Welcome to PC-cillin 2002

Trend Micro PC-cillin 2002 provides next generation secure computing for today’s personal computers. More than just antivirus software, PC-cillin includes a Personal Firewall, Site filter, Internet mail scanning, and more for all your secure computing needs.

Designed for the home or small office user, the friendly interface lets you quickly become familiar with all the powerful features of the software. However, the program behind the interface uses the latest technology and provides you with protection from the nastiest viruses, sneakiest Trojans, and the meanest hackers. With firewall technology, the Trojan System Cleaner tool, and more, PC-cillin gives you peace of mind whenever you connect to the Internet. And now that Trend Micro's *award winning ICSA approved* scan engine also includes ScriptTrap™ technology, personal computing has never been more secure.

Here's what PC-cillin will do "straight out of the box":

- Checks for viruses every time you open, copy, move, or save a file
- Protects against downloading infected files from the Internet or FTP sites
- Guards against malicious Java™ applets and Microsoft ActiveX™ controls while surfing the Web
- Detects and cleans live Trojans installed on your system
- Monitors your Microsoft Word® and Microsoft Excel® sessions for macro viruses, using MacroTrap™
- Scans and cleans all files on your hard drive
- Scans all program files for viruses
- Checks all your saved documents for macro viruses

Here's what you can do with just a click of a button:

- Scan every file on your system and clean any infected files
- Scan any file from Windows Explorer or My Computer by right-clicking the file icon
- Scan floppy disks and clean any infected files
- Check all of your Word and Excel document(s) for macro viruses
- Scan your email attachments as they are being downloaded from an Internet (POP3) mail server
- Protect your computer against attacks from the Internet using a combination of cloaking and firewall functions
- Make whatever Web sites you want "off limits" to other users of the computer
- Protect your handheld devices with updated Personal Digital Assistant (PDA) virus pattern files

Personal Firewall

PC-cillin 2002 provides secure Internet computing with its new Personal Firewall feature. Easy to operate, the Personal Firewall protects your computer from unwanted Internet connections. The Personal Firewall is ideal for computers using always-on broadband (DSL, cable modem) connections, or for those computers that are often online. Even computers that only connect to the Internet for short periods of time are still vulnerable to hacker attacks and need protection.

With adjustable security levels, a trusted site list, and a port blocking function, the Personal Firewall gives you the control to keep your computer safe from malicious code like spyware and Trojan horses. The Personal Firewall is comprised of the following components:

- **Cloaking:** Prevents your computer from being found. Cloaking hides the entry points (ports) of your computer making it appear to be disconnected from a network. Hackers using techniques like NetBIOS browsing, port scanning, or ICMP packet special processing will be unable to locate your computer.
- **Firewall:** Provides a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic coming into your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer. The firewall protects against attacks hackers commonly use including: *Ping of Death*, *IP conflict*, *SYN flooding*, and others.
- **Trojan Backdoor Blocking:** If a hacker has already broken into your system, he or she could have installed a Trojan (small hidden program) onto your computer (unlike viruses, Trojans do not replicate themselves, but can still wreak havoc on your system). To avoid being traced, the hacker can then use your computer to attack other computers. The Trojan Backdoor Blocking function prevents hackers from using your computer by blocking *Back Orifice, Back Orifice 2000, Net Bus, Deep Throat* and other known back door programs.

There may be Web sites that you know are safe and will not attack your computer. Using the Trusted Sites function, the Personal Firewall lets you add

these safe sites to a list. Your computer can connect to any Web site on this list because they will not be filtered.

See also:

Enabling Your Personal Firewall

About the Personal Firewall security level settings

Adjusting the Personal Firewall security level settings

About Trojans

How Trojans cause damage

PC-cillin for Wireless

Malicious code and other threats hidden inside files, email, or on the Web can enter your Palm, Pocket PC, or EPOC device during beaming, synchronization, or Internet access. Trend Micro PC-cillin for Wireless provides portable, easy-to-use antivirus security for wireless devices; to defend against potential threats. Best of all, PC-cillin for Wireless is bundled with PC-cillin 2002 providing you with secure computing on both your desktop and handheld.

See also:

About PC-cillin for Wireless

Updating PC-cillin for Wireless

Selecting PDA OS type

Installing PC-cillin for Wireless

Trojan System Cleaner

PC-cillin automatically runs the Trojan System Cleaner (TSC) during initial installation, and every time Real-time Scan runs. The TSC detects the activity of Trojan horse programs, recovers system files which are modified by Trojans, stop their processes, and deletes files dropped from Trojans.

