User's Manual

Intego VirusBarrier X4 for Macintosh

Intego

www.intego.com

Contents

1- About Intego VirusBarrier X4

What is Intego VirusBarrier X4?

Intego VirusBarrier X4 is the simple, fast and non-intrusive antivirus security solution for Macintosh computers, by Intego, the leading publisher of personal security software for Macintosh. It offers thorough protection against viruses of all types, coming from infected files or applications, whether on CD-ROMs, DVDs or other removable media, or on files downloaded over the Internet or other types of networks.

Intego VirusBarrier X4 protects your computer 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 Intego VirusBarrier X4 on your computer, you can rest assured that your Macintosh has the best protection available against viruses of all kinds.

Intego VirusBarrier X4 is an application that works in the background and checks everything that your computer does, looking for viruses. It knows the unique signatures of all known Macintosh viruses, and whenever a new virus is discovered, Intego's antivirus SWAT team goes into action to provide updated virus definitions, which you can only download using Intego VirusBarrier X4's automatic NetUpdate function.

When you purchase Intego VirusBarrier X4, you have access to virus definition updates for one year from the date of purchase. 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.

Intego VirusBarrier X4 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 Intego VirusBarrier X4 philosophy can be summed up in three words: **simple**, **fast** and **non-intrusive**.

Simple

Intego VirusBarrier X4 is the easiest to use antivirus program. After you install it, it works in the background, keeping a close eye on your computer, and verifies your files silently and efficiently.

Fast

Intego VirusBarrier X4 is fast and efficient. It does not slow down your computer, and you don't need to do anything while it works. Each time a file is created, opened or closed, Intego VirusBarrier X4 checks the file to make sure it is safe.

Non-intrusive

Intego VirusBarrier X4 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 is there, unless it detects a virus and alerts you. In addition, you do not need to deactivate Intego VirusBarrier X4 when installing new software, regardless of what the program's installer or manual may say. Intego VirusBarrier X4 can run all the time, in the background, protecting your computer without you needing to worry about it.

Intego VirusBarrier X4 is compatible with Mac OS X 10.2.8 or higher (Jaguar, Panther and Tiger).

Intego VirusBarrier X4's Features

Virus Scanning

Intego VirusBarrier X4 works in several ways. While it is constantly watching over your computer at all times, protecting you from any viruses, it can also work in manual mode, and you can ask it to scan any disk, or volume on a network.

Automatic Repairs

If Intego VirusBarrier X4 is running in automatic mode, it will repair any infected files it finds by eliminating the viruses, if possible, or, if not, indicating that the files are damaged. In this mode, you can just forget about Intego VirusBarrier X4's activity—you will only know it is there if it comes across any viruses or suspicious files. Intego VirusBarrier X4 also repairs any files dragged and dropped onto the icon or the program interface.

Manual Scan

You can also use Intego VirusBarrier X4 to manually scan your files. This is recommended the first time the program is installed, to make sure that your computer is safe. You can then use it at any time to manually scan any disks or volumes to ensure that they are virus-free. You can also scan individual files by dragging and dropping on the program icon or on its interface when it is running in the foreground. It is recommended to run a manual scan of your files each time you install new virus definition updates.

Turbo Mode

Turbo mode makes scanning much faster. The first time Intego VirusBarrier X4 scans your computer, it remembers all the files it examines. As long as these files are not updated, Intego VirusBarrier X4 will not rescan them, scanning from 5 to 40 times faster.

Scan Logs

Intego VirusBarrier X4 displays complete logs 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.

Dock

If you choose to keep Intego VirusBarrier X4 in the Dock, you can check files or folders for viruses without even opening the application, just by dragging them on the Intego VirusBarrier X4 icon.

NetUpdate X4

Intego VirusBarrier X4 features Intego's NetUpdate X4 program, which allows you to check for program updates or new virus definitions automatically. You can set the update frequency in NetUpdate X4 itself, so the program checks on a given day at a given time, every week. Current update status can even be checked at any time using the special NetUpdate X4 widget that is included with Intego VirusBarrier X4.

Virus Alerts

Intego VirusBarrier X4 allows you to set alert options so you can know if the program detects any viruses, while working in the background. You can choose to have the program display an alert screen, play a warning sound, or even send an e-mail message to a specific address. This can be useful if you want to run Intego VirusBarrier X4 on computers connected to a network, and to warn a network administrator or the computer's owner when they are away from their computer.

Secure Zone

Intego VirusBarrier X4 offers a zone you can specify where files will remain secure. This is a volume or folder that will be checked automatically for viruses as soon as anything changes in it. In addition, VirusBarrier X4 alerts you as soon as a file has been modified, guaranteeing the security of your data. This is particularly useful for users who have files or folders that are updated continually or automatically, such as shared folders, download folders or drop boxes.

Unsecured Zone

Intego VirusBarrier X4 offers the option to set an Unsecured Zone. This is an area that will not be scanned by VirusBarrier X4. This zone should only be used for safe files that have already been scanned by VirusBarrier X4.

Using this User’s Manual

This user's manual provides detailed information on installing, using and updating Intego VirusBarrier X4, 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 Installation instructions (chapter 3). Next, you should read the description of Intego VirusBarrier X4's features (chapter 5), and, if you want to know more about viruses, you can consult the Glossary (chapter 9).

If you are having problems with your computer, and you think you may have a virus, you should read the Diagnosis section (chapter 7), for instructions on troubleshooting your computer and determining whether you do, indeed, have a virus. If so, you will be instructed how to send any files that you think might be infected to Intego's Virus Monitoring Center so we can inspect them.

2 - Introduction to Computer Viruses

Why You Need to be Protected

You know very well that your computer 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 use your computer just 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.

An antivirus program is a kind of insurance policy. Of course, you imagine that this will never happen to you, but if it did, you would be very unhappy. Intego VirusBarrier X4 is your insurance against all kinds of viruses, watching over your computer so you don't have to worry about it.

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 computer 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. Their reaction can be seen as that of someone who has learned that they, too, had caught the disease. 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 with people exchanging many files on a daily basis. 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 over the Internet. Like 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.

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 X4, and, above all, make sure you keep the program and its virus definitions up to date.

Who Writes Viruses?

No one is really sure who writes viruses—angry teenagers, skillful hackers, who knows? Some virus writers are arrested, but this is only the tip of the iceberg. The ones that are caught may actually want the attention they get from their viruses—many viruses have been found with the author's name in them. Others are simply vandals, who get pleasure from seeing the havoc they can cause with their relatively simple programming. And still others are people who want to experiment, to see just how far their viruses can go in the wild, how many people's computers will catch them. Or, are viruses simply, as one virus writer has said, "the electronic form of graffiti"?

There are even cases of viruses that had no "bad intentions", but, nevertheless, ended up causing many problems. One example of this is the MacMag virus, which tried to spread a message of world peace. See chapter 9 for a description of this virus.

Since the rise of the Internet, the real fear concerning viruses is no longer that one isolated individual might try and spread a virus just for attention, but that truly malicious people might use viruses to do economic damage on a large scale. Virus outbreaks have shown just how much it can cost, in lost productivity and downtime, for a company to suffer a virus attack. If only for this reason, you should protect yourself in every way possible.

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 DOS and Windows computers have no effect on Macintosh computers, and vice versa. (Although, if you are running one of these operating systems in an emulator on your Macintosh, you will have to consider the vulnerability of the emulated system to any viruses that may target it.)

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 customer, 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, say, an animated greeting card. You double-click the file, and the application starts running. While it is running, however, it sets off its viral code and alters your System file. It copies malicious code into your System, and, at the same time, searches your company's local network for other System files, and copies itself there as well. 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 X4, you are also protecting others as well.

Everyone has heard of harmful viruses that have traveled around the world in less than 24 hours. While these high-profile viruses affected Windows computers, there is no reason why similar viruses could not target Macintosh computers.

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 the System file, extensions, or the Desktop file. The second type, file viruses, infect applications, data files, or even control panels and extensions.

System Viruses

System viruses are the most dangerous of all, since they can damage the operating system itself. We are also including, in this section, two other types of malware: Trojan horses and worms. While not technically the same as system viruses, they tend to act more globally than file viruses.

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.

Some of these viruses, such as the CDEF or WDEF viruses, only infect the Macintosh's Desktop files on versions of Mac OS 9 and earlier. These are invisible files that keep track of which icons go with which types of files and applications. These viruses, which do not affect other files, spread extremely quickly, since the first thing your Macintosh does when mounting a disk or volume is read its desktop files.

Other system viruses, such as versions of the SevenDust virus, can infect System files, control panels and applications, and at a certain time, on a certain date, delete all non-application files on your startup disk.

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.

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. Some examples are ChinaTalk, which looks like a system extension but deletes folders, or the famous MacMag Trojan, which infected System files.

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. One of the most serious worms on the Macintosh, called the AutoStart worm, created invisible files that could destroy data and files.

Worms use system functions to spread—the AutoStart worm spread from infected CD-ROMs using the Autoplay function of an earlier version of Mac OS. It created invisible extensions that activated each time the computer was restarted.

File Viruses

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. Examples of file viruses, that all targeted Windows computers, were the very damaging Melissa and LoveBug viruses. These viruses came in attachments, which, when opened, activated certain functions built in to Microsoft applications under Windows. In a way you could think that these were Trojan horses, but the difference is that a Trojan horse is an application that purports to do a certain task, whereas these file viruses were actually code embedded into files.

Macro Viruses

In general, file viruses are macro viruses. This family of viruses poses the greatest threat for Macintosh users today.

The first real macro virus that was found in the wild was the Concept virus, which attacked Microsoft Word files. This was quickly followed by other variants, as virus writers saw the potential to do great damage through the ubiquity of this program. Later, macro viruses were written to exploit Microsoft Excel as well. Several thousand macro viruses have been found.

The real danger of macro viruses is the fact that they are the first cross-platform viruses. For years, Macintosh users could be relatively secure from viruses, knowing that there only a few dozen viruses targeted Macintosh computers, compared to thousands for Windows. But now that macro viruses are prevalent, the danger is present.

Many programs provide the ability to create macro commands. These simple programs use either the internal functions of an application 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 base their macro functions on Visual Basic, which is similar to the Basic programming language.

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.

Most macro viruses that target Microsoft Word files use commands such as AutoOpen, AutoClose, AutoExec and AutoExit. These are commands that are executed when a certain event occurs to the file, and these four events always occur when you work with a file. If, for example, a macro were written to copy itself only when you choose a certain menu command, it would be far less certain of spreading.

The most common action for macro viruses is to act when a file opens, and, first, copy itself into the template that is opened as well. You don't physically open this template, but it is always open in the background—it contains certain customization information, such as toolbars, as well as any legitimate macros you may have added to it.

The most common macro virus that affects Microsoft Word copies itself into the active template, changes some menu items so you cannot edit the template, changes file types (which changes their icons, making them look like templates themselves), then copies itself from the corrupted template into all new files you create or open. This virus can be removed, if caught in time, by removing the active template file and any infected files.

Other macro viruses can be much more dangerous. They can corrupt or delete your 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 Macintosh computers and PCs running Windows.

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 includes 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.

Intego VirusBarrier X4 detects all known Word and Excel macro viruses, and is updated when new macro viruses are found.

Hoaxes

Hoaxes, that is, e-mail messages or newsgroup posts warning people about non-existent computer viruses, are a growing problem. While they are not viruses themselves, they do tend to reproduce in a similar way—worried users forward these messages to their friends and co-workers, thinking they are true, thus making them worry unduly about some imaginary virus.

One of the most widespread hoaxes was called Good Times. This took its name from the subject of an e-mail message that was supposed to contain a virus. You might think that if it were clearly such a hoax it would have not lasted very long, yet the Good Times "virus" message was still seen many years after its first appearance in 1994. Other copycat hoax messages are regularly circulated around the Internet as well, and you have probably already seen at least one, if not more.

These hoaxes capitalize on the lack of computer knowledge of Internet users. It is true that they always sound serious, and sometimes seem to be forwarded from major computer companies. Yet they are all jokes, although not very funny ones.

If you receive a message like this, and you are worried that it might not be a hoax but a real virus alert, the first thing you should do, if you work in a company, is contact your system administrator to find out if it is real. If you are a home user, you can always check the Intego web site at www.intego.com. If there are any new viruses around that you need to worry about, we will post information on our web site as soon as possible. Intego's Virus Monitoring Center is ready 24 hours a day, 7 days a week, and will react on the first signs of any new viruses.

If you think you have caught a new virus, see chapter 7, Diagnosis, for instructions on how to diagnose your computer, and how to contact Intego's Virus Monitoring Center.

How do Viruses Spread?

Viruses can spread in a few basic ways. They can only spread through two things: files or removable media. Media, such as CD-ROMs, DVDs, etc., for the Macintosh, contain invisible files called Desktop files. These files contain information for the System concerning file icons and applications. Viruses that infect Desktop files can spread when your computer reads these removable media, since the first thing your Macintosh does when mounting a disk or volume is read its desktop files. Intego VirusBarrier X4 protects your computer from these viruses by scanning all desktop files in removable media, before viruses have a chance to spread. If Intego VirusBarrier X4 detects a virus in these Desktop files, it will disinfect them before your computer reads the files.

Viruses can also spread through infected files. These files may be on CD-ROMs, 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. The same goes for data files—if you happen to receive a file with a macro virus, there is nothing to worry about as long as you don't open the file. Intego VirusBarrier X4 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 Intego VirusBarrier X4 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 Intego VirusBarrier X4 to constantly monitor your computer and automatically check for viruses. Intego VirusBarrier X4 provides the best protection for your Macintosh, and works in the background, to ensure that your computer remains safe.

To ensure that Intego VirusBarrier X4 is always watching out for all known viruses, you must update the program regularly. Intego VirusBarrier X4's NetUpdate function makes this easy to do, even automatic, if you choose. You should check for updates at least once a month, and you can even check the Intego web site (www.intego.com) from time to time to see if there are any new viruses that require a more immediate update.

Another very important point is that 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. Intego VirusBarrier X4 protects you by checking each file as you install software, making sure that they are safe.

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 recent viruses on Windows computers have spread because the virus was in attachments that came from friends and co-workers. In any case, if you get an attachment from someone you don't know, you are best not opening it. But this does not ensure that your colleagues are unwittingly spreading viruses in their files. Intego VirusBarrier

X4 protects you by scanning every file as you open it, and eliminating all known viruses automatically. If you are on a network, and Intego VirusBarrier X4 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 Intego VirusBarrier X4, 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 X4 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 CD-ROMs, 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 computer, you will be able to do this in just a few minutes.

3 - Installation

System Requirements

- Any officially-supported Mac OS X compatible computer
- Mac OS X or Mac OS X Server, 10.2.8 or higher (Jaguar, Panther and Tiger)
- 40 MB free hard disk space
- Minimum screen resolution 800 x 600

Note: Certain features of Intego VirusBarrier X4 are only available under Mac OS X 10.4 Tiger.

