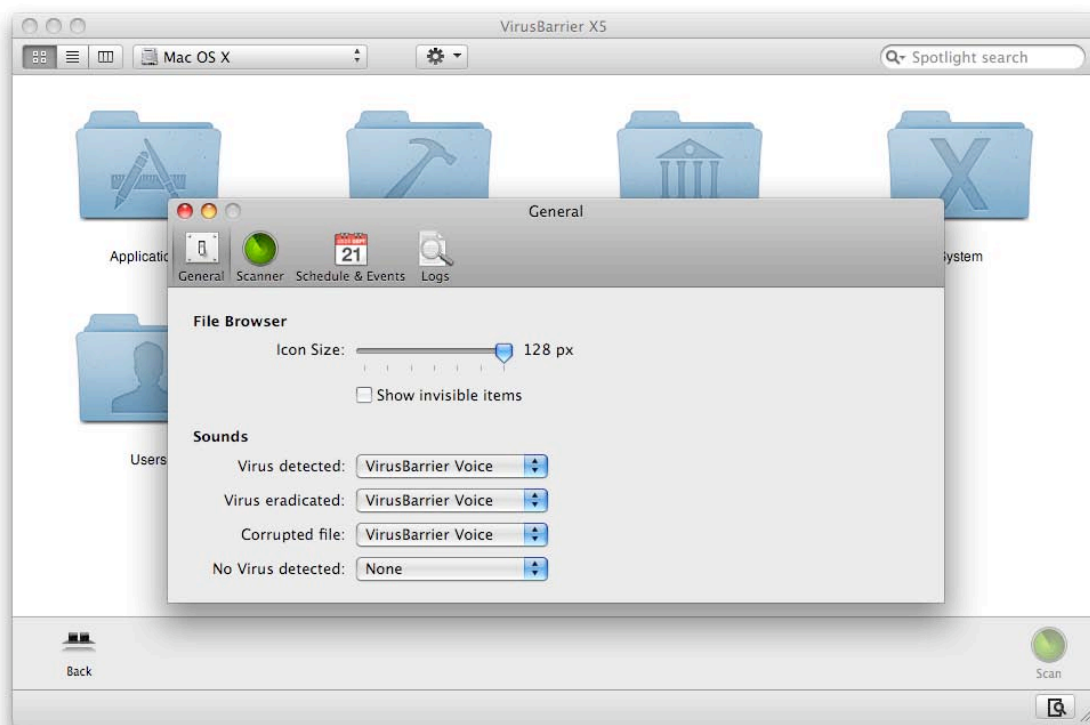


The second option, **Show invisible items**, displays files that Mac OS X usually keeps hidden. These are typically files that are needed for your Mac to function properly, and that shouldn't be changed. Viruses and other malware can hide in invisible files, so scanning them is of great importance. However, you don't need to show them to scan them: when you scan a folder, VirusBarrier X5 scans every item inside it, including invisible items.

Here is the Icon view with its default setting of 48-by-48-pixel icons and no invisible files visible:



Here's the same folder, but with larger icons and invisible items showing:

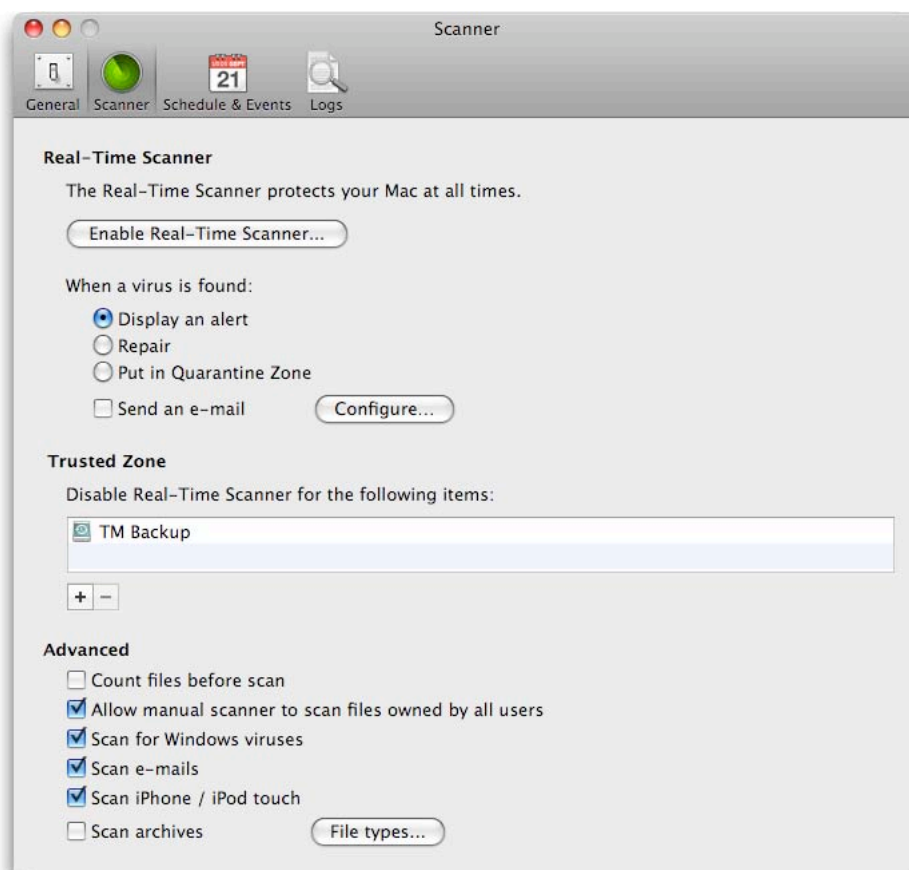


Note that the Quarantine Zone always displays invisible items regardless of the setting in these preferences.

The Sounds section lets you control what you hear when a virus is detected or eradicated (removed), when a corrupted file is found, or when VirusBarrier X5 completes a scan without finding any viruses. By default, these are set to speak their announcements: you can hear how they sound by clicking the appropriate popup menu and re-selecting “VirusBarrier Voice”. You can also change each sound by selecting any of the other sounds in that popup menu. To turn off any of the sounds entirely, select None from its popup menu.



Scanner Preferences



The Scanner preference pane controls VirusBarrier X5's behavior when it runs background scans. Because the Real-Time Scanner is so unobtrusive, VirusBarrier X5 offers several methods of notification when a virus is found.

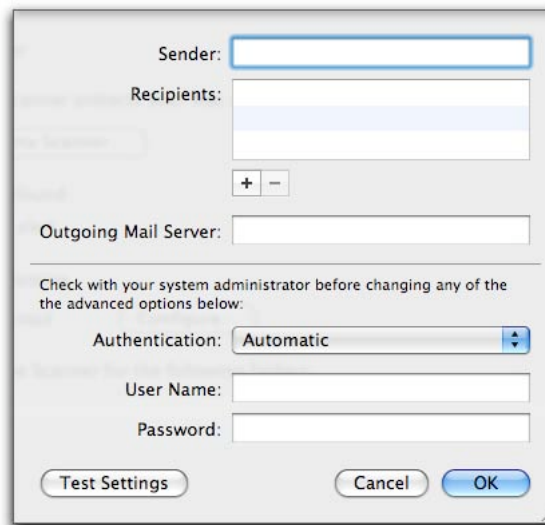
To turn on the Real-Time Scanner, click the Enable Real-Time Scanner... button; to turn it off, click the Disable Real-Time Scanner... button. In normal operation, you will not need to disable the Real-Time Scanner; this is only useful for troubleshooting when you have a problem with your Mac. Note that you can also disable or enable the Real-Time Scanner from the Intego menu, by selecting VirusBarrier X5 > Disable/Enable Real-Time Scanner.



The next control lets you indicate what VirusBarrier X5 should do when it finds a virus. Your options are:

- Display an alert. This is most appropriate when you're running a virus scan on an "attended" Mac—that is, one that you're watching closely enough to see the alert when it pops up. Note that if you don't respond to an alert within one minute, VirusBarrier X5 places infected files in the Quarantine Zone.
- Repair, which attempts to remove the virus.
- Put in quarantine, which ensures that the file cannot be opened or read. See the Quarantine Zone section in Chapter 4, "Scanning and Repairing Your Mac with VirusBarrier X5" for more about using the Quarantine Zone.

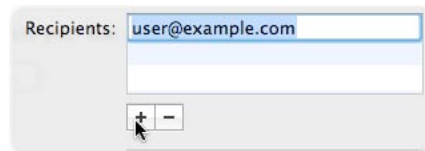
In addition, you can choose to have VirusBarrier X5 send you an email whenever it discovers a virus. To set this up, check the **Send an email...** checkbox, then click the **Configure...** button next to it.

The image shows a configuration window for email alerts. It has a light gray background and a standard Mac OS X window title bar. The fields include: 'Sender:' with a text input field; 'Recipients:' with a list box containing a dummy address and '+' and '-' buttons; 'Outgoing Mail Server:' with a text input field; a warning message 'Check with your system administrator before changing any of the the advanced options below:'; 'Authentication:' with a dropdown menu set to 'Automatic'; 'User Name:' with a text input field; and 'Password:' with a text input field. At the bottom are three buttons: 'Test Settings', 'Cancel', and 'OK'.