Traditional antivirus products only scan "files", they open files and check for virus code. But they don't check and clean system files and can't clean or delete Trojan horse programs (also known as *Trojans*) if it is already run in the system.

The TSC uses patterns to define how to clean a Trojan. These patterns are built into Trend Micro virus pattern files and are kept up-to-date. Whenever TSC is executed, it finds the newest pattern file and tries to read Trojan clean section from the pattern file.

See also:

Running the Trojan System Cleaner

About Trojans

How Trojans cause damage

ScriptTrap Technology

With the addition of ScriptTrap technology, PC-cillin now more than ever provides rock-solid protection for your computer. PC-cillin not only guards against harmful known script-based viruses ("I Love You" and "Anna Kournikova"), but can also protect your PC from new, unknown script-based threats.

Using the following processes, ScriptTrap automatically scans for scripting viruses based on "what they do" rather than how they are written:

- **lexical analysis**- divides the script's source code into components, called tokens, based on punctuation and other keys.
- **semantic parsing**- attempts to determine the meaning of each component.

Emergency Lock

PC-cillin also includes an Internet Emergency Lock function that lets you immediately disable all Internet activity if you suspect an attack. Enabling the Emergency Lock function immediately stops all traffic to and from the Internet.

See also:

Activating the Emergency Lock

User Interface

Designed for the home or small office user, the program's friendly interface quickly familiarizes you with the powerful features of PC-cillin 2002. The interface now includes a Simple and Standard mode. Using a tab interface, you can easily switch between the two modes.

Simple mode: Perform common PC-cillin tasks such as: view a simplified version of your system status, and scan all drives. In addition, you can update and register your software.

Standard mode: Access more advanced PC-cillin 2002 functions including: viewing your system status in more detail, selectively scanning folders, synchronizing your PDA, quarantining files, and viewing logs. In the Standard mode, as in the Simple mode, you can also update and register your software.

See also:

About Simple mode
About Standard mode

About Intelligent Update

Intelligent Update automatically searches for and downloads the latest files for PC-cillin 2002. This includes pattern and program files for both the main program and PC-cillin for Wireless. In addition, Intelligent Update ensures you have the latest Personal Firewall rules. This powerful function keeps PC-cillin and all its components updated; offering you maximum protection with minimal user intervention.

Once your computer is running, PC-cillin checks for an Internet connection. When this feature is enabled and your computer is online, PC-cillin automatically connects to the Trend Micro server to check if the latest update is available. If newer components are on the server, a pop-up window appears asking if you want to start downloading. If you choose not to download immediately, the pop-up window re-appears in 10 minutes.

See also:

About Virus Pattern Files

Viewing pattern file and scan engine information

Updating PC-cillin 2002

Updating PC-cillin for Wireless

Enabling Intelligent Update

Scheduling Intelligent Update

New product registration method

PC-cillin 2002 offers a new way to register your software online. On our Registration Web page, simply type your name and email address in the appropriate fields, receive your License Key via email, and insert it into the correct field on the Register Now screen of the PC-cillin window.

Registration only takes a few minutes and Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

See also:

Upgrading your trial version software

Registering your software

Can I install PC-cillin 2002 on another computer?

What if I lost my serial number?

What happens to my License Key if I reinstall my operating system?

Registering your software

Take a few minutes to register your software online and receive the benefits. Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

To register your software:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Register link. The Register Now screen appears.
3. Confirm that your full version serial number already exists and click Register Now. The Register Web page loads in your browser.
4. On the Register Web page in the appropriate fields, type your name and email address.
5. Type your email address again to confirm it's the correct address.
6. Click Send. A Confirmation Web page loads and a License Key is sent to the email address you just typed.
7. Copy the License Key from the Web page or email and paste it under Step 3 in the Register Now screen.
8. Click Finish.

Congratulations! You have registered your software and can now use the full functionality of PC-cillin 2002 and receive the benefits.

See also:

New product registration method

Upgrading your trial version software

Can I install PC-cillin 2002 on another computer?

What if I lost my serial number?

What happens to my License Key if I reinstall my operating system?

Upgrading your trial version software

Upgrade your software and register online to take full advantage of PC-cillin 2002. If you are still using the trial version after 30 days, the virus scanning services become disabled. Upgrading your software to the full version and registering enables you to use all PC-cillin 2002 functions.

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

To upgrade your trial version software:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Register link. The Register Now screen appears.
3. Under Step 1 on the Register Now screen, type your serial number.
4. Click Upgrade Now.

   Congratulations! You have upgraded your trial verson software to the full version. You should now continue and register your software.