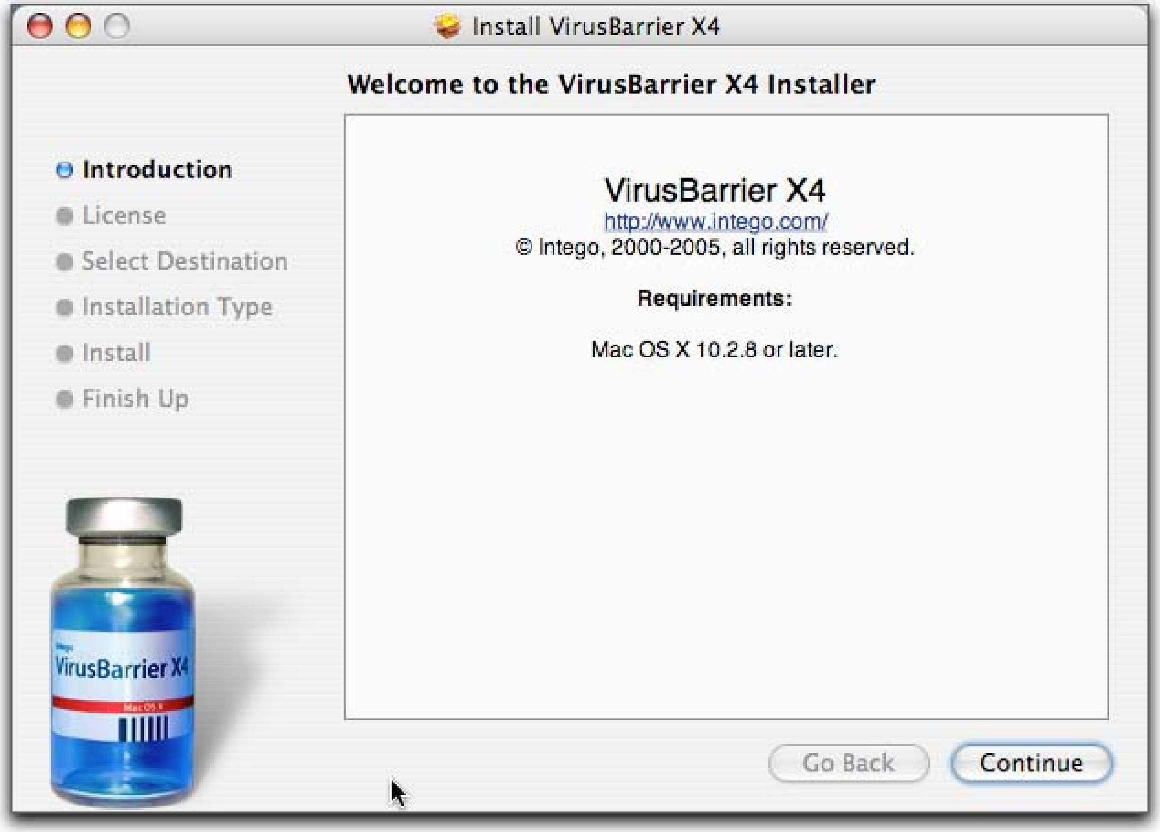
Installing Intego VirusBarrier X4

Installing Intego VirusBarrier X4 is very simple.

If you downloaded the VirusBarrier X4 installer from the Internet, locate the disk image file that you downloaded. Double-click the folder corresponding to the language version that you want to install. Then double-click the VirusBarrier X4 install file.

Insert the Intego installer CD in your computer. A window will open advising you to be sure a serial number. Click OK. A window will now open showing several different Intego software programs. Select Install in the ViursBarrier X4 dropdown list. A green arrow will then display on the VirusBarrier X4 icon, indicating that you have chosen to install this software. Click the Launch Installation… button.

You will see a window displayed informing you that you must enter an administrator's password to install Intego VirusBarrier X4. Enter your password in the dialogue that is displayed. Enter your password, and then click OK. The following window will be displayed:



Install VirusBarrier X4

Welcome to the VirusBarrier X4 Installer

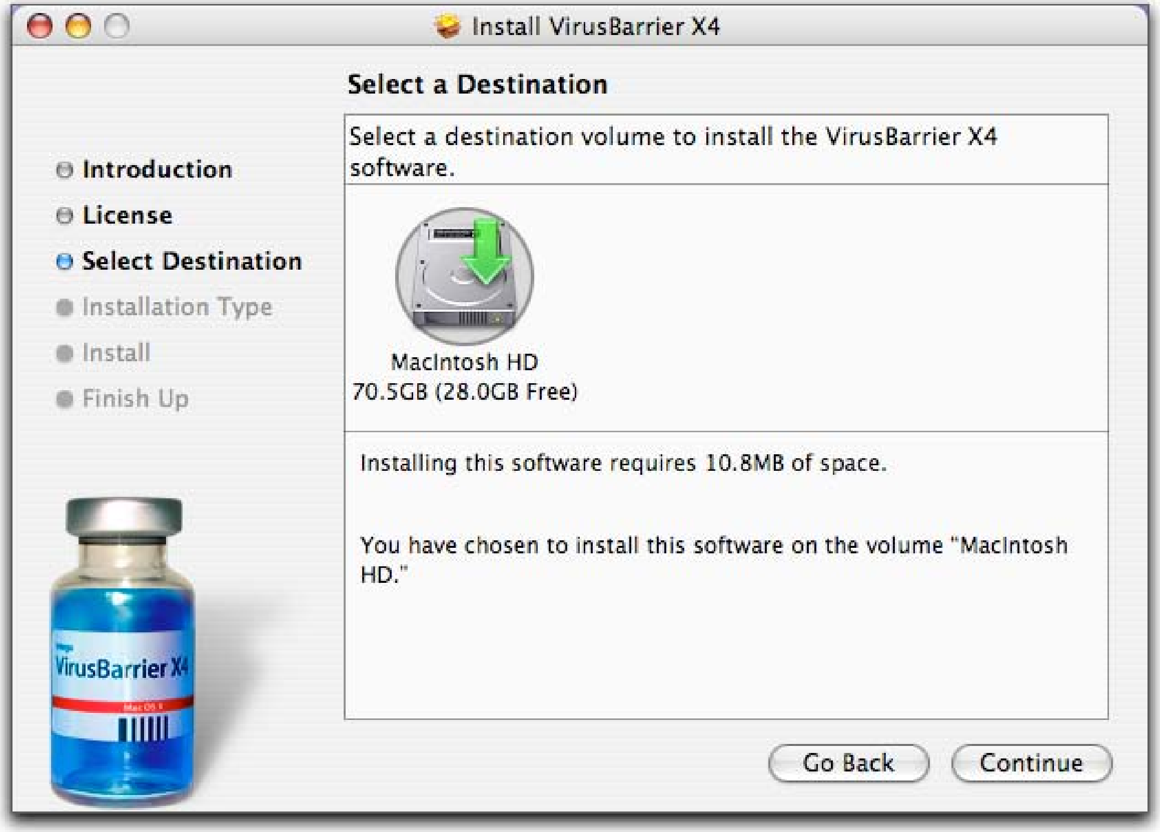
VirusBarrier X4
http://www.intego.com/
© Intego, 2000-2005, all rights reserved.

Requirements:

Mac OS X 10.2.8 or later.

To install Intego VirusBarrier X4, click Continue. You will then be asked to agree to the Software License Agreement, as for all software. You can print or save this information before proceeding if you wish. However, you must agree with the License in order to install the software.

You will then see a window asking you to select a destination disk for the software, as below. Disks on which the software cannot be installed (because they have no Operating System, for example) will be shown with a red exclamation point (!), and the selected disk will be marked with a green arrow.



Install VirusBarrier X4

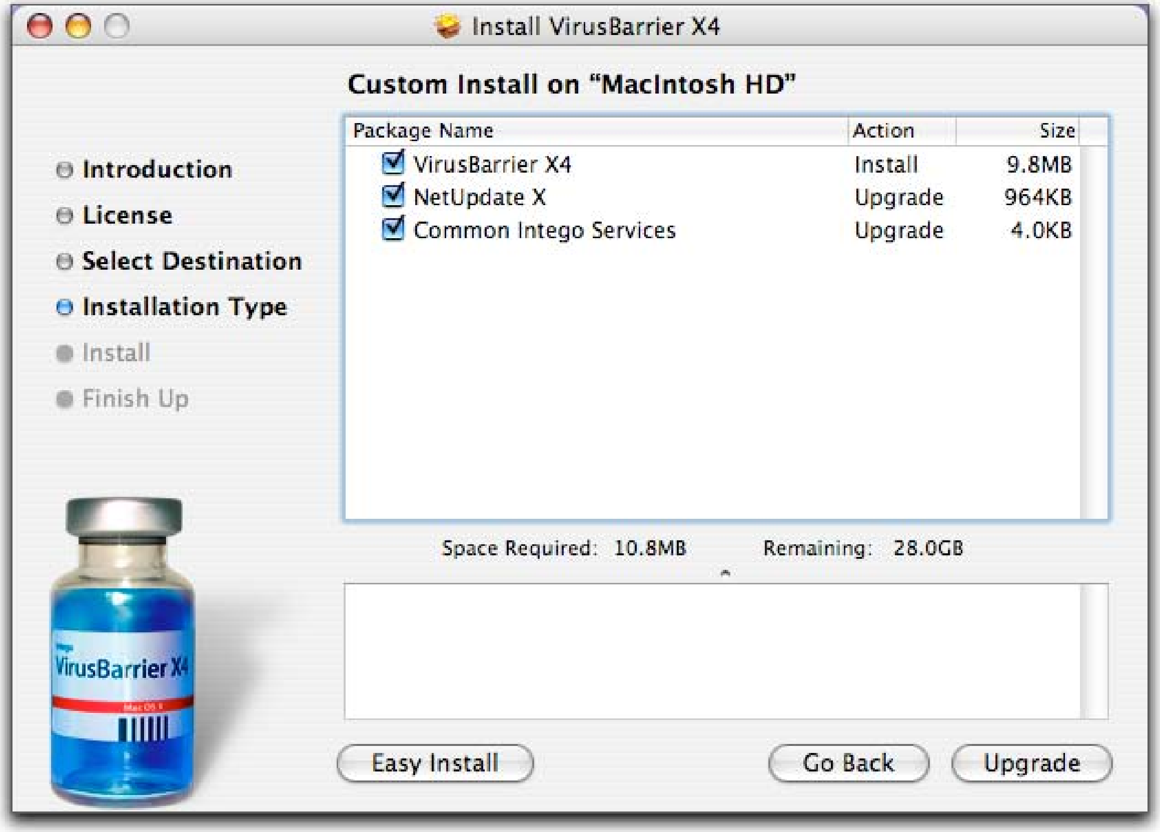
Select a Destination

Select a destination volume to install the VirusBarrier X4 software.

Installing this software requires 10.8MB of space.

You have chosen to install this software on the volume "MacIntosh HD."

At this point you will see a window asking you if you want to install the software (or upgrade it, if you own a previous version). Click Install to install Intego VirusBarrier X4. This will perform a basic installation. If you wish to perform a custom installation, click Customize. The following window will be displayed:



Custom Install on "MacIntosh HD"

Package Name	Action	Size
☑ VirusBarrier X4	Install	9.8MB
☑ NetUpdate X	Upgrade	964KB
☑ Common Intego Services	Upgrade	4.0KB

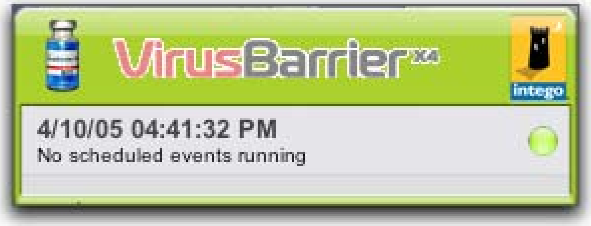
Space Required: 10.8MB   Remaining: 28.0GB

This window lets you choose which items will be installed, or return to the previous screen by clicking the Easy Install button, which means that all the components will be installed. Alternatively, you can click on the Upgrade button directly from this window to proceed to the next step in the installation process.

You will see a window displayed informing you that you must enter an administrator's password to install Intego VirusBarrier X4. Enter your password in the dialogue that is displayed, and then click OK.

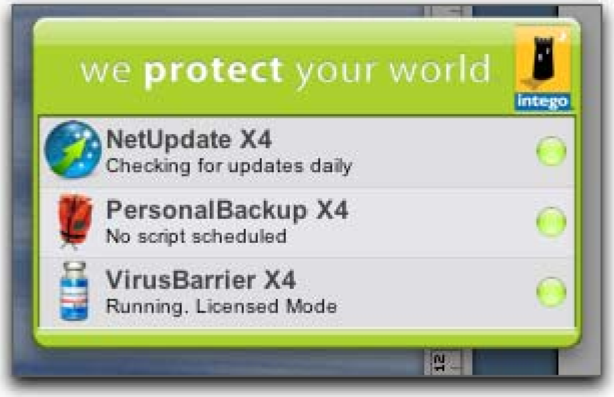
After installation, you will have to restart your computer.

Intego VirusBarrier X4 also installs a widget that loads into the Mac OS X dashboard (Mac OS X 10.4 Tiger and higher only) to display the status of Intego VirusBarrier X4 scheduling at any time. This widget looks like this:



4/10/05 04:41:32 PM
No scheduled events running

There is a further Intego widget installed to show the status of all other Intego software that might be running concurrently, such as Intego Personal Backup X4.

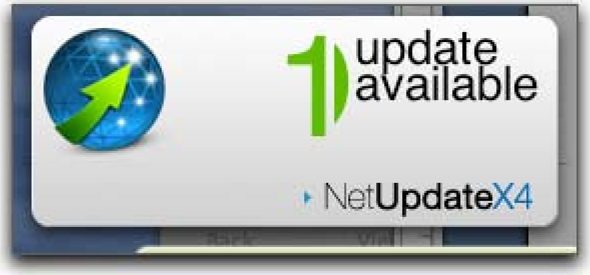


NetUpdate X4
Checking for updates daily

PersonalBackup X4
No script scheduled

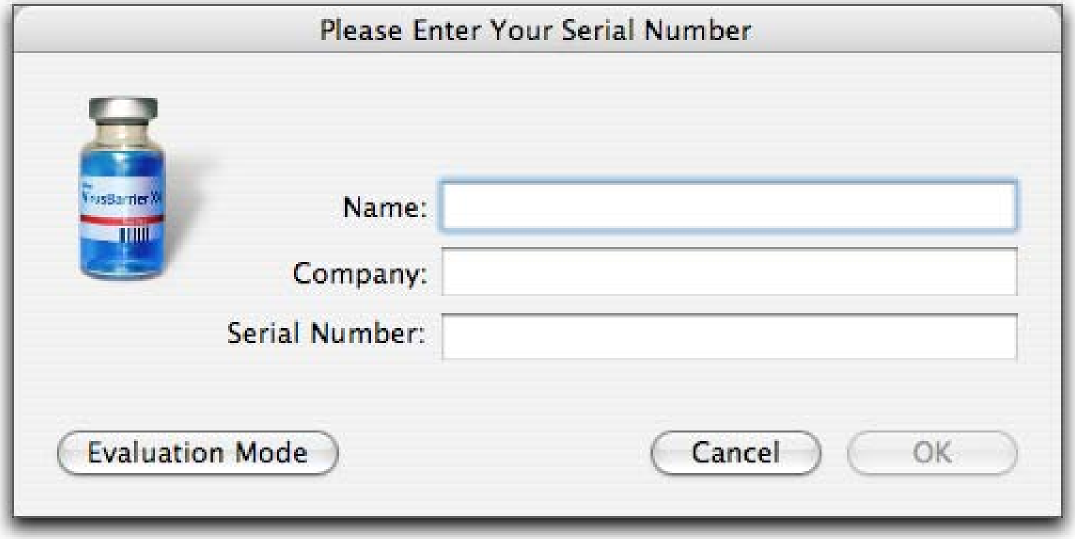
VirusBarrier X4
Running, Licensed Mode

Finally, Intego VirusBarrier X4 also installs the Intego NetUpdate widget to so you can easily check if any updates are currently available. It looks something like this:



Serializing Intego VirusBarrier X4

When you restart your computer, open Intego VirusBarrier X4 - it is located in your Applications folder, unless you have moved it elsewhere. Intego VirusBarrier X4 will open and display the following window:



Please Enter Your Serial Number

Name:

Company:

Serial Number:

Since Mac OS X is a multi-user operating system, not all users have the same privileges. When starting up Intego VirusBarrier X4 for the first time, any user can enter the serial number, but only a user with administrator privileges can configure the program.

You must enter your name, company, if any, and your serial number. The serial number is found on a sticker either in the DVD case or on the envelope containing the CD. If you have downloaded Intego VirusBarrier X4, the serial number will be sent to you in your order confirmation e-mail. When registration is completed, Intego VirusBarrier X4 will open, and, if you are an administrator, you can configure the program.

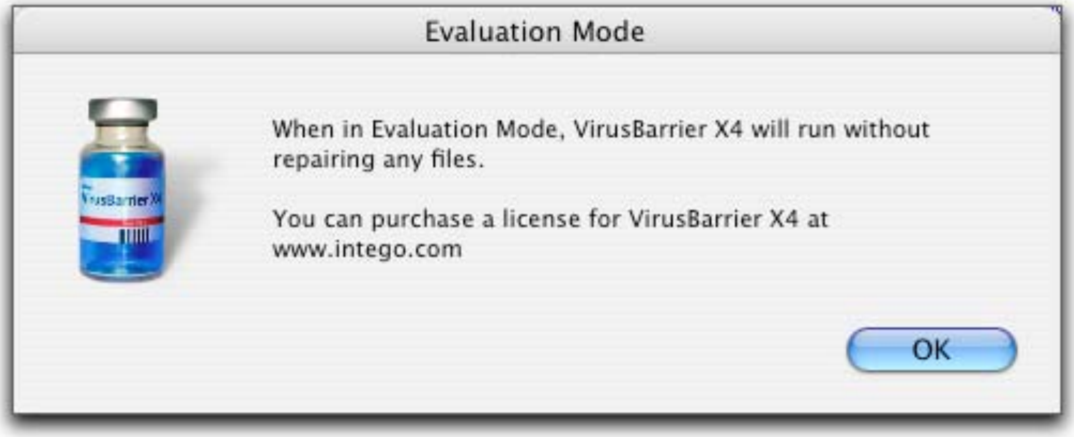
If you purchase a license when using Intego VirusBarrier X4 in Evaluation Mode and want to enter your serial number, this is what you must do:

If VirusBarrier X4 is not launched, then launch it. A window will display telling you that VirusBarrier X4 is currently running in Evaluation Mode. Click the Serialize… button at the bottom of the window. The serialization window will open. Enter your name, company, if any, and your serial number.