The e-mail addresses must be entered for the sender of the message and the recipient(s), as well as the address of the outgoing mail server. You can send this e-mail message to multiple recipients. To enter their addresses, click the + button. A dummy address will appear as shown below. Replace the dummy address by the real address of the person you wish the alert message to be sent to. To remove recipients, use the – button.

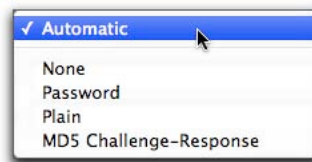


You must enter e-mail addresses for the Sender and Recipient(s), as well as the Outgoing Mail Server. Further, you'll need to enter a username and password that your mail server will accept. E-mail messages can be sent to multiple recipients. To add a recipient, click the + button. To remove a recipient, click the – button.



The lower half of the Mail Settings dialog deals with advanced options that VirusBarrier X5 may require to send e-mail.

The drop-down menu shows the various types of e-mail authentication handled, as shown below.



You should use the same Authentication, User Name and Password as you use in your usual e-mail program, if you administer your own system. If on the other hand, you have a system administrator, you should check with this person to see what settings should be used here. If you don't know which type of authentication you use, select Automatic.

When you're done, you can confirm that the email will go through by clicking the Test Settings button. You may have to wait several seconds for your mail server to respond; when finished, a dialog box appears with the test's results.

The next section of the Scanner Preferences window allows you to exclude files, folders, and volumes from real-time scans by adding them to the Trusted Zone. (See the Trusted Zone section in Chapter 4, "Scanning and Repairing Your Mac with VirusBarrier X5" for more on using this feature.)



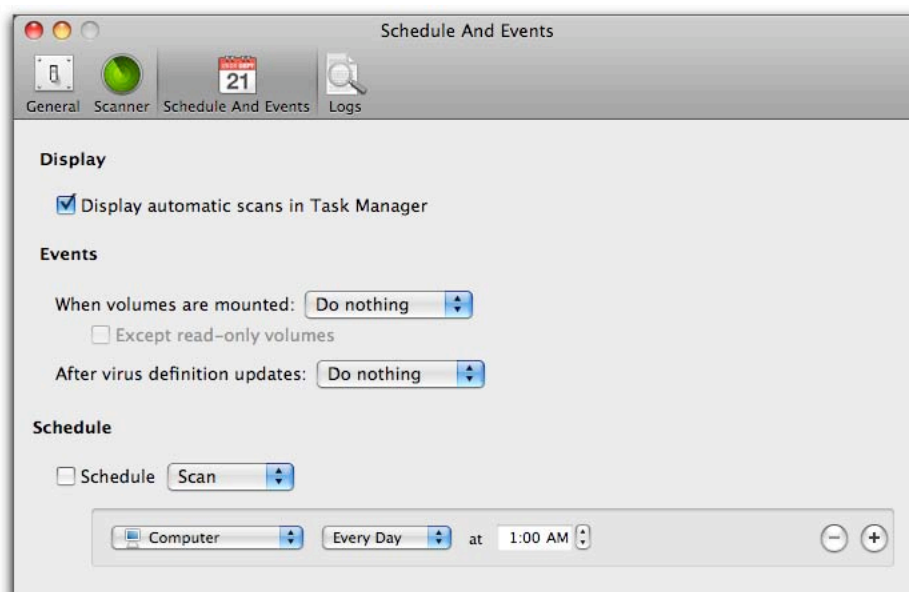
The very bottom of the Scanner Preferences pane provides access to six Advanced settings, which affect both automatic and manual scans:

- The **Count files before scan** option makes VirusBarrier X5 count how many files are to be scanned, thereby giving more accurate information on how long a scan is going to take by displaying a number of files and a percentage in the Orb during a manual scan.
- **Allow manual scan to scan files owned by all users** allows VirusBarrier X5 to reach beyond the user account that's logged in at the time the scan begins, to scan files on your Mac, including those belonging to other users. If you select this option, you'll immediately be required to enter an administrator password; if you don't have that password, the checkbox will revert to its unchecked state. If you don't check this option and VirusBarrier X5 finds an infected file owned by a different user or by the system, VirusBarrier X5's alert and Quarantine Zone window will display a crossed-out pencil icon, signifying that you will need to enter an administrator's user name and password to perform any action on the file.
- **Scan for Windows viruses** tells VirusBarrier X5 to watch for viruses that affect Windows. Although these files generally can't damage your Mac, you could pass them on to your Windows-using friends, and they could affect you if you use Windows on your Apple computer through a program such as Apple Boot Camp, VMware Fusion or Parallels Desktop.
- **Scan e-mails.** VirusBarrier X5 scans both incoming and outgoing e-mails, both for their content and any attachments they contain.
- **Scan iPhone / iPod touch** tells VirusBarrier X5 to scan any iPhone or iPod touch that is connected to your Mac when you run a scan. If this option is unchecked, VirusBarrier X5 will not show any iPhone or iPod touch in its browser or in its shelf.
- **Scan archives.** Archives contain one or more files, usually in a compressed format, so that they can be transferred easily and quickly. By selecting this checkbox, VirusBarrier X5 will look inside several popular formats of archive, scanning not only the archive file itself, but also the uncompressed files that it contains. By default, VirusBarrier X5 will scan all archive types that it understands; however, you could choose to scan only certain archive types by clicking the File types... button. A window will appear where you can select and unselect archive types according to your preference.



Schedule and Events Preferences

The Schedule and Events Preferences pane is divided into three areas: Display, Events, and Schedule.



The Display section has only one checkbox: **Display automatic scans in Task Manager**. When checked, you'll see a small window appear whenever your Mac executes scheduled scans; when unchecked, such scans will pass without notification (unless a virus is found).

The Events section lets you direct VirusBarrier X5 to automatically run a scan, do repairs, or do nothing when certain events occur.

The first, **When volumes are mounted:**, is triggered whenever you connect to a new storage device, whether local (such as a hard drive) or remote (such as a network drive). If the **Except read-only volumes** checkbox is checked, VirusBarrier X5 will perform the action only on those volumes where it could change the drive being scanned (for example, to repair a disk that contains a virus).

The second event, **After virus definition updates:**, lets you tell VirusBarrier X5 what to do after NetUpdate downloads and installs new virus definitions. Virus definitions are updated regularly,

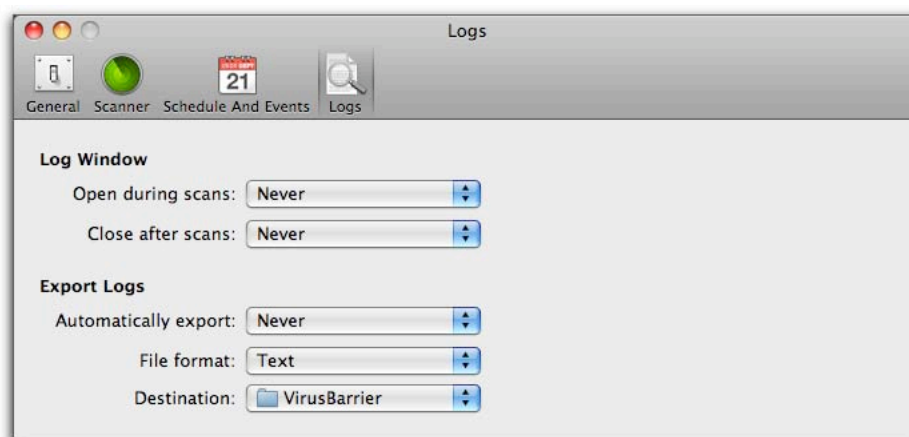


and especially when a new virus is discovered to offer protection against that virus. Therefore, you should perform a new scan at those times to check for the new virus, whether manually or (by checking this checkbox) automatically.

The **Schedule** section lets you determine when VirusBarrier X5 will run automated scans. For details on setting these schedules, see the “Scheduled Scanning” section in Chapter 4, “**Scanning and Repairing Your Mac with VirusBarrier X5**.”



Logs Preferences



The Logs preference pane has two sections, one controlling whether the behavior of the log window itself, the other telling VirusBarrier X5 whether to create automated exports of scan logs.

The Log Window section has two popup menus telling whether the window should **Open during scans** and **Close after scans**. Each popup menu has three options: Never, Always, and If a Virus is Found / If no Virus is Found. By default the Log window will remain closed during scans but you could (for example) set it to open for every scan, and remain open when it's done only if VirusBarrier X5 discovers a virus.

The Export Logs section of the pane features three popup menus:

- The **Automatically Export** menu has four options: Never, Every Day, Every Week, and Every Month.
- The **File Format** menu has three options. Text creates a log file with no styling or markup codes; HTML creates one in styled text that can be read easily in a web browser; XML creates a data file that's in a format designed for easy integration with other applications that use the XML format.
- The **Destination...** menu by default puts all log files in the folder at /Library/Logs/VirusBarrier. However, you can change that location by choosing Other... navigating to the folder you want through the file browser, and clicking Choose.