5. Click Register Now. A Web page appears.
6. On the Register Web page in the appropriate fields, type your name and email address.
7. Type your email address again to confirm it’s the correct address.
8. Click Send. A Confirmation Web page loads and a License Key is sent to the email address you just typed.
9. Copy the License Key from the Web page or email and paste it under Step 3 in the Register Now screen.
10. Click Finish.

Congratulations! You have registered your software and now can use the full functionality of PC-cillin 2002 and receive the benefits.

See also:

Enabling the Real-time Monitor

The Real-time Monitor watches over your system and detects viruses as they arrive at your computer. Each time you open, copy, save, or move a file, the Real-time Monitor ensures that the real-time scanner performs a quick check of the file. Because it works in the background, it doesn't interfere with your normal daily computing and won't distract you.

In addition, the Real-time Monitor lets you quickly perform PC-cillin commands.

To enable the Real-time Monitor:

1. Click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor. The Real-time Monitor appears in the system tray (located in the lower-right corner)
2. Right-click the Real-time Monitor. A pop-up menu appears.
3. You can choose the following:

- **Startup PC-cillin**- Displays the PC-cillin window.
- **Emergency Lock**- Sets the Emergency Lock, which immediately halts all network activity.
- **Real-time Monitor**- Enables the Real-time Scan function. If there is a check mark beside Real-time Monitor, Real-time Scan is enabled.
- **Configuration**- Displays the Settings window.
- **Real-time Status**- Displays Real-time scan information, including the pattern file version and the last scanned file.
- **Exit**- Disables the Real-time Monitor and asks you if you also want to stop real-time scanning.

See also:

About the Real-time Monitor
Starting the Real-time Monitor

Scanning a single file

PC-cillin can easily run a quick scan of any file. PC-cillin scans the file types and executes the necessary virus actions according to the Manual Scan settings.

For the quickest results, use one of the following methods.

To scan a single file using Windows Explorer, do one of the following:

- Right-click the file, and then click PC-cillin.
- Right-click the file, and then click Properties. Click the Virus Property tab. PC-cillin scans the file.

To scan a single file, "drag" the file(s) onto the PC-cillin window.

See also:

Scanning folders

About virus scan actions

About Manual Scan

Scanning folders

With PC-cillin you can scan the entire contents of a folder. PC-cillin scans the file types and executes the necessary virus actions according to the Manual Scan settings.

For the quickest results, do one of the following:

To scan a folder using Windows Explorer, right-click the folder you want to scan and click PC-cillin.

To scan a folder, "drag" the folder you want to scan onto the PC-cillin window.

See also:

Scanning a single file

About virus scan actions

About Manual Scan

Scanning all drives

Scan all drives to make sure your system is virus-free. With one click, PC-cillin provides a fast and easy way to scan all drives for infected files that are connected to your computer.

To scan all drives:

1. On the PC-cillin window, click the Simple tab. The Simple mode menu appears.
2. Click the Scan All Drives link. The Scan Files dialog box appears and PC-cillin begins scanning. To stop scanning, click the Stop button. A confirmation message box appears. Click Yes to stop.

Note: PC-cillin scans the file types and executes the necessary virus actions according to the Manual Scan settings.

See also:

[About Manual Scan]
[Scanning folders]
[Scanning a single file]

Enabling your Personal Firewall

Enable your Personal Firewall so you can connect to the Internet without worrying about someone invading your computer. The Personal Firewall protects you from hackers trying to damage files, steal personal information, or create mischief.

To enable your Personal Firewall:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Security Level link. The Security Level screen appears.
4. Select the *Enable Personal Firewall* check box.
5. Click Apply.

See also:

About Personal Firewalls
About the Personal Firewall security settings
About trusted sites
About blocked ports
Activating the Emergency Lock
About Trojans
How Trojans cause damage

Activating the Emergency Lock

If you suspect an attack originating from the Internet, use the Emergency Lock function to quickly halt all Internet activity. Activating the Emergency Lock immediately stops all traffic to and from the Internet.

To activate the Emergency Lock:

1. Make sure the Real-time Monitor is displayed in the system tray. If not, click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor.
2. In the system tray, right-click the Real-time Monitor icon and click Emergency Lock. Emergency Lock is selected (a check appears beside the name). The locks shuts and all Internet activity is stopped. To deactivate the Emergency Lock, make sure there is no check beside the name.

Notes:

- You can also activate the Emergency Lock if a real-time scan detects a virus. Simply click Emergency Lock on the dialog box that appears.
- If the Real-time Monitor is already displayed in the system tray and you try to open the Real-time Monitor, the Real-time Monitor dialog box appears.