If VirusBarrier X4 is already launched, quit VirusBarrier X4, relaunch it and follow the instructions in the preceding paragraph.

Using Intego VirusBarrier X4 in Evaluation Mode

Intego VirusBarrier X4 offers an evaluation mode, to allow you to discover how it works before purchasing the program. To use Intego VirusBarrier X4 in evaluation mode, click Evaluation Mode when when you launch the program and you see a screen asking you to Serialize or to use Evaluation Mode. Intego VirusBarrier X4 then displays the following window:



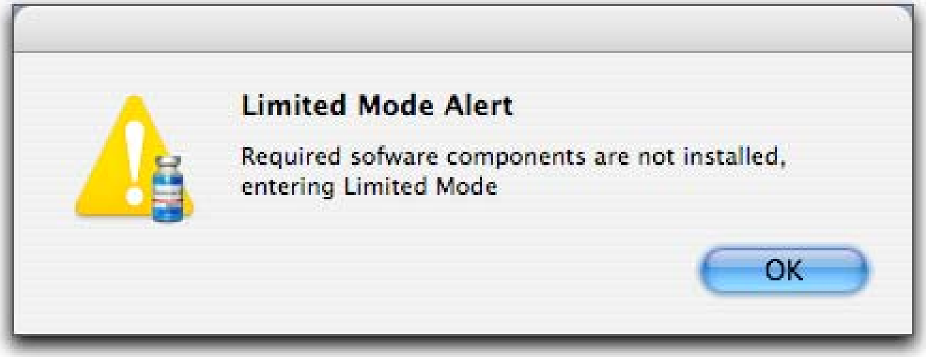
When in Evaluation Mode, VirusBarrier X4 will run without repairing any files.

You can purchase a license for VirusBarrier X4 at www.intego.com

To enter your serial number when you are using VirusBarrier X4 in Evaluation Mode see Serializing Intego VirusBarrier X4 above.

When Intego VirusBarrier X4 Runs in Limited Mode

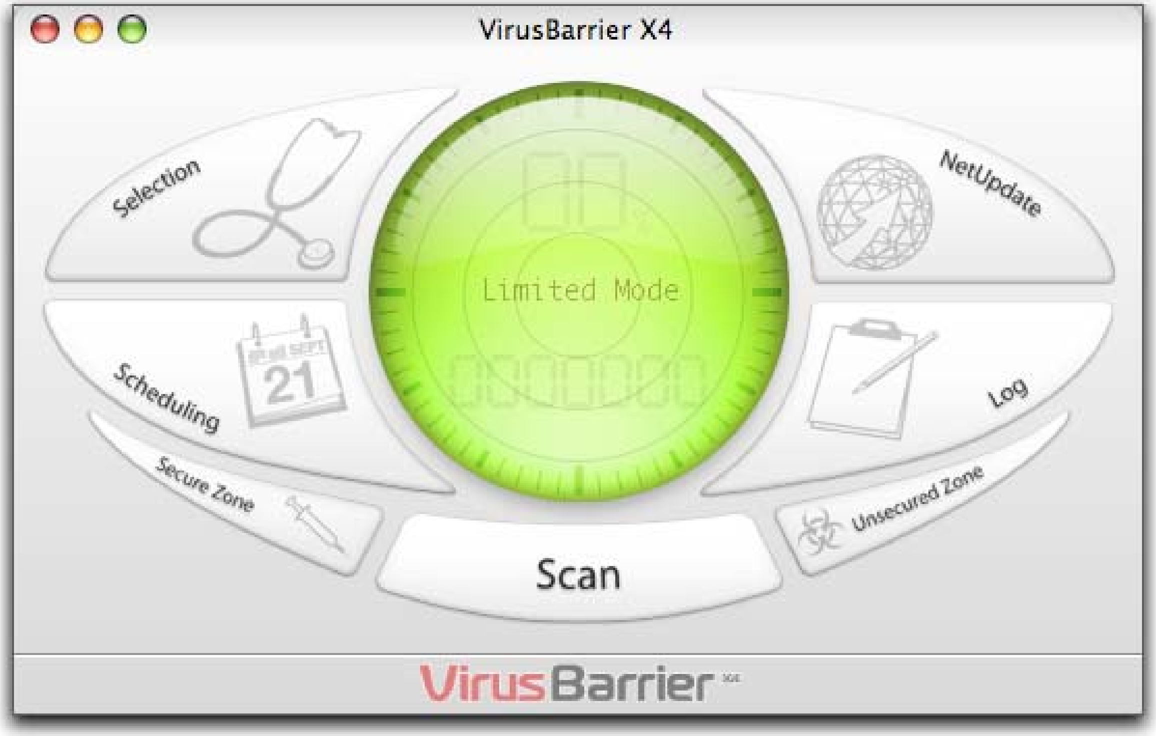
Intego VirusBarrier X4 will run in Limited Mode if, following an installation error or an incompatibility, parts of Intego VirusBarrier X4 have been temporarily disabled. The following Alert will usually display:



Limited Mode Alert

Required sofware components are not installed, entering Limited Mode

When in Limited Mode, Intego VirusBarrier X4 will not repair any files, nor will it allow virus definitions to be updated automatically. It will run using VirusBarrier X4's default settings, which permits manual scans only.



If you should find that Intego VirusBarrier X4 is running in Limited Mode, try restarting the computer. If that does not solve the problem, contact Technical Support as described in **chapter 8 (Technical Support)**.

4 - Quick Start

Intego VirusBarrier X4's Default Mode

When you install Intego VirusBarrier X4, and restart your Macintosh, it automatically begins watching over your computer. Intego VirusBarrier X4 is designed to be simple and non-intrusive, and it fully protects your computer without your doing anything at all.

Once the program is installed, you can just let it run on its own. However, it is recommended that you either set the NetUpdate X4 feature to make automatic checks, to find if the program has been updated, or that you make manual checks at least once a month.

To open Intego VirusBarrier X4, and change any of the settings, or run a manual scan, find the Intego VirusBarrier X4 icon in the Applications folder, and double-click it.

Intego VirusBarrier X4 Interface

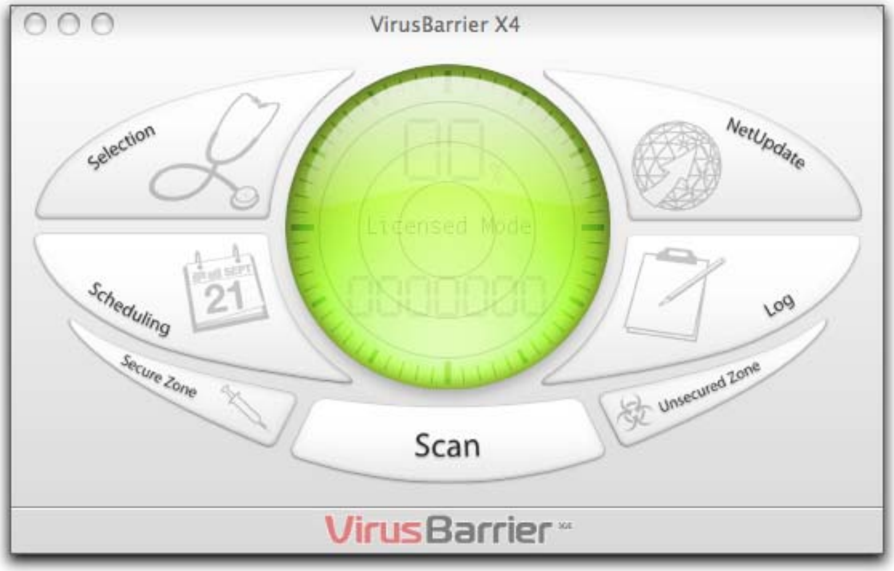
The Intego VirusBarrier X4 application looks like this. It contains the Orb, the contextual control button, and several other buttons for choosing settings or running scans. To access any of these features, click on one of the buttons on the interface.

The Intego VirusBarrier X4 Orb
This gives you information about the current operation.

The Contextual Control button
This button changes according to the function it can have, such as Scan, Pause, Stop, etc.

The Selection button
This button lets you select a volume, folder or file to scan for viruses.

The Log button
This button opens a list of logs, showing you the dates and times of any manual scans and any infected or damaged files found.



The NetUpdate button
This button lets you check for updates to Intego VirusBarrier X4.

The Scheduler Button
This button allows you to set a schedule of fixed times when you want to run the Intego VirusBarrier X4 program.

The Secure Zone button

This button allows you to specify items that you want to secure, by automatically running a virus scan on all new, downloaded, altered or shared files. It alerts you of any modifications that occur.

The Unsecured Zone button

This button allows you to specify a part of your data storage (for example, a folder, a partition or a hard disk), on which you do not want to run scans, as this contains nothing but known healthy files.

The VirusBarrier X4 button

This button gives you information about Intego VirusBarrier X4, including its version number.

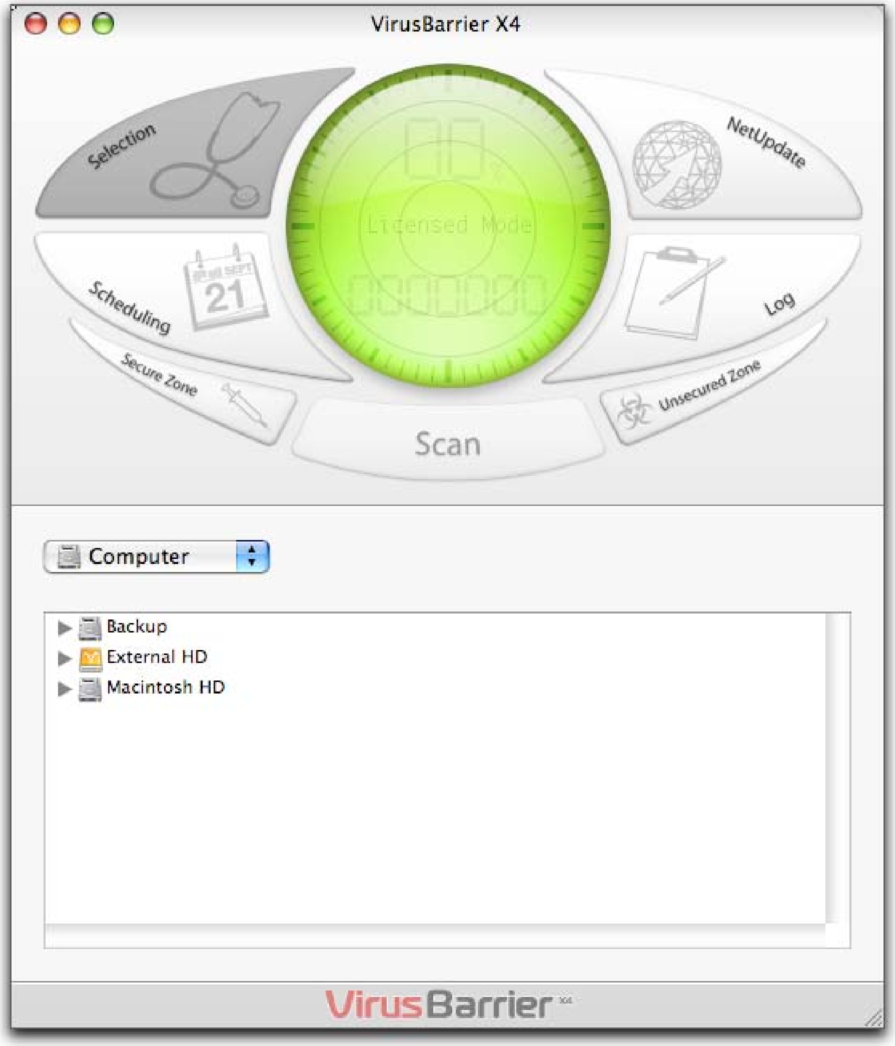
Running a Manual Scan

Once Intego VirusBarrier X4 is installed, it watches over your files ensuring that they are safe from viruses. But Intego VirusBarrier X4 also checks files as they are opened and when modified files are closed. This is a unique feature of VirusBarrier X4 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, Intego VirusBarrier X4 makes sure that any new files are safe.

If you did not choose to run a manual scan after installation, or to run a manual scan at any time, open Intego VirusBarrier X4 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 icon when it is running in the background, or onto the Orb program interface when it is in the foreground. You can also drag and drop files onto the VirusBarrier X4 icon in the Dock.

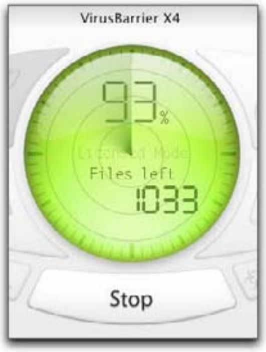
Click the Selection button, and a browser panel will open showing all of the volumes currently mounted on your computer. This view is similar to a Finder list view, showing volumes, folders and files according to their hierarchy. To expand a volume or folder, and view its contents, click the triangle to its left, and all the files and folders it contains will be displayed below it. To collapse an open volume or folder, click the triangle to close it.



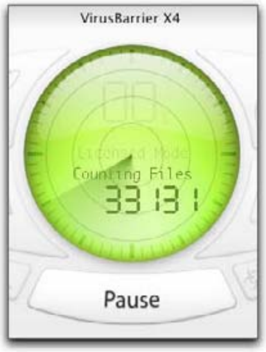
To run a manual scan on any of your volumes, folders or files, double-click the item you wish to scan, or click it once to select it, and click the Scan button. You can also scan any individual volumes, files or folders by simply dragging and dropping them either onto the program icon when it is running in the background, or onto the Orb program interface when it is in the foreground. You will see from the activity in the Orb that scanning has begun. The Orb first displays the number of files scanned as it works.

You will note that the list of files shown in the Selection Panel refreshes whenever you mount a volume, or otherwise navigate to a zone on your system, so that you can keep track at all times where you are, and what data you are working on.

If you have selected Show files left in the Preferences, Intego VirusBarrier X4 counts how many files are to be scanned, then displays the number of files left and the percentage of the scan remaining. If you click the Orb, the display will change to show the number of files scanned, and the corresponding percentage.



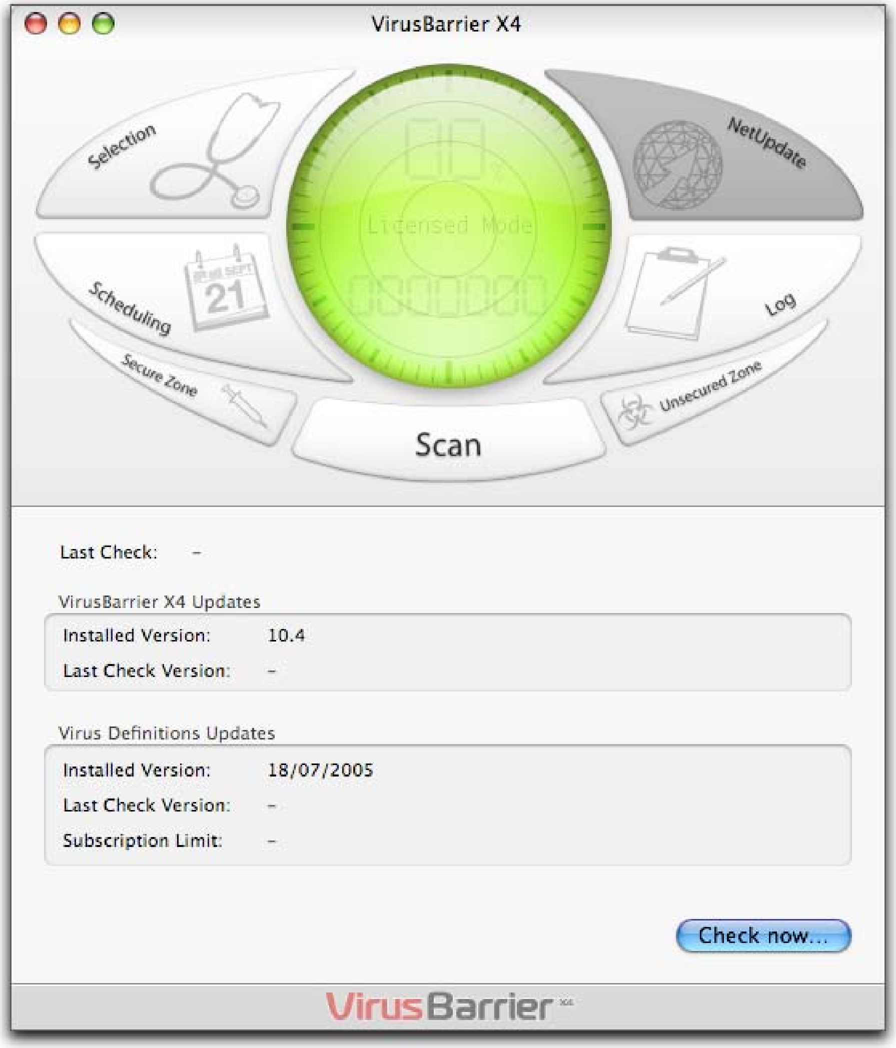
You can stop the scan at any time by pressing the Stop button. If you wish to pause the scan, hold down the Shift key on your keyboard, and you will notice that the Stop button now displays Pause. Click this button, and scanning will pause.