Locking and Unlocking Preferences

VirusBarrier X5 gives you a way to lock the program's preferences so that even those who have physical access to your Mac won't be able to change its settings. To lock VirusBarrier X5's preferences, either press Command-L, or choose File > Lock Preferences. To unlock the preferences, press Command-L or choose File > Unlock Interface, then enter your administrator's password to complete the process.



About Intego VirusBarrier X5



To get information about your copy of VirusBarrier X5, choose VirusBarrier X5 > About VirusBarrier X5. It gives information about Intego VirusBarrier X5, such as the version number, your support number (a number you will need for technical support), and a clickable link to send email to Intego's support department. .



7 - Technical support



Help Menu

The complete VirusBarrier X5 user's manual is available via the Help menu in VirusBarrier X5. You may find the answer you need in the manual, before resorting to contacting Intego for Technical Support.

Technical Support

Technical support is available for registered purchasers of VirusBarrier X5. Do not forget to quote your precise build number, which you can display by clicking on the Version number just above the VirusBarrier X5 icon in the About VirusBarrier X5 window. To display this window, open VirusBarrier X5 and choose About VirusBarrier X5 in the VirusBarrier X5 menu.

By e-mail

support@intego.com: North and South America

eurosupport@intego.com: Europe, Middle East, Africa

supportfr@intego.com: France

supportjp@intego.com: Japan

From the Intego web site

www.intego.com

To send files to the Intego Virus Monitoring Center, contact sample@virusbarrier.com.

Alternatively you can highlight them in the Finder, Control-Click on them to display a contextual menu. Choose More, then VirusBarrier X5, then Send Suspicious File to Intego. You can send files, folders or applications to Intego in this manner, without your even having to open your e-mail program.



8 - Glossary



Glossary

Antivirus	A program that protects your computer from viruses by scanning, disinfecting and repairing infected files. It looks for bits of code that make up the virus's "signature", in certain places in files and applications.
Archive	A file that contains several files, and is usually compressed, to save space.
Boot	To start up a computer. It comes from the word bootstrap, as in "pulling yourself up by your bootstraps".
Code	Computer programs are written in code, or programming languages. Viruses, since they too are computer programs, are also written in code.
Infect	If a file is infected, this means that a virus has copied itself onto the file. This may be a macro, copied onto a word processor file, or other types of code, copied onto an application.
Macro	A short program that uses the built-in functions of a given application's macro language. Many applications have macro functions, designed to let you carry out repetitive functions more easily. Unfortunately, macros also can do damage to your system, and there are many macro viruses in the wild, especially those that run under Microsoft Word or Excel.
Macro Command	A small programming command that is accessible in a macro. It uses a macro language that is specific to a given application.
Macro Virus	A virus that takes advantage of an application's built-in macro language. Macro viruses are currently the most dangerous viruses for Macintosh users, especially those that run under Microsoft Word or Excel, since they can be transmitted from Macintosh computers to Windows computers.



Partition	A partition, or volume, is a logical part of a hard disk. It is possible to create many partitions on a hard disk, each of which functions as if it were a smaller hard drive. The operating system sees partitions as separate volumes.
Removable Media	Any data storage media that is inserted into a drive, such as a CD-ROM or DVD.
Strain	A variation or mutation of a certain virus. Just as this term is used in medicine, for mutations of bio-viruses, it is also used for computer viruses, which can, in some cases, mutate, creating new strains.
Trojan Horse	A Trojan horse, or Trojan for short, is a program that hides malicious code. It is not really a virus, since it does not reproduce, but it may contain viral code, which, when the Trojan is run, will copy itself into other files. The name Trojan Horse comes from the huge, hollow wooden horse that the Greeks built and gave to the Trojans, apparently as a gift. The horse was taken inside their stronghold, and, later that night, Greek warriors emerged from the horse, opened the city gates, and Greek soldiers from outside stormed the city.
Virus	<p>A computer program or a bit of computer code capable of reproducing and propagating. Most viruses are malicious, and infect files by attaching to them.</p> <p>They then use these host files to spread when the files are open or run.</p>
Volume	A volume is, in essence, a hard drive, or other removable media unit. It can be an entire hard disk, a partition on a hard disk, a remote computer on a network, or a floppy disk. What is special about a volume is that it contains its own directory files indicating where, on the volume, files are stored.
Worm	A worm is a program that propagates itself over a network, reproducing itself as it goes. While most people tend to consider that a worm is just a kind of virus, since worms can be capable of malicious activities, they do not function the same way. Worms do not need host files to reproduce.