See also:

About the Real-time Monitor
Starting the Real-time Monitor

Running the Trojan System Cleaner

To scan for and destroy Trojan horse programs, PC-cillin automatically runs the Trojan System Cleaner during initial installation, and every time Real-time Scan starts. However, you can also manually run the Trojan System Cleaner.

To manually run the Trojan System Cleaner:

1. Click Start > Programs > Windows Explorer. The Windows Explorer appears.
2. Locate the folder where you installed PC-cillin 2002 (for example, the default location is; C:\Program Files\Trend Micro\PC-cillin 2002).
3. Double-click the Tsc.exe file. The Trojan System Cleaner runs.

See also:

Trojan System Cleaner

About Trojans

How Trojans cause damage

Scanning for PDA viruses

To scan for viruses on your PDA, simply tap the Scan button on your PDA. After completion of the scan, you are shown a list of viruses that were found on your computer. You can also see the number of files scanned.

See also:

About PDA viruses

Dealing with PDA viruses

Getting PDA virus information

Virus Prevention

Take the following measures to protect your computer from infection:

- **Use the latest virus pattern file**- Register your software and download the latest versions of the PC-cillin pattern files and program components to ensure PC-cillin uses the latest antivirus technology.
- **Beware of suspicious email attachments**- Email is the most common way viruses and malicious code spread. If an email is sent to you by a stranger, you shouldn't save or run any files attached to the email. However, regardless of who sent you the email, be suspicious of email attachments that contain executable files (for example .EXE, .COM).
- **Enable Real-time Scan**- Real-time scanning provides constant protection against viruses. With real-time scanning enabled, you reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), we recommend that you always keep real-time scanning enabled.
- **Set scheduled scan tasks**- Scan tasks are a quick and easy way to perform a variety of scans. Using scan tasks automates routine antivirus maintenance procedures on your desktop and improves antivirus management efficiency and control over antivirus policy. For more information, refer to the online help topic About Scan Tasks.
- **Keep informed**- Regularly visit the Trend Micro Web site (www.antivirus.com) for the latest virus information and security alerts. In addition, you can learn more about viruses by accessing the online Trend Micro Virus Encyclopedia.

See also:

Registering your software

What happens if a virus is detected

With the amount of viruses already released and the number of new ones being created, it is very likely you will encounter a virus. When PC-cillin detects a virus either by Real-time Scan, Manual Scan, or an Internet mail scan, PC-cillin notifies you of the virus and the action it takes. The actions for Real-time Scan, Manual Scan, or Internet mail scan depend on the settings you have configured for each scan, respectively. However, the default action for all scans is *Clean*. This simply means if a file becomes infected, PC-cillin first attempts to clean the file.

See also:

About virus scan actions

About Manual Scan

About Real-time Scan

About Internet mail scan

About scan tasks

Actions to take if PC-cillin cannot clean file

What do you do if you have updated your pattern files, scan engine and program files and find that an infected file still cannot be cleaned? This depends on the actions you have set for the different PC-cillin scans (Real-time Scan, Manual Scan, Internet mail scan). The default Real-time and Manual Scan action for files that cannot be cleaned is *Quarantine*. This means PC-cillin will move the file to the Quarantine folder. Files placed in the Quarantine folder are isolated and rendered harmless. After you quarantine the file you have several options, for example, after the next pattern file update you can clean the file. You can also restore it, send it to Trend Micro for analysis and manually cleaning, or ultimately you can still delete it if you choose.

The following provides further information about alternate methods on how to proceed for different types of viruses.

Important: Infected files that cannot be cleaned may be important system files. If you choose to quarantine or delete a file, it might cause a system error or failure to boot up the system. You need to be careful what the file is when you choose to take these actions.

Trojan horses (Virus name: Troj_xxx)

Because Trojan horses do not infect other files, but rather destroy or steal information from your computer, there is no way to clean the file. The only way to clean a Trojan is to delete the actual Trojan horse file.

Compressed files

While the Trend Micro scanning engine can detect viruses within compressed files, it cannot clean the files inside of a compressed archive beyond the second layer of compression. To clean a virus in a deeper layer of compression, you must first decompress the file.

To clean a compressed file:

1. Disable PC-cillin’s real-time scanning function so that it will not interfere with the decompression process.
2. Use an archive utility (for example, WinZip) to extract the files from the compressed file.
3. Start PC-cillin's real-time scanning function.
4. Run the main program. You can now manually scan and clean the infected files that were extracted in the second step.

Insufficient disk space or write-protected diskettes

PC-cillin creates a backup file, *.rb0, before attempting to clean an infected file. This is to prevent files from being corrupted if the cleaning fails. You need to provide enough disk space or you have to copy the infected files to a hard disk drive before attempting to clean the files. If the disk is write-protected, make it writeable before attempting to clean the file.