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

NetUpdate X4 Settings

If you click the NetUpdate button, the NetUpdate panel opens. This drawer lets you check for updates, and also gives you information on the last time you checked, the version number of Intego VirusBarrier X4, and the subscription limit of your virus definition updates. When you purchase Intego VirusBarrier X4, you have access to minor program updates and virus definition updates for one year from the date of purchase.



Last Check: –

VirusBarrier X4 Updates

Installed Version: 10.4

Last Check Version: –

Virus Definitions Updates

Installed Version: 18/07/2005

Last Check Version: –

Subscription Limit: –

It is essential that you make regular updates to Intego VirusBarrier X4, to ensure that you are protected from the latest viruses. Intego VirusBarrier X4 includes Intego's NetUpdate, which can check automatically to see if the program has been updated, and download and install the update for you.

To check for updates, click the Check now… button. Intego NetUpdate will open and will connect to Intego’s server to check for updates to the program or to virus definitions. When you purchase Intego VirusBarrier X4, you have access to minor program updates and to virus definition updates for one year from the date of purchase.

You can set NetUpdate settings, such as choosing days and times for automatic updates, from the Intego NetUpdate Preferences Pane in the System Preferences.

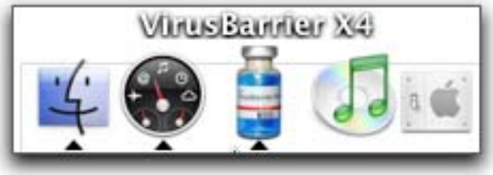
For more on NetUpdate, see chapter 6, Intego VirusBarrier X4 Settings, and see the NetUpdate manual.

Drag and Drop Scanning

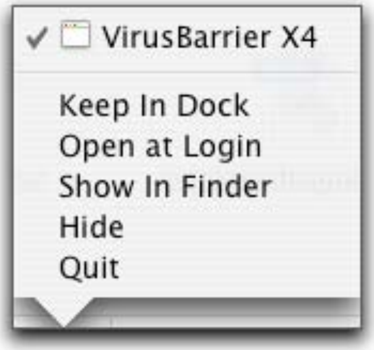
You can scan any volume, folder or file by dragging it on to any part of the VirusBarrier X4 interface. You can also do this by dragging and dropping the volume, folder or file onto the Intego VirusBarrier X4 icon. Once you release the item to be scanned, Intego VirusBarrier X4 will start scanning it, the same as for any other manual scan.

Using Intego VirusBarrier X4 in the Dock

After you open Intego VirusBarrier X4, you will see its icon in the Dock.



If you click this icon, and select Keep in Dock from the menu that appears, the icon will remain in the Dock even after you quit the application.



You can drag files, folders or volumes onto the Intego VirusBarrier X4 icon, and Intego VirusBarrier X4 will open and begin to check the files.

If you check Hide application at startup in the System Preferences, the Intego VirusBarrier X4 application will not become visible in normal use. For more on preferences, see **chapter 6, Intego VirusBarrier X4 Settings**.

5 – Intego VirusBarrier X4 Features

Intego VirusBarrier X4 is a powerful, easy-to-use program that protects your computer from all known types of viruses. It works in the background, providing you silent and efficient protection all the time.

Virus Scanning

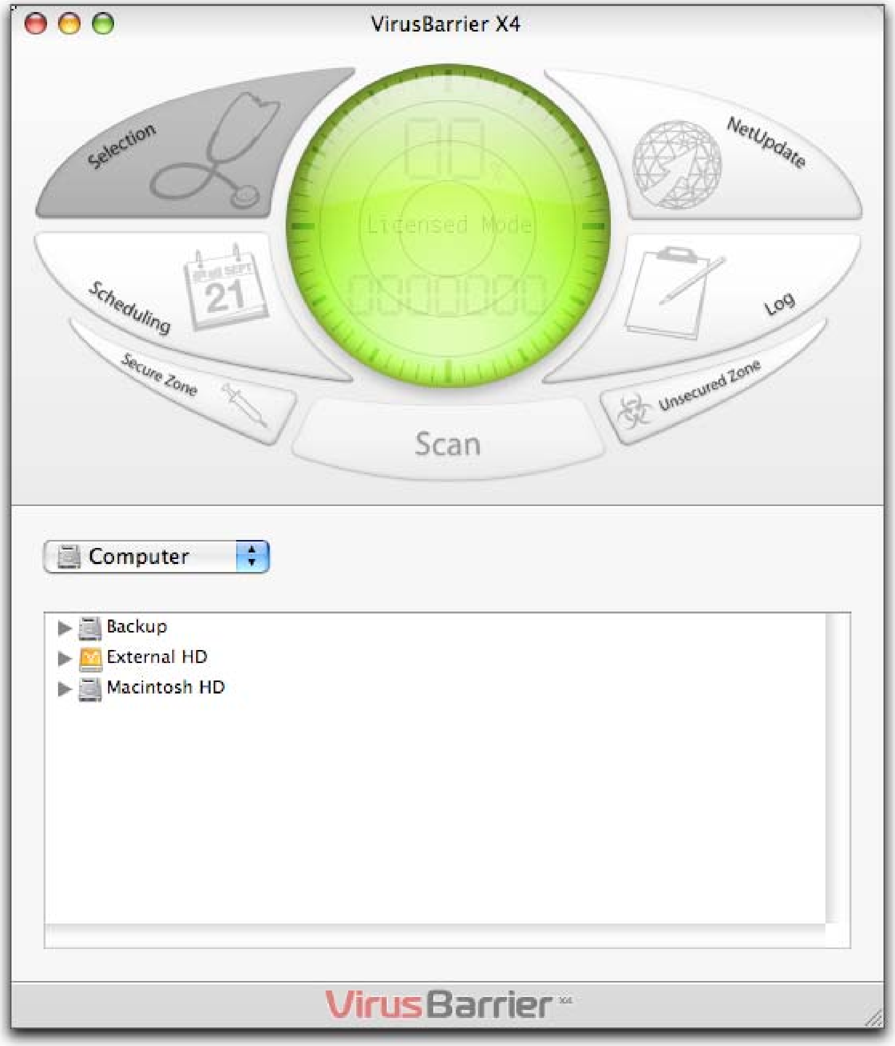
Intego VirusBarrier X4 works in several ways. It constantly watches over your computer at all times, protecting you from viruses, and it automatically checks all files when they are opened and when you close them after making modifications. It can also work in manual mode, allowing you to scan any computer, disk, or volume on your computer or on a network.

Note that when File Vault has been activated, VirusBarrier X4 continues to protect your computer and volumes continuously by scanning files when they are opened or when modified files are closed, even in folders that you are not authorized for. This is not the case, however, for manual scans. In this instance, only files that you are authorized to access can be scanned.

Manual Scans

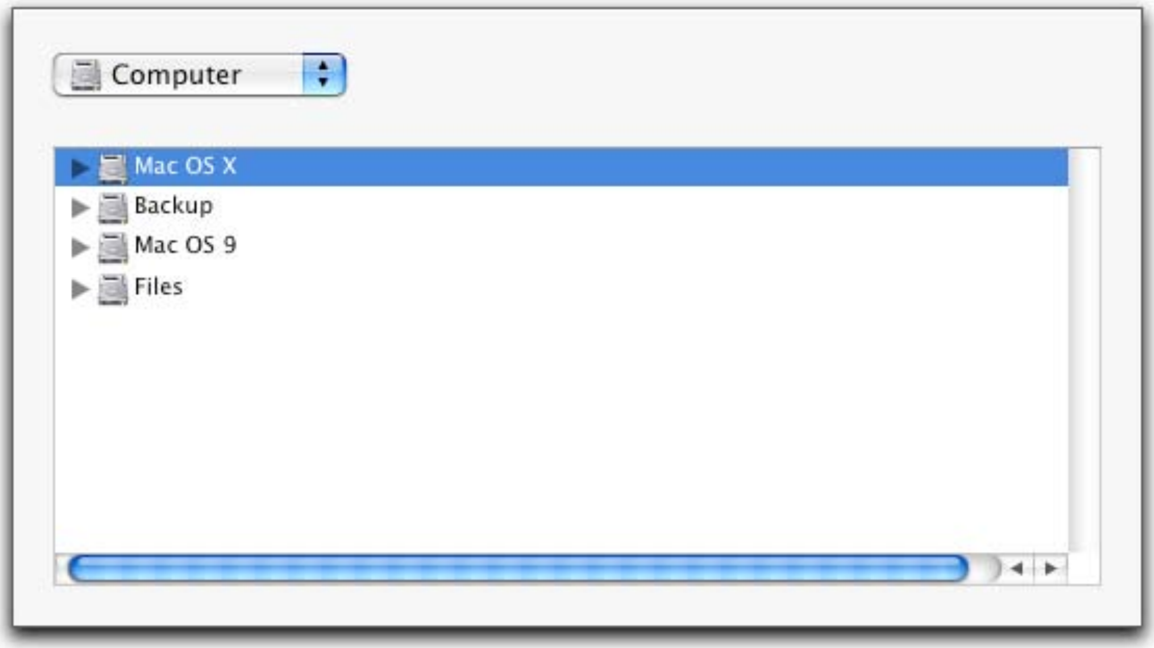
The first time you use Intego VirusBarrier X4, you should run a manual scan on all of your computer's hard disks or volumes. This ensures that there are no viruses hiding on your computer. You should do this right after you install the program.

You can also run a manual scan on any volume, folder or file, at any time. To do this, open Intego VirusBarrier X4, and click the Selection button.



A drawer will open showing all of the volumes currently mounted on your computer. This view is similar to a Finder list view, showing volumes, folders and files according to their hierarchy. To expand a volume or folder, and view its contents, click the triangle to its left, and all the files and folders it contains will be displayed below it. To collapse an open volume or folder, click the triangle to close it.

Scanning a Volume



To scan a volume, just double-click it, or click it once to select it, and click the Scan button. You can also scan any individual volumes by simply dragging and dropping them either onto the program icon when it is running in the background, or onto the Orb when it is in the foreground. You will see from the activity in the Orb that scanning has begun. The Orb first displays the number of files scanned as it works.

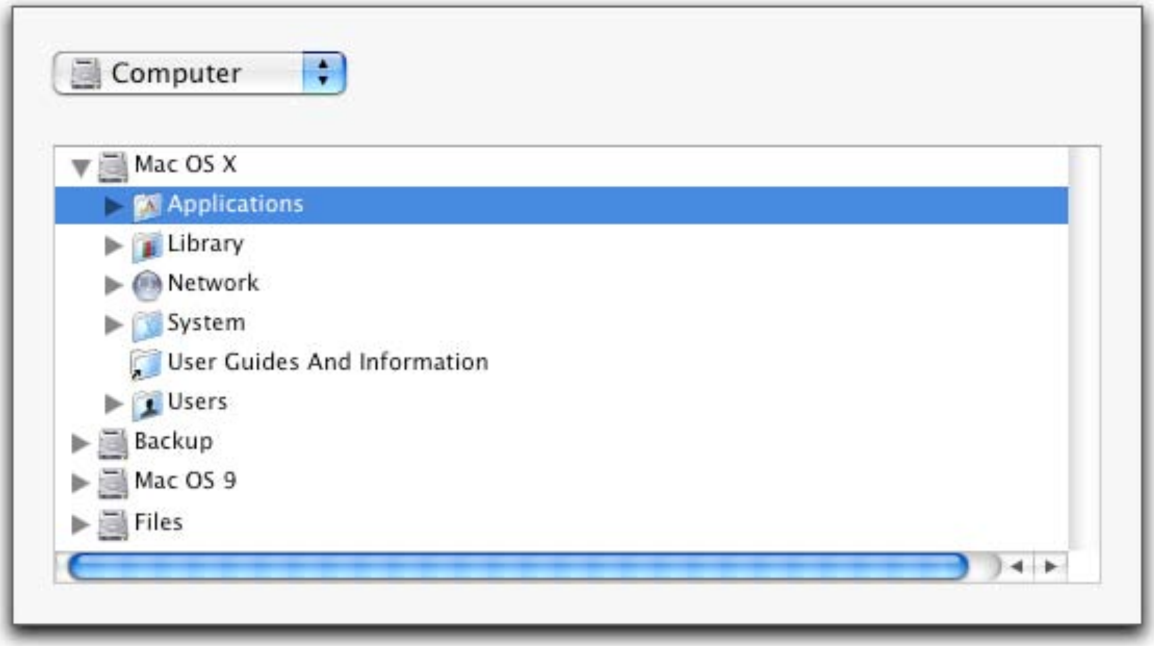
If you have selected Show files left in the Preferences, Intego VirusBarrier X4 counts how many files are to be scanned, then displays the number of files left and the percentage of the scan remaining. If you click the Orb, the display will change to show the number of files scanned, and the corresponding percentage.

You can stop the scan at any time by pressing the Stop button.

If you wish to pause the scan, hold down the Shift 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.

Scanning a Folder



To scan any folder on your computer, click the triangle at the left of a volume, and navigate in this manner until you find the folder you want to scan. Double-click this folder, or click it once to select it, and then click the Scan button.

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

You will see from the activity in the Orb that scanning has begun. The Orb first displays the number of files scanned as it works.

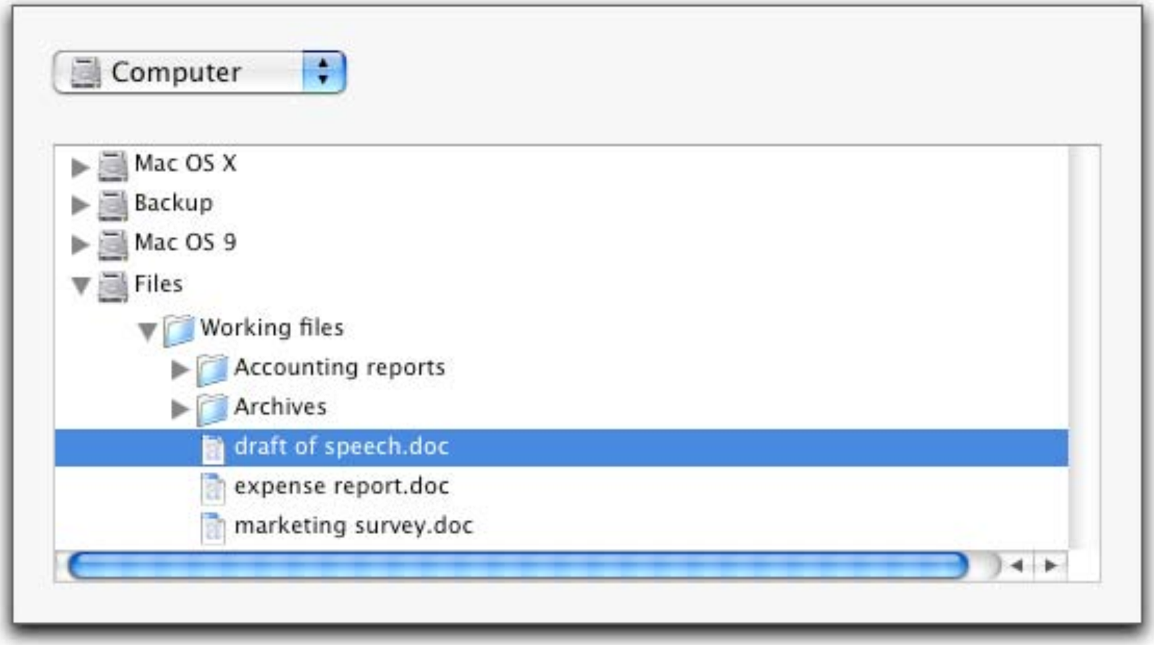
If you have selected Show files left in the Preferences, Intego VirusBarrier X4 counts how many files are to be scanned, then displays the number of files left and the percentage of the scan remaining. If you click the Orb, the display will change to show the number of files scanned, and the corresponding percentage.