Password-protected files

If the infected file is password-protected (for example, a password-protected ZIP or Word file), PC-cillin will not be able to detect or clean it. Please disable the password-protection before attempting to scan or clean the file.

PE-type virus infection (Virus name: PE_xxxx)

Since PE-type viruses (Portable Executable: standard Win32 file format) always stay in memory, the virus may not be completely cleaned.

To clean a PE-type virus:

1. Boot your computer with the rescue disk labeled *Emergency Boot Disk (Disk 1)*.
2. Insert the PC-cillin rescue disk labeled *PCSCAN Files Disk (Disk 2)* into the A:\drive and at the DOS command prompt type:

   A:\>PCSCAN /V/C

Follow the onscreen instructions. You can now start scanning and cleaning the viruses.

Note: If you do not have emergency rescue disks, refer to the Creating rescue disks procedure.

See also:

About virus scan actions

About Manual Scan

About Real-time Scan

About Internet mail scan

About quarantined files

About scan tasks

About rescue disks

About Virus Pattern Files

To detect and clean viruses, PC-cillin uses an extensive database of virus "signatures," (inert sections of virus code) that hold the signatures of thousands and thousands of viruses.

As new viruses are written, released onto the public, and discovered; Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. By some estimates, thousands of new viruses are created each year, a rate of several each day. In fact, virus making has become so easy that free "virus kits" are even available over the Internet from rogue Web sites. Therefore, it is very important to keep the virus pattern file up to date.

To keep up with the onslaught of viruses, Trend Micro publishes a new virus pattern file weekly (available for download from our Web site). Both home and office users should consider scheduling weekly updates. Virus pattern file updates are available for a year to registered PC-cillin users.

The virus pattern file is located in the Trend Micro PC-cillin folder on your computer and will have a name such as Lpt$vpn.120. The number represents the pattern version. If more than one virus pattern file exists in the folder, the scan engine only uses the latest.

See also:

Viewing pattern file and scan engine information
Updating PC-cillin 2002
Updating PC-cillin for Wireless
About Intelligent Update

Viewing pattern file and scan engine information

It is important to make sure your pattern files and scan engine are kept current. Using the latest versions of these PC-cillin components ensures you have the best virus protection available for your computer. To confirm you have the latest updates, you can view your current pattern file and scan engine version.

To view pattern file and scan engine information, on the PC-cillin menu bar, click About. The About PC-cillin 2002 dialog box appears displaying the following information:

- Program Version, Engine Version, Pattern Version
- Serial Number, User name, Company

See also:

About Virus Pattern Files
Viewing your PC-cillin serial number
Updating PC-cillin 2002
Updating PC-cillin for Wireless
About Intelligent Update

Updating PC-cillin 2002

To protect your computer against the latest threats, you need to regularly update your program files, scan engine, and pattern files. Since new viruses are rapidly being discovered, it is crucial to regularly update your virus pattern files. In addition, as new viruses appear, and existing ones evolve, it becomes necessary to update certain program files and add new functionality to the scan engine. Updating your scan engine ensures PC-cillin can act on the new instructions in the virus pattern and successfully identify and clean the virus.

Before you can update PC-cillin you must register your software.

To update PC-cillin 2002:

1. On the PC-cillin window, click the Simple tab. The Simple mode menu appears.
2. Click the Update Now link. The Upgrade Now screen appears. The meter displays the update progress. If you need to halt the update, click Stop. To continue updating, click Update.

See also:

Registering your software

About Virus Pattern Files

Viewing pattern file and scan engine information

Updating PC-cillin for Wireless

About Intelligent Update

Updating PC-cillin for Wireless

To ensure protection against the latest threats on your PDA, you need to regularly update your PC-cillin for Wireless pattern and program files. PC-cillin can download the latest PC-cillin for Wireless files and you can synchronize the existing files on your PDA.

Updating PC-cillin for Wireless involves verifying your PDA type, making sure your PDA type is selected for synchronizing with your PDA, and updating your pattern and program files with Intelligent Update.

To update PC-cillin for Wireless:

1. On the Settings window, click the Program Update link the menu expands.
2. Click the Update PDA link. The Update PDA screen appears.
3. Make sure your PDA type is selected. If it is not, select your PDA type check box (for example Palm OS, Pocket PC, or EPOC), and then click Apply.
4. On the menu bar, click Go Main. The PC-cillin window appears.
5. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
6. Click the Sync PDA link. The Sync PDA screen appears.
7. Verify your PDA type is selected and under the Standard tab, click the Update link. The Update Now screen appears.
8. Click the Update button. PC-cillin begins to update.
9. After the update has finished, click the Sync PDA link.
10. Place your PDA into its cradle, and then click Sync Now.

Note: You must connect your PDA device to your PC before executing Sync Now. Do not use any applications or remove your PDA device during synchronization.

See also:

Updating PC-cillin 2002

About PC-cillin for Wireless

Selecting PDA OS type

About Intelligent Update

Accessing PC-cillin online help

PC-cillin’s online help provides comprehensive coverage of all the functions and features of PC-cillin 2002. Quickly find the answers to all of your PC-cillin questions. The online help is also a handy reference and provides frequently asked questions and virus information.

To access PC-cillin online help, on the PC-cillin menu bar, click Help.

In addition, depending on the screens or dialog boxes that appear, you will see Help buttons. Click these Help buttons to view relevant help information (context-sensitive help) based on what you are currently viewing.

See also:

Accessing PC-cillin online help

Viewing pattern file and scan engine information

Viewing your PC-cillin serial number

Quickly view your PC-cillin serial number if you ever need to provide it. For example, if you have to contact technical support for help with an issue or re-install PC-cillin 2002, you need your serial number.

To view your PC-cillin serial number, on the PC-cillin menu bar, click About.

See also:

Accessing PC-cillin online help

Viewing pattern file and scan engine information

Contacting Technical Support

About rescue disks

Certain types of boot viruses can prevent your computer from booting normally. To clean these viruses you need to start your computer from a clean disk and not the infected hard drive. A "rescue disk" is a bootable floppy disk that PC-cillin can create if you are running Microsoft Windows 95/98/Me.

Rescue disks should be write-protected after they are created. You need multiple disks to create the complete set of rescue disks.

(Disk 1) Emergency Boot Disk: Contains files necessary to start your computer. Use to start your computer if a boot virus has infected your computer and you cannot start your computer normally.

(Disk 2) PCSCAN Files Disk: Contains the scan engine. Use with the Pattern File disks to detect and clean viruses located in the boot sector of your computer.

(Disks 3 and others) Pattern File Disks: Contains pattern files so you can detect the latest viruses. Use with the PCSCAN Files disk to detect and clean viruses located in the boot sector of your computer.

Important: *Do not restart your computer using rescue disks that were created for an earlier version of PC-cillin--this can result in data loss.*

See also:

Creating rescue disks

Updating rescue disks

Cleaning boot viruses

Boot viruses

Creating rescue disks

Before creating your rescue disks, make sure you have a writing utensil to label the disks. You need multiple disks to create a complete set of rescue disks.

If you've already got a set of rescue disks from a previous version of PC-cillin, you should nevertheless create a new set after installing PC-cillin 2002. Likewise, if you created your rescue disks under Windows 95 and have subsequently upgraded to Windows 98, you need to create a new set of rescue disks. Of course, you can re-use your old floppies for the new disks. All data on the old disks will be lost in the creation of the new disks.

To create your rescue disks:

1. Obtain some disks; insert one into the floppy drive of your computer.
2. Insert the Trend Micro PC-cillin 2002 CD into the appropriate drive.
3. Click Start > Programs > Trend Micro PC-cillin 2002 > Create the Rescue Disks. A message box appears asking for confirmation.
4. Click Yes. The Creating the rescue disks dialog box appears. You can choose where the rescue disk files are extracted or just use the default location. To change where the rescue disks files are extracted, click Change and browse to a different folder.
5. Click Next. PC-cillin extracts the rescue disk files to the specified location.
6. Click Complete Rescue Disk set, and then Click Next.
7. Make sure the Target drive is correct and click Next. The Format dialog box appears.
8. Choose your format type (we recommend Full) and click Start. The disk starts formatting.
9. When the formatting is finished, click Close. The Format Dialog closes and PC-cillin starts copying the files to the disk.
10. As each floppy is finished, remove it and immediately label it. You should also write-protect it by sliding up the plastic button that is in the upper left hand corner of the back of the disk. The disk is write-protected when you can see through both squares in the upper corners. Creating the rescue disks takes about 10 minutes.
11. Repeat the procedure for each disk, starting from the formatting step.

12. Click Finish.

Important: *You cannot make rescue disks on a machine infected with a boot virus. Be sure to clean (or delete) any viruses that have been detected.*

See also:

About rescue disks

Updating rescue disks

Cleaning boot viruses

Boot viruses

Updating rescue disks

Rescue Disk 3 and others contain pattern files that must be kept updated to provide the most effective virus scanning.