You can stop the scan at any time by pressing the Stop button.

If you wish to pause the scan, hold down the Shift 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.

Scanning a File



To scan any folder on your computer, click the triangle at the left of a volume, and navigate in this manner until you find the file you want to scan. Double-click this file, or click it once to select it, and then click the Scan button.

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

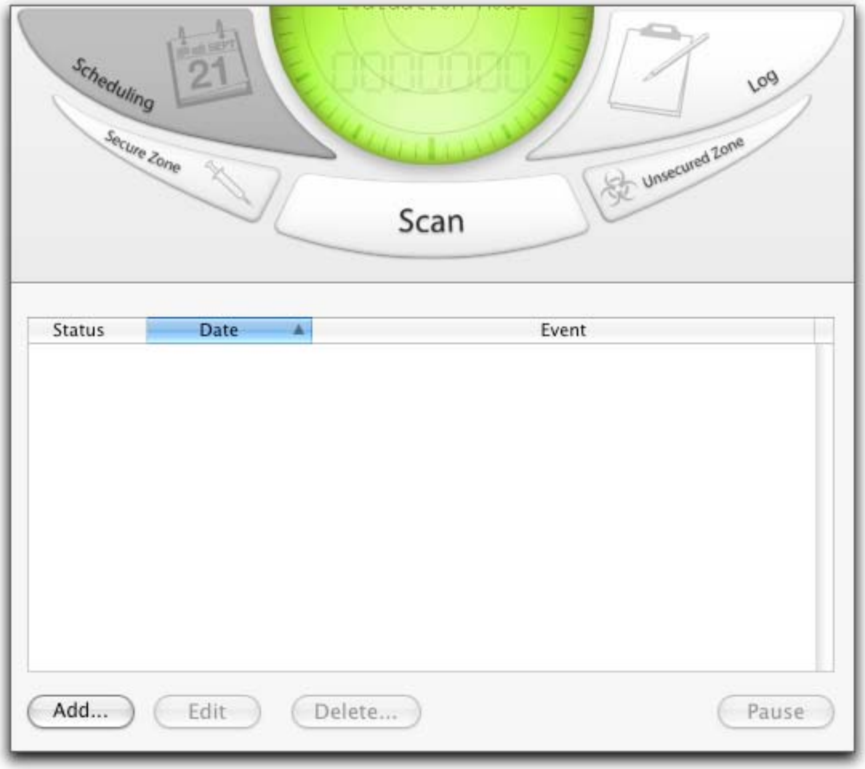
You will see from the activity in the Orb that scanning has begun, but, in most cases, if you are scanning just one file, the scan will be completed almost immediately.

Drag and Drop Scanning

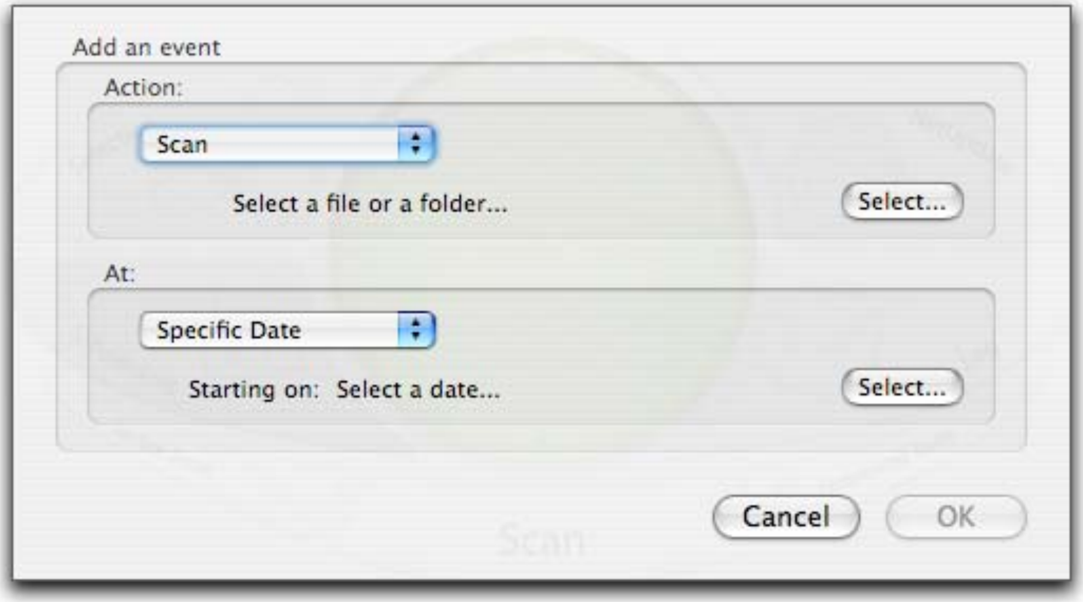
You can scan any volume, folder or file by dragging it onto any part of the Intego VirusBarrier X4 interface. You can also do this by dragging and dropping the volume, folder or file onto the Intego VirusBarrier X4 program icon or Dock icon. Once you release the item to be scanned, Intego VirusBarrier X4 will start scanning it, the same as for any other manual scan.

Scheduled Scanning

Intego VirusBarrier X4 now offers the option of running at pre-arranged times. To access this function, click on the Scheduling button on the interface. The first time you do this, the following window will display:



To add a new schedule, click on the Add… button and the following window will open:



Add an event

Action:

Scan

Select a file or a folder...

At:

Specific Date

Starting on: Select a date...

You can set the action to Scan, Repair, Export a Log or Clear a Log on any selected file, folder or volume of your choice. You can also drag and drop a file onto the Scheduler.

Similarly you can set the scheduler to run at any specific date (and time), every day, week or month, and most usefully when mounting or unmounting a volume. The last choices are perfect for ensuring that any data added to the computer inadvertently, through mounting a removable disk, or even a USB drive, will be scanned automatically, thus keeping your system safe at all times.

Intego Calendar for Apple's iCal

You can choose to subscribe to Intego's calendar for Apple's iCal software. To do this, launch VirusBarrier X4, go to the VirusBarrier X4 menu and select Subscribe to Intego's Calendar… This will launch iCal, and a window will display requesting the address of the calendar to subscribe to.

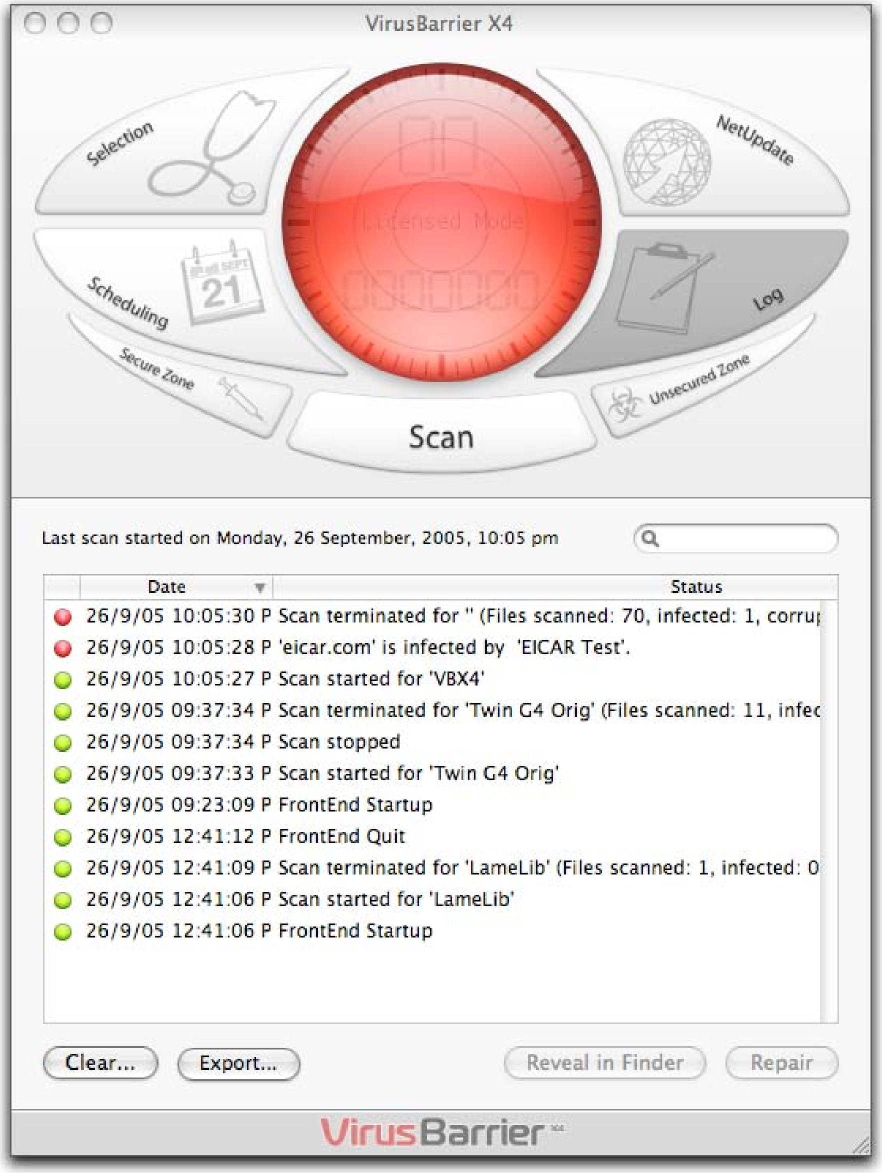
E-mail Analysis

Another useful feature of Intego VirusBarrier X4 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.

Intego VirusBarrier X4 also scans and analyses outgoing e-mail and attachments, thus making sure that you are not passing on any viruses to your correspondents either.

Scan Results – The Log Panel

If Intego VirusBarrier X4 finds any infected files, the Log panel will open, showing the names of any infected files, and the type of viruses they are infected with. You can also open the Log at any time by clicking on the Log button. The panel below will then open:



Last scan started on Monday, 26 September, 2005, 10:05 pm

```
Date                 Status
🔴 26/9/05 10:05:30 P Scan terminated for '' (Files scanned: 70, infected: 1, corru
🔴 26/9/05 10:05:28 P 'eicar.com' is infected by  'EICAR Test'.
🟢 26/9/05 10:05:27 P Scan started for 'VBX4'
🟢 26/9/05 09:37:34 P Scan terminated for 'Twin G4 Orig' (Files scanned: 11, infec
🟢 26/9/05 09:37:34 P Scan stopped
🟢 26/9/05 09:37:33 P Scan started for 'Twin G4 Orig'
🟢 26/9/05 09:23:09 P FrontEnd Startup
🟢 26/9/05 12:41:12 P FrontEnd Quit
🟢 26/9/05 12:41:09 P Scan terminated for 'LameLib' (Files scanned: 1, infected: 0
🟢 26/9/05 12:41:06 P Scan started for 'LameLib'
🟢 26/9/05 12:41:06 P FrontEnd Startup
```

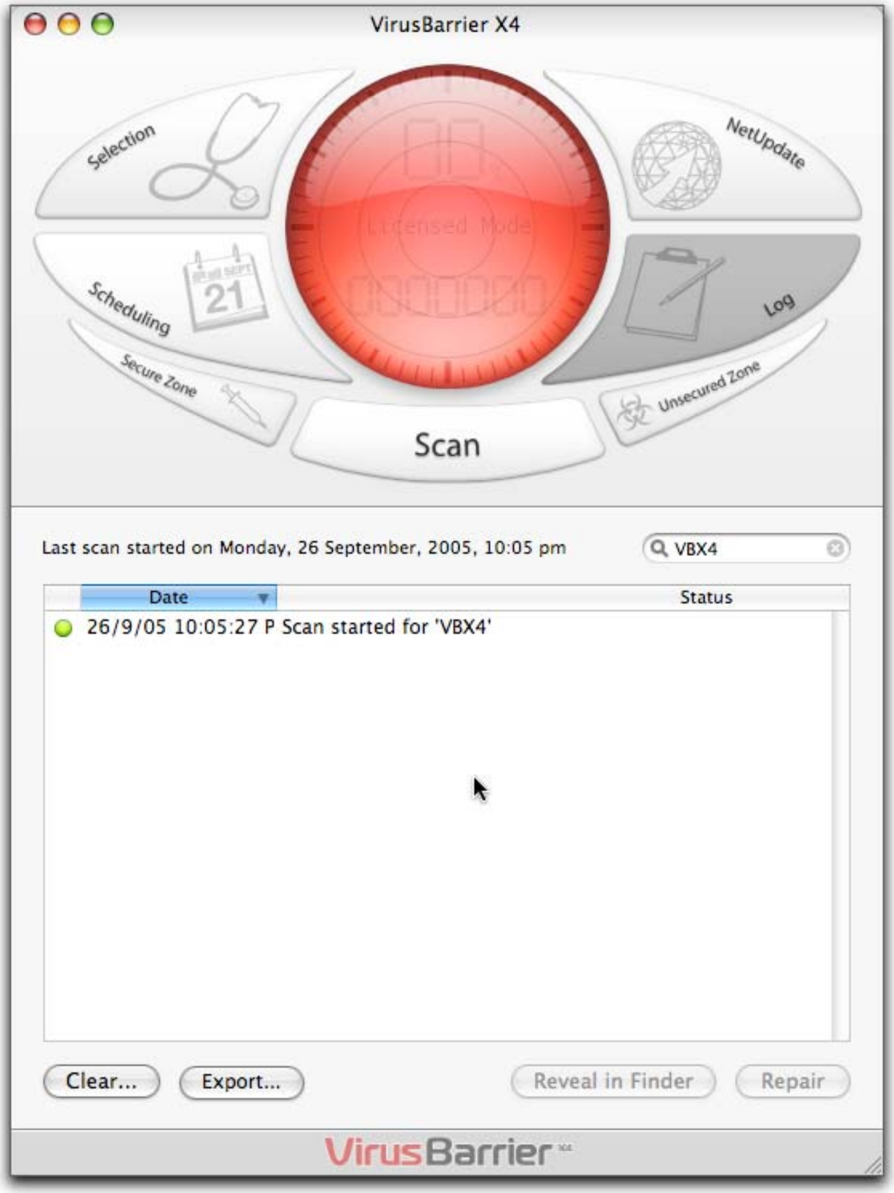
If you have set Intego VirusBarrier X4 to scan only and not repair, the Log panel will show any infected files and the type of viruses they are infected with. If Intego VirusBarrier X4 is set to repair files automatically, you will see the names of any repaired files, and what type of viruses they had.

You can easily see any clean scans and any infected files found. The files, folders or volumes selected for each scan are clearly identified, as are any problems found.

It is possible that all the details might not fit in the window. This can be remedied either by dragging the window wider, until all details of the files scanned, infected, corrupted and repaired are clearly legible, or by exporting the log using the Export button at the bottom of the window.

In the lower pane of the log panel you can also click and drag the column headings to show more or less of the text in either column, and to change the sort order in the date column to show ascending or descending order. If you still need to see more, you can always click and drag the bottom right corner of the window to expand (or shrink) it as a whole.