To update the pattern files on your rescue disks:

1. Insert the first pattern file disk into the floppy drive of your computer.
2. Insert the Trend Micro PC-cillin 2002 CD into the appropriate drive.
3. Click Start > Programs > Trend Micro PC-cillin 2002 > Create the Rescue Disks. A message box appears asking for confirmation.
4. Click Yes. The Creating the rescue disks dialog box appears.You can choose where the rescue disk files are extracted or just use the default location. To change where the rescue disks files are extracted, click Change and browse to a different folder.
5. Click Next. PC-cillin extracts the rescue disk files to the specified location.
6. Click Pattern Disk only, and then Click Next.
7. Make sure the Target drive is correct and click Next. The Format dialog box appears.
8. Choose your format type (we recommend Full) and click Start. The disk starts formatting.
9. When the formatting is finished, click Close. The Format Dialog closes and PC-cillin starts copying the files to the disk.
10. As each floppy is finished, remove it and immediately label it. You should also write-protect it by sliding up the plastic button that is in the upper left hand corner of the back of the disk. The disk is write-protected when you can see through both squares in the upper corners. Creating the rescue disks takes about 10 minutes.
11. For each disk, repeat the procedure starting from the formatting step.
12. Click Finish.

Important: *Do not restart your computer using a rescue disk that was created for an earlier version of PC-cillin -- data loss can result. Nor should you boot from rescue disks created for one operating system (Windows 95) if you are running a different one (Windows 98, Windows Me).*

See also:

About rescue disks

Creating rescue disks

Cleaning boot viruses

Boot viruses

Cleaning boot viruses

Boot sector viruses are especially troublesome (and dangerous) viruses because they occupy a sensitive part of the hard drive, the boot sector, and load into memory whenever the system is started. From memory, they spread easily to any files that are subsequently opened and floppy disks that are used.

To clean a boot virus:

1. Shutdown your computer and turn off the power.
2. Insert the rescue disk labeled *Emergency Boot Disk (Disk 1)* in the floppy drive of your computer.
3. After waiting a few seconds, turn your computer on. Make sure your computer boots from the floppy drive (refer to your BIOS manual for instructions).
4. Insert the *PCSCAN Files Disk (Disk 2)* and at the DOS prompt, and type the following:

   pcscan /V /C

5. Press Enter.
6. When prompted, insert the Pattern File Disk 1 and press Enter.
7. When prompted, insert the Pattern File Disk 2 and press Enter.
8. When prompted, insert the Pattern File Disk 3 and others and press Enter.

   The last command tells PC-cillin to scan and clean all files on all drives, including the boot sector.

Important: *Boot viruses spread easily. If PC-cillin detected a boot virus, it is very likely that one or more of your floppy disks are also infected. Be sure to run the Floppy Scan task and check all your floppies for viruses.*

See also:

About rescue disks
Creating rescue disks
Updating rescue disks
Boot viruses

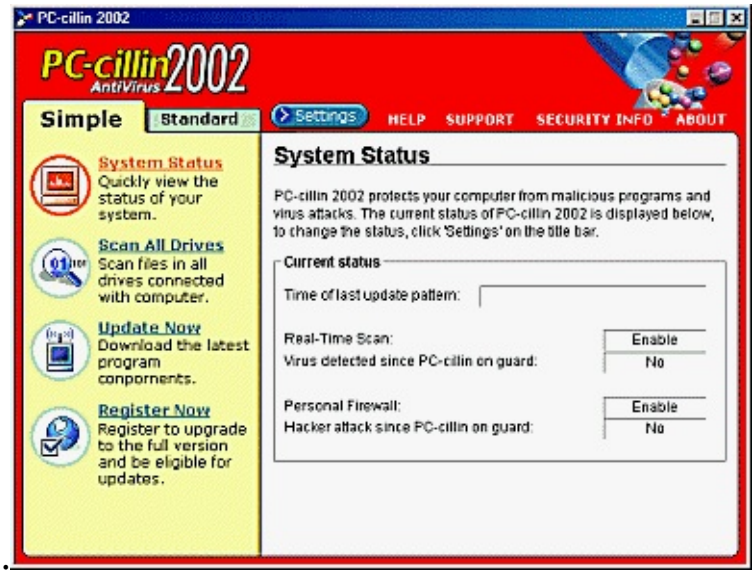
Viewing the PC-cillin window

View the PC-cillin window to rapidly carry out your actions. On the PC-cillin window you can access both Simple and Standard modes as well as the menu bar. View the following image to become more familiar with the PC-cillin window.

To view the PC-cillin window, do one of the following:

- Click Start > Programs > Trend Micro PC-cillin 2002 > PC-cillin 2002.
- In the system tray, right-click the Real-time Monitor and click Startup PC-cillin.