A feature that adds flexibility is the option to do a search on the results. This means that the log can safely be kept for quite some time, and searched for details relating to the scans actually run. An example is shown below:

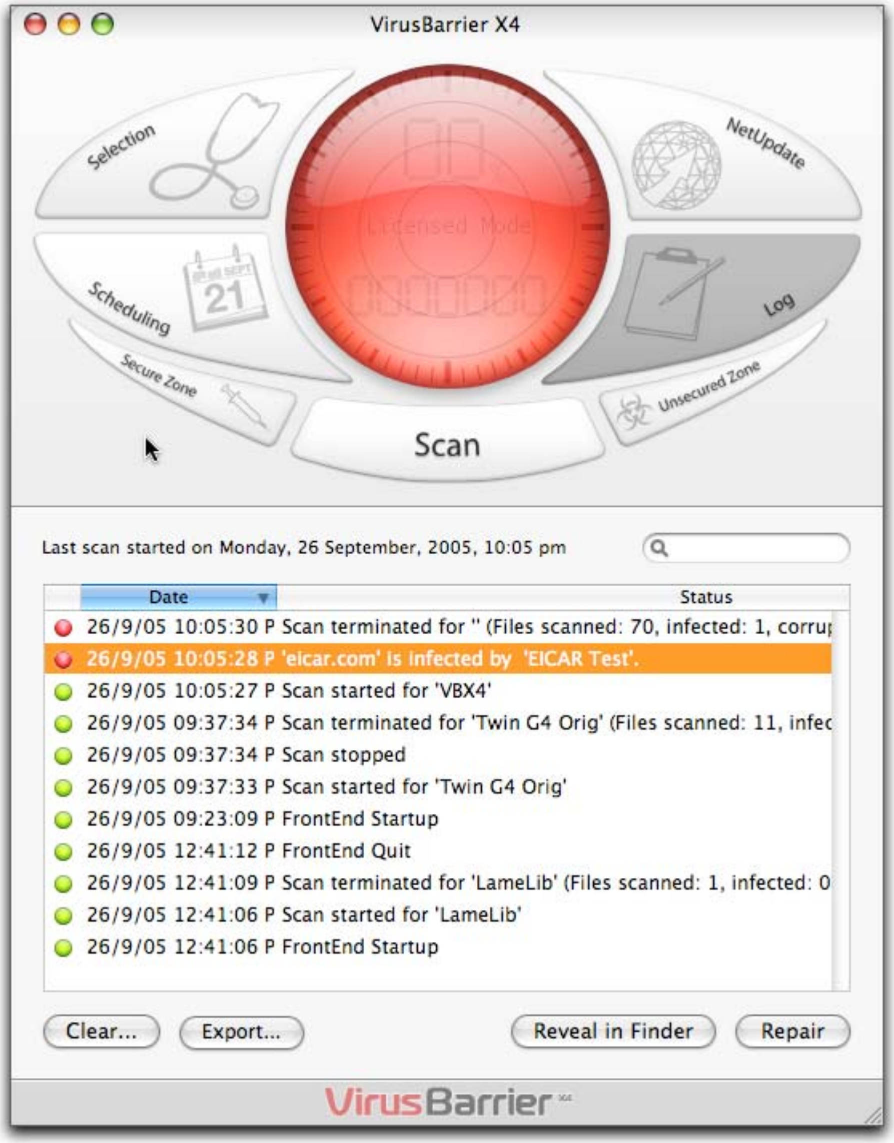


Last scan started on Monday, 26 September, 2005, 10:05 pm

Date	Status
26/9/05 10:05:27 P	Scan started for 'VBX4'

It is worth noting that the results of the last scan determine the color of the Orb section of the window. This acts as a permanent reminder that action may be required before quitting the program, to keep the system completely safe.

If the Log shows an infected file has been found, you can click on it in the listing, and then two further options become available, as shown below:



Last scan started on Monday, 26 September, 2005, 10:05 pm

```
Date                  Status
26/9/05 10:05:30 P Scan terminated for '' (Files scanned: 70, infected: 1, corru
26/9/05 10:05:28 P 'eicar.com' is infected by 'EICAR Test'.
26/9/05 10:05:27 P Scan started for 'VBX4'
26/9/05 09:37:34 P Scan terminated for 'Twin G4 Orig' (Files scanned: 11, infec
26/9/05 09:37:34 P Scan stopped
26/9/05 09:37:33 P Scan started for 'Twin G4 Orig'
26/9/05 09:23:09 P FrontEnd Startup
26/9/05 12:41:12 P FrontEnd Quit
26/9/05 12:41:09 P Scan terminated for 'LameLib' (Files scanned: 1, infected: 0
26/9/05 12:41:06 P Scan started for 'LameLib'
26/9/05 12:41:06 P FrontEnd Startup
```

Clicking on the Reveal in Finder button opens a new Finder window showing the folder in which the infected file is found. This enables you to simply delete the file if you wish.

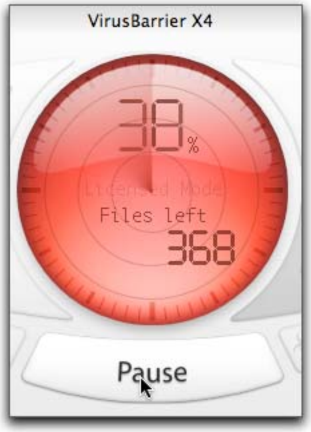
Clicking on Repair will repair the file that is damaged, if VirusBarrier X4 can do so; this is not possible in all cases, since files that are severely damaged may not be reparable. The log will not show any change after you repair a file, since it simply records what VirusBarrier X4 found during its last scan. If you run VirusBarrier X4 again to scan your files, you will no longer find the repaired file in the log (if VirusBarrier X4 was indeed able to repair the file).

Lastly, whenever you like, you can clear the Log, returning Intego VirusBarrier X4 to a clean status, with a green Orb in the interface, to show that everything is normal.

Understanding Scan Results

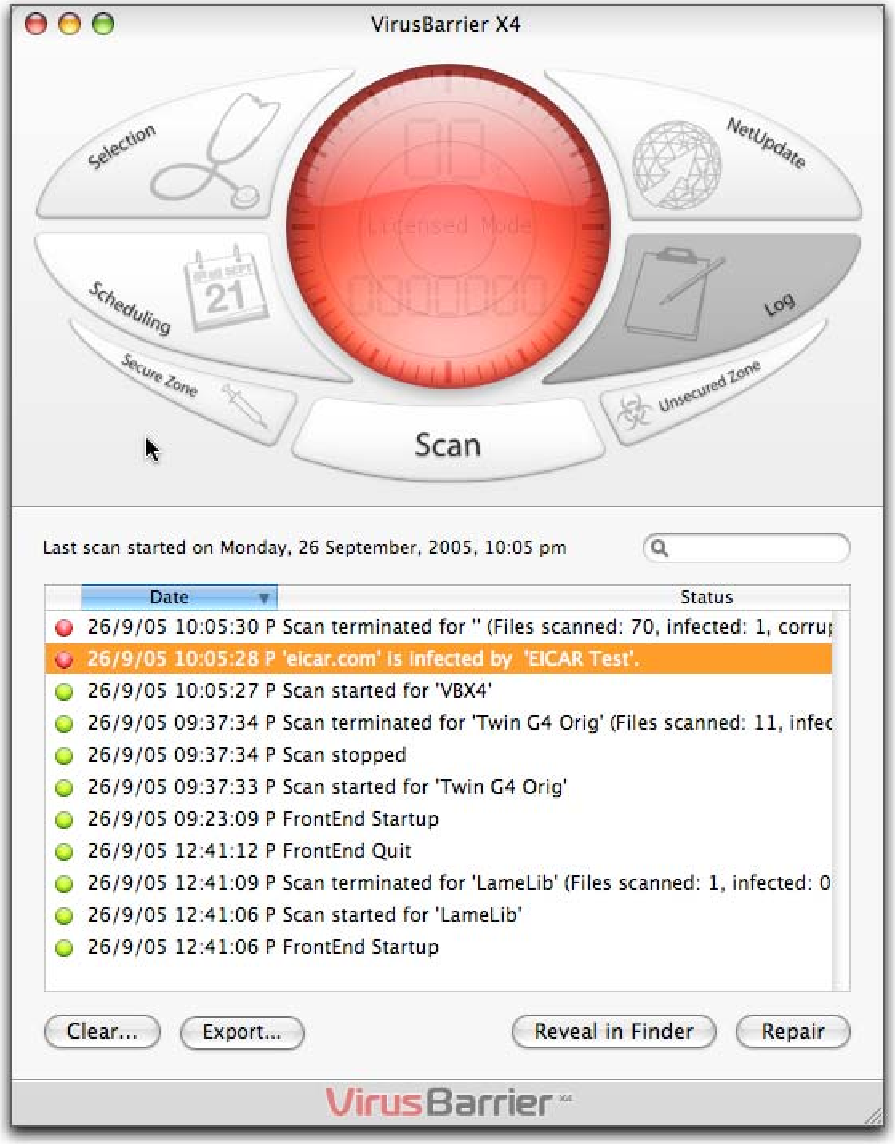
Intego VirusBarrier X4 will inform you if it finds any files infected by any known viruses. It will also alert you if any damaged files are found.

Infected Files



If any infected files are found, the Intego VirusBarrier X4 Orb will turn red, and the Log panel will open. This panel will open as soon as an infected file is found, so the scan may still be going on when this drawer opens. Intego VirusBarrier X4 will also alert you, according to the alert options you have set in the Preferences. For more on alert options, see chapter 6, Intego VirusBarrier X4 Settings.

The display in the Log panel will also depend on the Scan Mode you have selected in the Preferences. You have the choice between having Intego VirusBarrier X4 make automatic repairs (Repair Mode), or merely alerting you when infected or damaged files are found (Scan Mode). If you have chosen Repair Mode, repairs will be made immediately, if possible. If you have chosen Scan Mode, repairs must be made manually. For more on Repair Mode and Scan Mode, see chapter 6, Intego VirusBarrier X4 Settings.



Last scan started on Monday, 26 September, 2005, 10:05 pm

```
Date                 Status
● 26/9/05 10:05:30 P Scan terminated for '' (Files scanned: 70, infected: 1, corru
● 26/9/05 10:05:28 P 'eicar.com' is infected by 'EICAR Test'.
● 26/9/05 10:05:27 P Scan started for 'VBX4'
● 26/9/05 09:37:34 P Scan terminated for 'Twin G4 Orig' (Files scanned: 11, infec
● 26/9/05 09:37:34 P Scan stopped
● 26/9/05 09:37:33 P Scan started for 'Twin G4 Orig'
● 26/9/05 09:23:09 P FrontEnd Startup
● 26/9/05 12:41:12 P FrontEnd Quit
● 26/9/05 12:41:09 P Scan terminated for 'LameLib' (Files scanned: 1, infected: 0
● 26/9/05 12:41:06 P Scan started for 'LameLib'
● 26/9/05 12:41:06 P FrontEnd Startup
```

If you have chosen Scan Mode, the Log panel will show the names of any files that are infected. To repair a file or files, select the items you wish to repair, and click the Repair button at the bottom of the window. The file will be repaired, and the Log panel will show this change. To view any of these files in the Finder, click a file to select it and click Reveal in Finder.

Corrupted Files

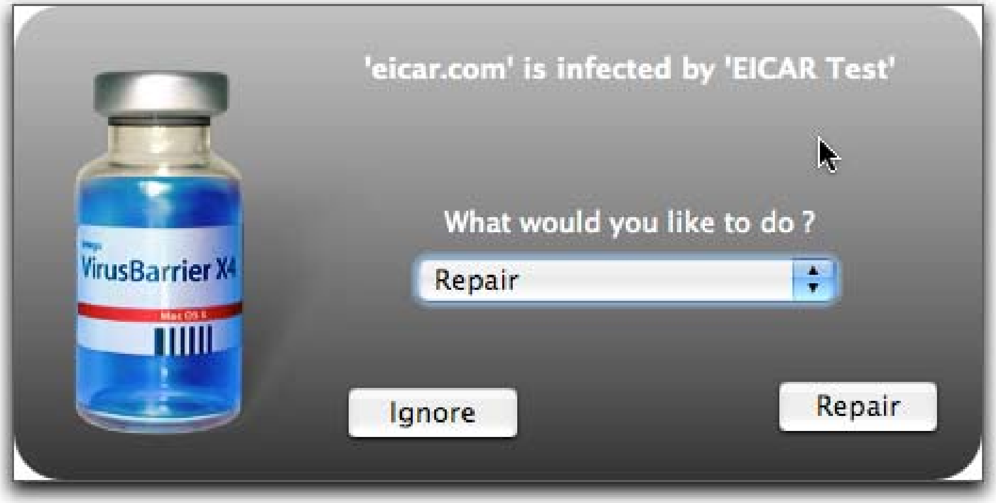
If any corrupted files are found, the Intego VirusBarrier X4 Log panel will open. This panel will open as soon as a damaged file is found, so the scan may still be going on when this drawer opens.

Corrupted files may or may not contain viruses. Viruses, however, can damage files, even if they do not copy themselves to these files. These files could also have been damaged by such things as disk errors, or crashes when files are opened. If any damaged files are found, you should replace them as soon as possible.

Alerts

While Intego VirusBarrier X4 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 Intego VirusBarrier X4 detects any infected files, and you have set it to scan, and not automatically repair infected files, it will display an alert.


'eicar.com' is infected by 'EICAR Test'

What would you like to do ?

Repair

If you want Intego VirusBarrier X4 to repair the file, click Repair. If not, click Ignore, and the file will not be repaired. Warning: this can be dangerous! Only select to not repair files if you are sure of what you are doing!

For more on setting Alert preferences, see **chapter 6, Intego VirusBarrier X4 settings.**

Secure Zone

Intego VirusBarrier X4 offers a zone you can specify where files will remain secure. This is a volume or folder that will be checked automatically for viruses as soon as anything changes in it. In addition, VirusBarrier X4 alerts you as soon as a file has been modified or created on your computer, letting you know of any changes made to files on your Mac. This is particularly useful for users who have files or folders that are updated continually or automatically, such as shared folders, download folders or drop boxes.

To designate a folder as a secure zone, open the VirusBarrier X4 interface and click on the Secure Zone button. Drag and drop the folder in the lower portion of the interface the folder you want to add to the zone, or click the Add… button to choose the items you wish to add. Note that subfolders are not automatically included in the Secure Zone – you will have to add any subfolders to be protected individually.

Unsecured Zone

Intego VirusBarrier X4 offers the option to set an Unsecured Zone. This is an area that will not be scanned by VirusBarrier X4. This zone should only be used for safe files that have already been scanned by VirusBarrier X4. To ensure that the files you place in the Unsecured Zone are indeed free of viruses, VirusBarrier X4 will automatically scan them when you add them to the zone.

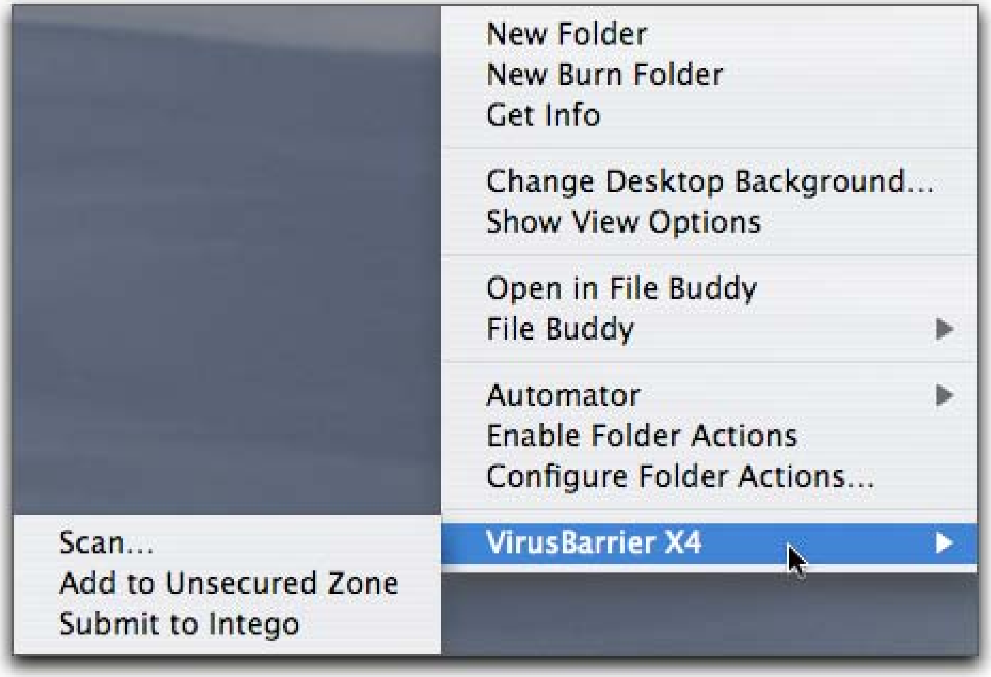
You can also use the Contextual Menu to add items to the Unsecured Zone. See the following section of this manual for more information.

It is worth noting that the results of a Spotlight search (in Mac OS X 10.4 Tiger or higher) can be used to define the Unsecured Zone of your system – which is useful if you want do define your safe files by date, or creator.

Contextual Menu

Intego VirusBarrier X4 also offers an option to run directly from the Finder under Mac OS X, using a Contextual Menu.

To do so, just Control-Click anywhere on the Desktop, or on any Finder icon, and the following contextual menu will open:



You can scan the highlighted item (and repair it if your settings allow).

Alternatively, you can add the item to the Unsecured Zone (exceptions to scans, where data is known to be so safe that no scans are run).

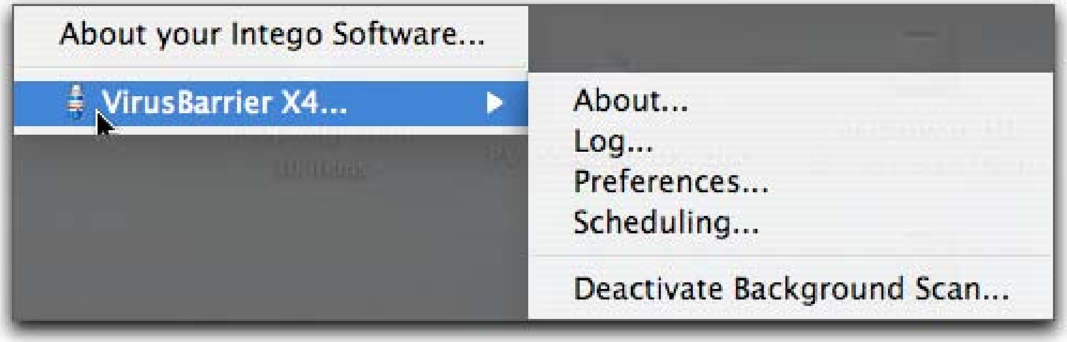
Lastly, and this is especially useful in the case of files that you suspect are infected with new or unrecognized viruses, you can submit a copy of the data to Intego by using the Submit to Intego button. This works directly, without your even having to use your e-mail program, providing you have an active Internet connection.

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.

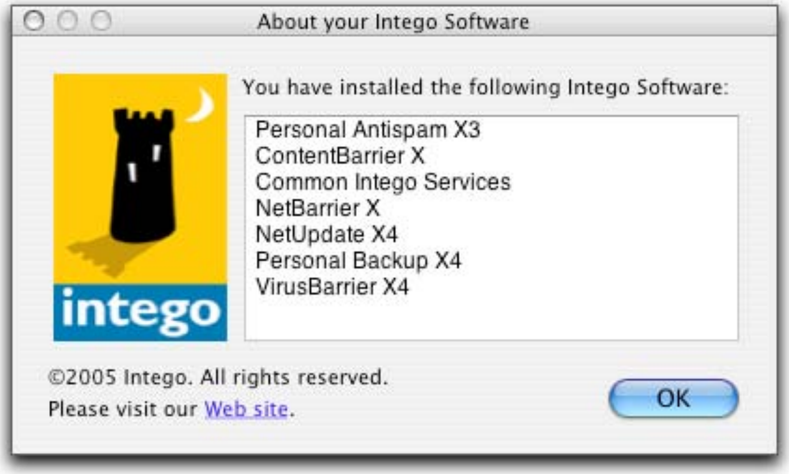
The Intego Menu

Alongside all its other features, Intego VirusBarrier X4 installs a menu in the Finder menu bar, called the Intego menu. Its icon is the yellow and black Intego logo.

Click on the Intego menu icon to see a drop-down menu that looks like this:



The About your Intego Software… menu option details all Intego software currently installed on your computer, and will look something like this:



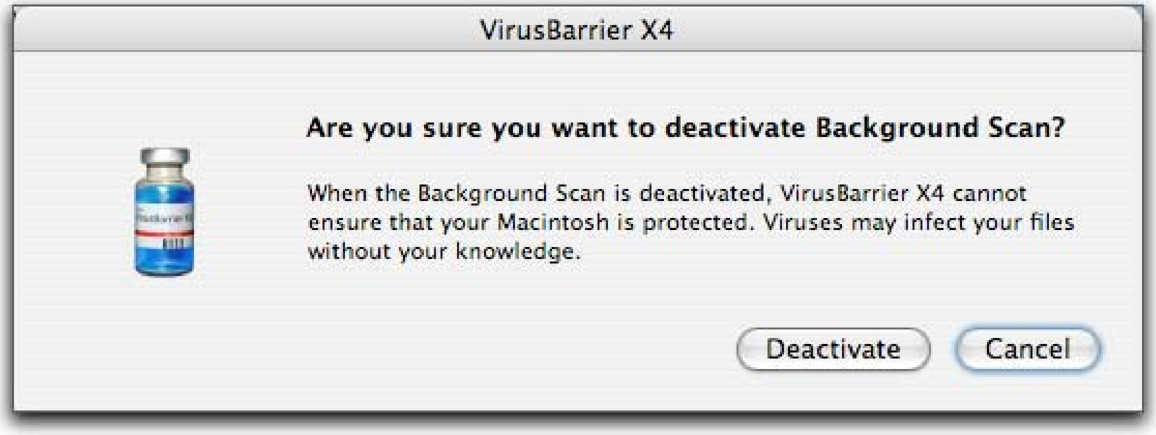
You have installed the following Intego Software:

Personal Antispam X3
ContentBarrier X
Common Intego Services
NetBarrier X
NetUpdate X4
Personal Backup X4
VirusBarrier X4

©2005 Intego. All rights reserved.
Please visit our Web site.

When you select VirusBarrier X4 in the Intego menu, five menu options are displayed. The first four options open the corresponding panel in VirusBarrier X4.

The last option is different. If you drag down and release on Deactivate Background Scan…, you will then see the following Alert window:



VirusBarrier X4

Are you sure you want to deactivate Background Scan?

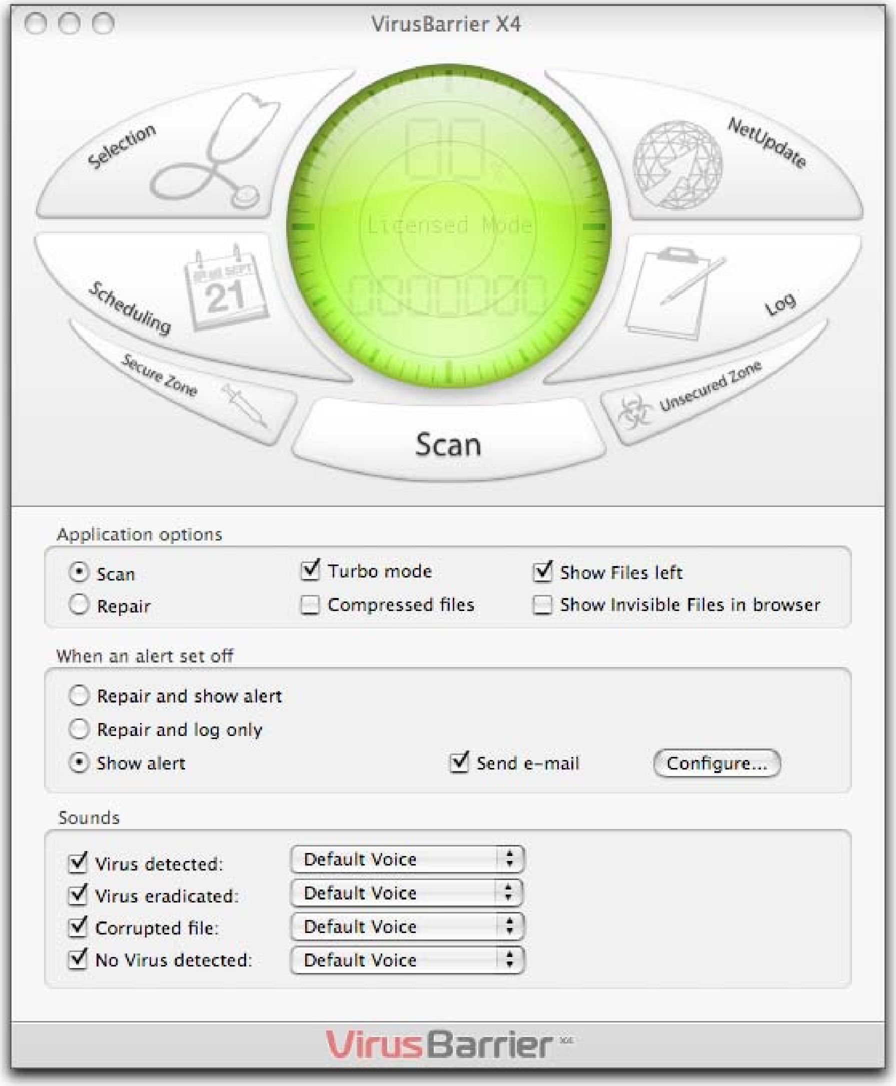
When the Background Scan is deactivated, VirusBarrier X4 cannot ensure that your Macintosh is protected. Viruses may infect your files without your knowledge.

You should only deactivate the Background Scan if you are sure that there is no way that you want your system to remain protected from viruses. This should really only be used as a last resort, such as when specifically required to install special security software.

6 – Intego VirusBarrier X4 Settings

Preferences

If you click the Preferences button on the Intego VirusBarrier X4 interface, or select Preferences… from the Intego VirusBarrier X4 menu, you can set several different options. The first panel lets you set Scan mode options, and the second and third let you set several alert options.



Application options

● Scan ☑ Turbo mode ☑ Show Files left
○ Repair ☐ Compressed files ☐ Show Invisible Files in browser

When an alert set off

○ Repair and show alert
○ Repair and log only
● Show alert ☑ Send e-mail Configure…

Sounds

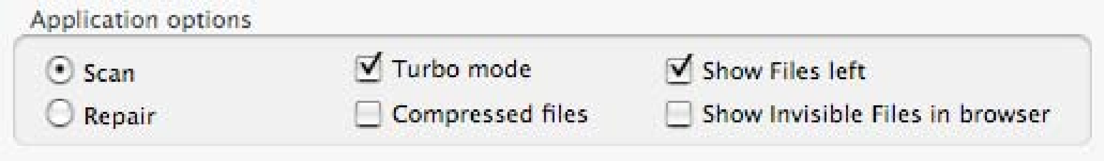
☑ Virus detected: Default Voice
☑ Virus eradicated: Default Voice
☑ Corrupted file: Default Voice
☑ No Virus detected: Default Voice

Scan Mode

This tab lets you set options concerning the way Intego VirusBarrier X4 scans for viruses, and other options concerning the information provided in the Orb.

Modes and Options

This section lets you choose the scanning mode and various other options.



Application options

● Scan ☑ Turbo mode ☑ Show Files left

○ Repair □ Compressed files □ Show Invisible Files in browser

Intego VirusBarrier X4 lets you choose between two virus-scanning modes: Scan Mode and Repair Mode. If you select Scan Mode, Intego VirusBarrier X4 will alert you any time it finds infected files, but will not automatically repair the files by disinfecting them. If a file is found during a scan, Intego VirusBarrier X4 will alert you, or, if you are running a manual scan, the Log will display the infected file, but you will need to repair the file manually. This may be useful if you are on a network, and your network administrator needs to examine any infected files you might find.

To select the Scan Mode you wish to use, click the appropriate radio button.

Several other options are available which control the way Intego VirusBarrier X4 functions.

Turbo Mode

If you check the Turbo mode check box, Intego VirusBarrier X4 will scan your files more quickly. The first time Intego VirusBarrier X4 scans your computer it remembers all the files it examines. As long as these files are not updated or modified, Intego VirusBarrier X4 will not rescan them, scanning from 5 to 40 times faster. However, if any of these files are changed, they will be scanned. Also, when updating Intego VirusBarrier X4 for new virus definitions, all files will be scanned to ensure that all your files are free of all known viruses.

Show Files Left

If you check this option, the Intego VirusBarrier X4 Orb will show the number of files left to be checked when scanning files, rather than the number of files that have been scanned.

Compressed Files

If you check Compressed Files, Intego VirusBarrier X4 will scan compressed files contained in various kinds of archives directly, even if Stuffit Expander is not installed on the computer.

If you have Stuffit Expander installed, .sit archives are handled according to the preferences you set in Stuffit Expander. To scan .sit files with VirusBarrier X4 once they have been decompressed, check this option in the Stuffit Expander preferences.

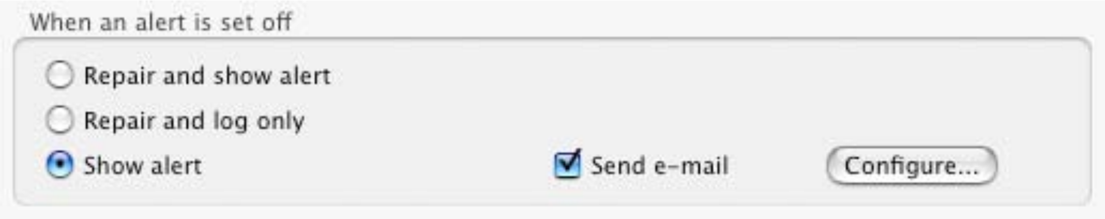
Any infected or corrupted files contained in an archive will be signaled, and they can be repaired or disinfected using Intego VirusBarrier X4 in the usual way. Repairs or disinfection can only take place once the archive file is expanded, and not at the time of scanning.

Show Invisible Files in Browser

If you check this option, Intego VirusBarrier X4 will display invisible files in the Selection panel.

Alerts

This section gives you several options as to how Intego VirusBarrier X4 will act when presenting an Alert.



When an alert is set off

○ Repair and show alert

○ Repair and log only

● Show alert ☑ Send e-mail

There are three options for the way Intego VirusBarrier X4 alerts you to any viruses found in your files when working in the background.

Repair and show alert
If this is checked, Intego VirusBarrier X4 repairs infected files automatically and displays an alert to inform you of the name of the infected file and the virus found.

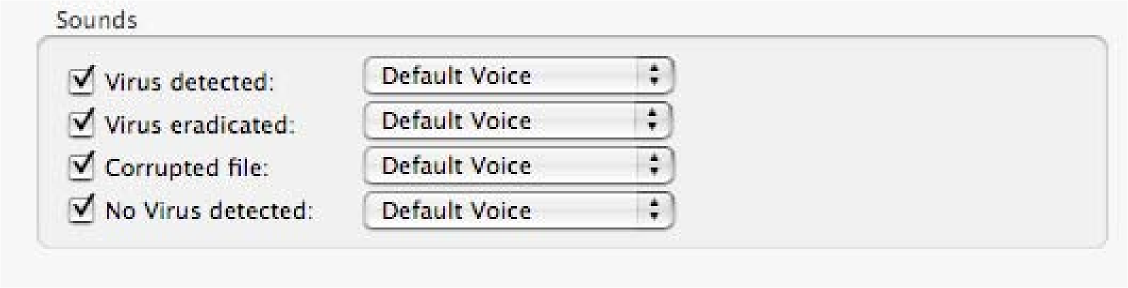
Repair and log only
If this is checked, Intego VirusBarrier X4 repairs infected files automatically and records the name of the infected file and the virus found in its log. It will not alert you, and you must check the log to see if any infected files are found.

Show alert
If this is checked, Intego VirusBarrier X4 displays an alert to inform you of the name of the infected file and the virus found. The alert asks whether you want to repair the infected file or not.

Sounds

Intego VirusBarrier X4 can play sounds to notify you of four events:

- Virus detected
- Virus eradicated
- Corrupted file
- No Virus detected



Sounds

☑ Virus detected: Default Voice

☑ Virus eradicated: Default Voice

☑ Corrupted file: Default Voice

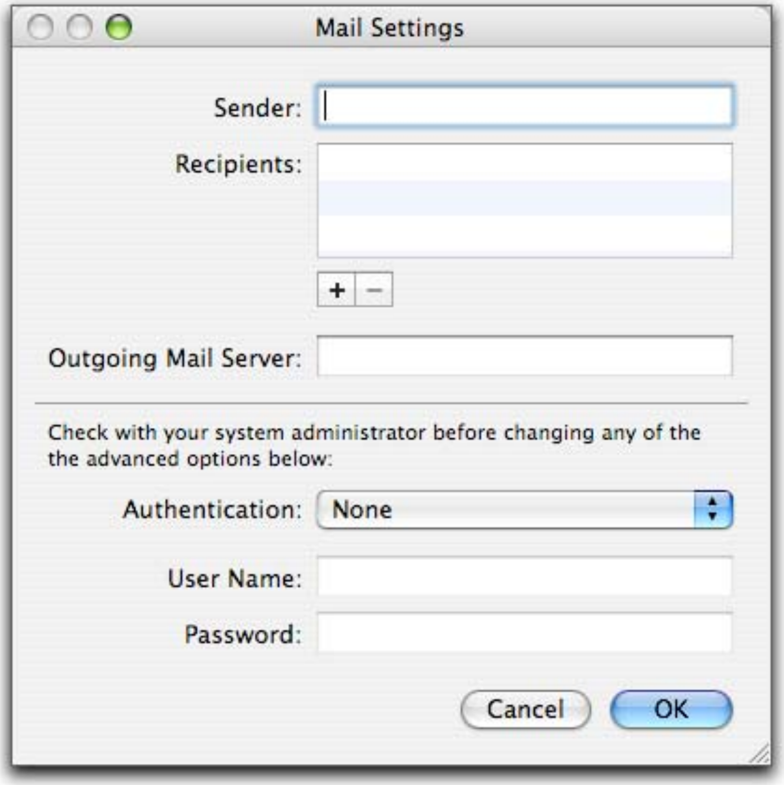
☑ No Virus detected: Default Voice

Choose from the default sounds, which use synthesized voices to inform you of these events, or select any other sound available on your computer by selecting it from the dropdown menu.

Options

Send e-mail

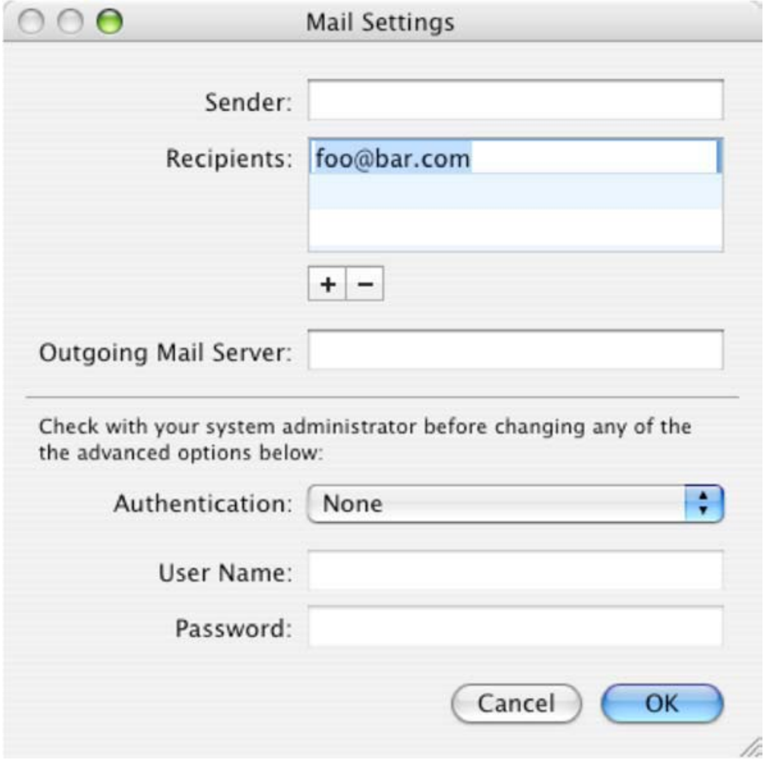
If Send e-mail is checked, Intego VirusBarrier X4 will automatically send an e-mail message to the recipients you specify when an alert is set off.



Check with your system administrator before changing any of the the advanced options below:

Authentication: None

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 adresses, 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.



Mail Settings

Sender:

Recipients: foo@bar.com

Outgoing Mail Server:

Check with your system administrator before changing any of the the advanced options below:

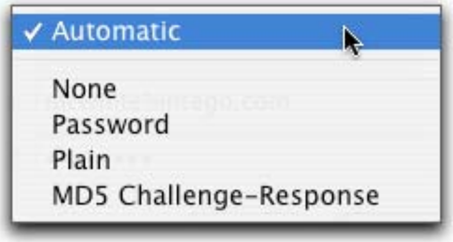
Authentication: None

User Name:

Password:

The lower half of the Mail Settings dialog deals with advanced options that VirusBarrier X4 may require to send e-mail.

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



✓ Automatic

None

Password

Plain

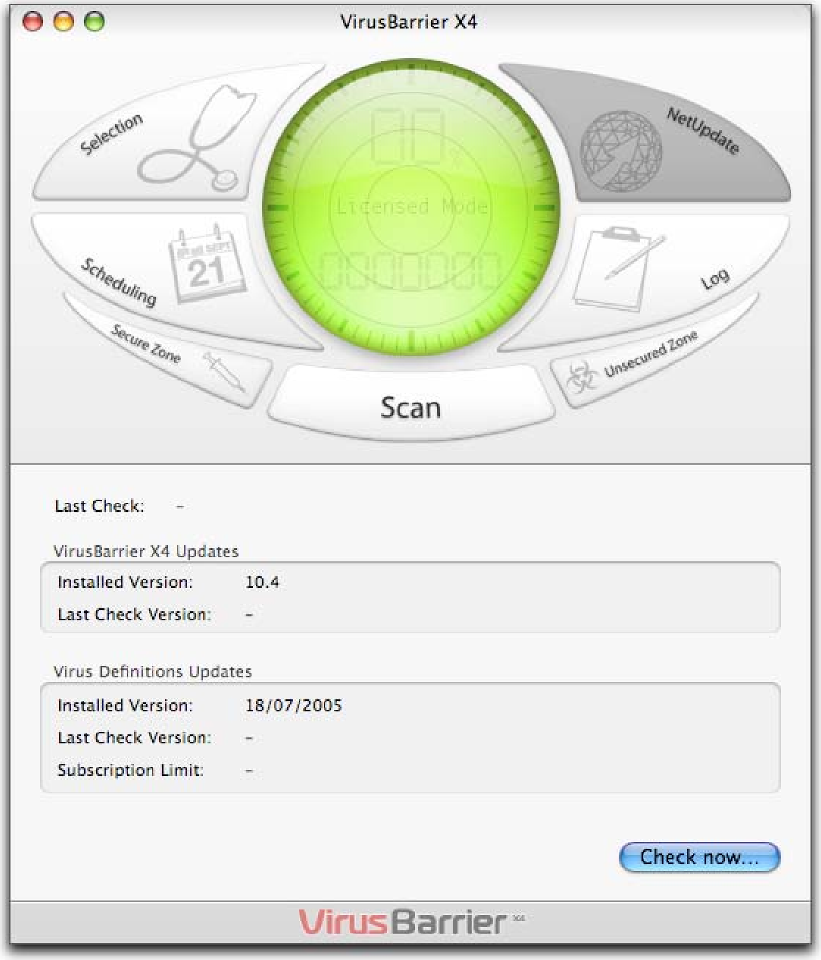
MD5 Challenge-Response

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.

NetUpdate

If you click the NetUpdate button, the NetUpdate panel opens. This drawer lets you check for updates, and also gives you information on the last time you checked, the version number of Intego VirusBarrier X4, and your subscription limit. When you purchase Intego VirusBarrier X4, you have access to minor updates and virus definition updates for one year from the date of purchase.

Intego VirusBarrier X4 also warns you when virus definitions are more than 45 days old.



Last Check: -

VirusBarrier X4 Updates

Installed Version: 10.4

Last Check Version: -

Virus Definitions Updates

Installed Version: 18/07/2005

Last Check Version: -

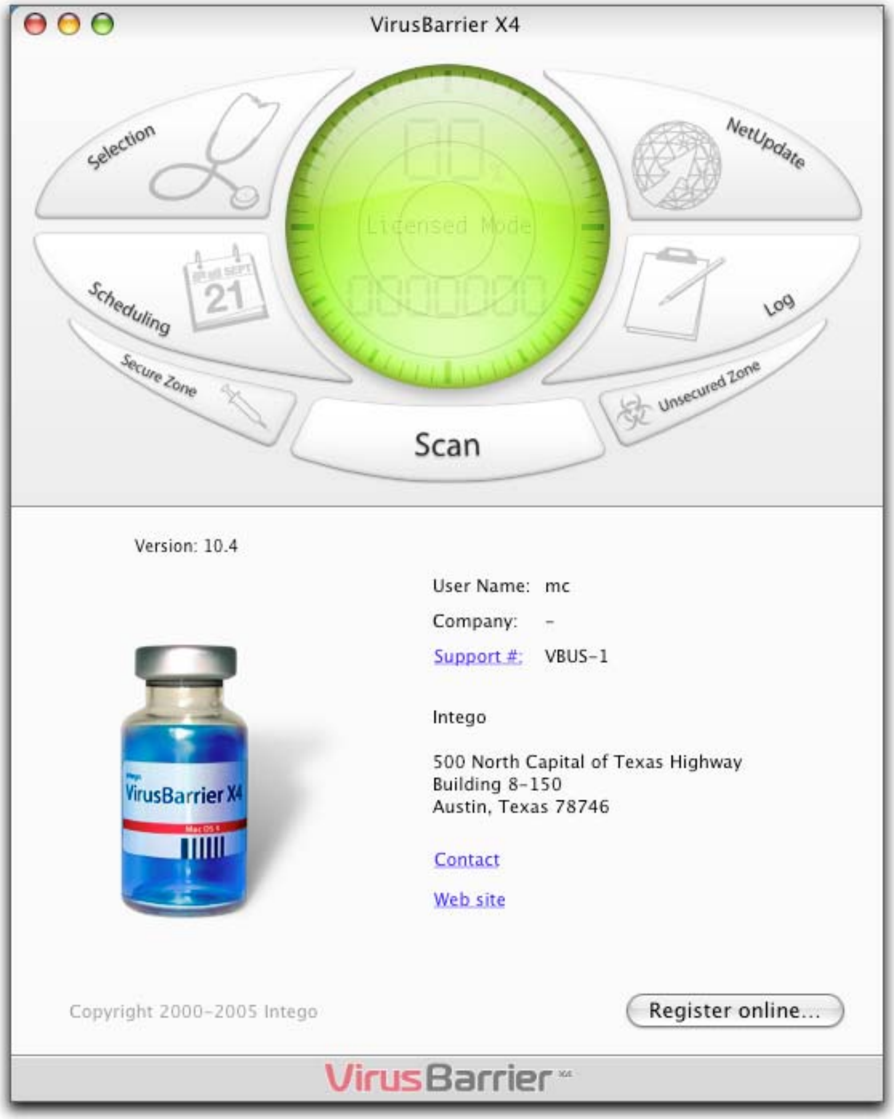
Subscription Limit: -

To check for updates, click the Check now… button. Intego NetUpdate will open and will connect to the Intego server to check for updates to the program or to virus definitions. When you purchase Intego VirusBarrier X4, you have access to virus definition updates for one year from the date of purchase.

You can set NetUpdate settings, such as choosing days and times for automatic updates, from the Intego NetUpdate Preferences Pane in the System Preferences.

For more on NetUpdate, and NetUpdate Settings, see the NetUpdate X4 manual.

About Intego VirusBarrier X4



Version: 10.4

User Name: mc

Company: -

Support #: VBUS-1

Intego

500 North Capital of Texas Highway
Building 8-150
Austin, Texas 78746

Contact

Web site

Copyright 2000-2005 Intego

To display the above panel, either click on the words VirusBarrier at the bottom of the Orb or go to the VirusBarrier X4 menu when Intego VirusBarrier X4 is running in the foreground, and select “About VirusBarrier X4”.

This panel gives information about Intego VirusBarrier X4, such as the version number, your support number (a number you will need for technical support), clickable links to Intego's web site and e-mail address, and Intego's address and telephone number.

In addition, clicking on the version number displays the precise build number, which is very helpful in handling technical support issues. You should quote this number in any messages to Intego's technical support staff.

If you wish to contact Intego with any questions, click the **Contact** link, and your e-mail program will create a new message to Intego, with a subject "message from client #" followed by your client number You can then type the text of your message, and send it to Intego.

If you need to contact Intego for technical support, click the **Support** # link. Your e-mail program will create a new message to Intego, with a subject "support message from client #" followed by your client number. Do not forget to quote your precise build number, which you can display by clicking on the Version number just above the VirusBarrier X4 icon. You can then type the text of your message, and click the send button to send it to Intego.

Clicking the **Register online…** button will take you to the registration page on the Intego web site. It is important to register your software, so Intego can keep you up-to-date on the latest information concerning Intego VirusBarrier X4 and its other products.

Clicking the **Web site** link will take you to the Intego web site.

7 - Diagnosis

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:

- unexpected error messages,
- your Macintosh "crashes" inexplicably,
- your hard disks or floppy disks are being read for no reason,
- your system seems to be running unusually slowly,
- your disk space seems to have reduced significantly, even though you have not added many files.

If your computer 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 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.

As a last resort, 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 8, Technical Support.

Basic precautions

Even though Intego VirusBarrier X4 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 X4 to run automatic backups.
- 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).
- Do not deactivate Intego VirusBarrier X4 unless you absolutely must: you do not need to deactivate VirusBarrier X4 to install new applications, even though most installation programs request this.
- Do not use pirated software: not only is it against the law, but also these programs often carry viruses, because they travel from one computer to another.

- 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 Intego VirusBarrier X4 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 Intego VirusBarrier X4 to protect your computer against viruses.

8 - Technical support

Help Menu

The complete Intego VirusBarrier X4 user's manual is available via the Help menu in Intego VirusBarrier X4. You may well find the answer you need in the manual, before resorting to contacting Intego for Technical Support.

Intego VirusBarrier X4 in Limited Mode

Intego VirusBarrier X4 will run in Limited Mode if, following an installation error or an incompatibility, parts of Intego VirusBarrier X4 have been temporarily disabled.

When in Limited Mode, Intego VirusBarrier X4 will not repair any files, nor will it allow virus definitions to be updated automatically, nor does it allow any but a predetermined range of preferences (to protect your system at all times –even when it is not fully functional).

However, it does continue to run and will scan data, and it also displays the fact it is running in Limited Mode in the Orb.

If you should find that Intego VirusBarrier X4 is running in Limited Mode, try restarting the machine. If that does not solve the problem, contact Technical Support as shown below.

Technical Support

Technical support is available for registered purchasers of Intego VirusBarrier X4. Do not forget to quote your precise build number, which you can display by clicking on the Version number just above the Intego VirusBarrier X4 icon in the About VirusBarrier X4 panel. To display this panel, open the Intego VirusBarrier X4 application and either click About VirusBarrier X4 in the VirusBarrier X4 menu or double-click on the words VirusBarrier at the bottom of the Orb.

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 sendvirus@intego.com.

Alternatively you can highlight them in the Finder, Control-Click on them to highlight the Intego VirusBarrier X4 Contextual Menu, and select the last option, which will send the data to them, without your even having to open your e-mail program.

9 - Appendix

Glossary

Antivirus – An antivirus is 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 – An archive is a file that contains several files, and is usually compressed, to save space. The standard for compression on the Macintosh is Stuffit.
Boot – Booting a computer means starting it up. 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.
Desktop File – Desktop files are invisible files that keep track of which icons go with which types of files and applications. Every volume, or disk, on your computer has invisible desktop files, called, under Mac OS 9, Desktop DB and Desktop DF. Certain old viruses target desktop files, since your computer automatically reads these files whenever you insert any removable media into a drive.
Extension – Extensions (also called inits), like control panels, are part of the Macintosh operating system. They add functions to the basic system, or are used as drivers for specific hardware. There are two types of extensions: those that get loaded along with the system when you boot your computer, and those that are called upon when needed by the system.
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.
Hoax – A hoax is a virus warning that is not true. There are many hoaxes that circulate by e-mail, and they all talk of getting a virus by merely reading an e-mail message.

INIT – An init is another name for an extension. This term comes from the fact that these files are initialized when the computers boots.

Macro – A macro is 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 macro command is 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.

Resource – Macintosh files have two parts: a resource fork and a data fork. The resource fork can contain such elements as icons, code, or other instructions for applications. Some viruses hide in resources, or corrupt or change resources.

Removable Media –Any data storage media that is inserted into a drive, such as a CD-ROM, a DVD, a Zip cartridge, or a floppy disk.

Strain – A strain of a virus is 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 which, in reality, hides some sort of 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 – 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. They then use these host files to spread when the files are open or run.

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.