The PC-cillin window appears



See also:

Viewing the Settings window
About the Real-time Monitor
Starting the Real-time Monitor

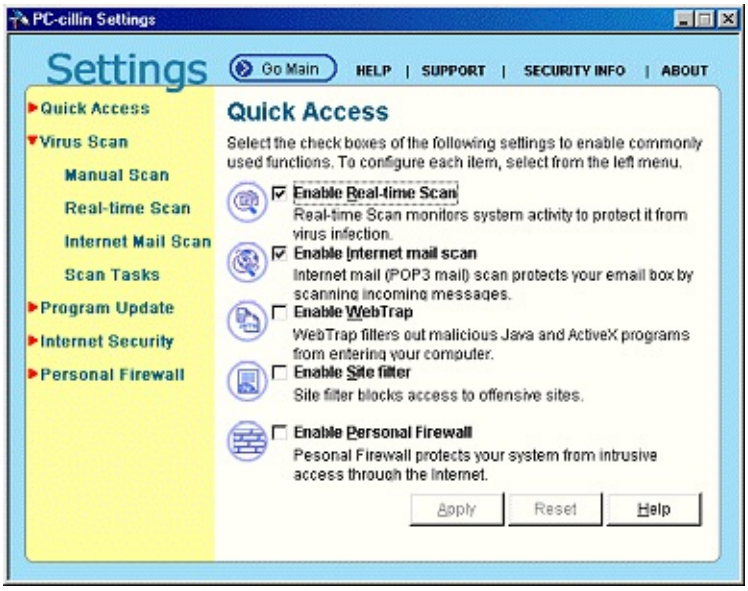
Viewing the Settings window

While the PC-cillin window provides the quick interface to rapidly carry out your actions, the Settings window provides the interface where you define the actions. View the following image to become more familiar with the Settings window.

To view the Settings window, do one of the following:

- Click Start > Programs > Trend Micro PC-cillin 2002 > PC-cillin 2002 Settings.
- In the system tray, right-click the Real-time Monitor and click Configuration.

The Settings window appears.



See also:

Viewing the PC-cillin window

About the Real-time Monitor

Starting the Real-time Monitor

About Simple mode

PC-cillin 2002 lets you choose between Simple and Standard modes. The Simple mode lets you quickly and easily perform common PC-cillin tasks such as viewing a simplified version of your system status, and scanning all drives. In addition you can update and register your software.

To view the Simple mode, on the PC-cillin window, click the Simple tab.

See also:

About Standard mode

Viewing Simple mode System Status

Viewing the Simple mode System Status lets you instantly know the following about your system:

- **Time of last update pattern**- The last time you updated your pattern file.
- **Real-time Scan**- Whether the Real-time Scan is turned on (Enabled) or turned off (Disabled).
- **Virus detected since PC-cillin was on guard**- If PC-cillin detected a virus.
- **Personal Firewall**- Whether the Personal Firewall is turned on (Enabled) or turned off (Disabled).
- **Hacker attack since PC-cillin was on guard**- If PC-cillin has detected a hacker attack.

To view the Simple mode System Status:

1. On the PC-cillin window, click the Simple tab. The Simple mode menu appears.
2. Click the System Status link. The System Status screen appears.

See also:

Viewing Standard mode System Status

About Standard mode

The Standard mode menu lets you perform advanced PC-cillin 2002 functions including viewing your system status in more detail, selectively scanning folders, synchronizing your PDA, quarantining files, and viewing logs. In the Standard mode, as in the Simple mode, you can also update and register your software.

To view the Standard mode, on the PC-cillin window, click the Standard tab.

See also:

About Simple mode

Viewing Standard mode System Status

Viewing the Standard mode System Status provides detailed Real-time Scan and Personal Firewall information:

- **Real-time Scan**- Whether the Real-time Scan is turned on (Enabled) or turned off (Disabled).
- **Time of last virus found**- Last time PC-cillin found a virus on your computer.
- **Last virus found**- Name of the last virus PC-cillin found.
- **Last infected file**- Name of the last infected file.
- **Personal Firewall**- Whether the Personal Firewall is turned on (Enabled) or turned off (Disabled).
- **Time of last attack-** Last time your computer experienced a hacker attack
- **Source of last attack**- Location the last hacker attack originated from.
- **Last attack type**- Type of attack used to try to harm your computer.
- **Bytes sent**- Number of bytes sent by your computer.
- **Bytes received**- Number of bytes received by your computer.

To view the Standard mode System Status:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. Click the System Status link. The System Status screen appears.

See also:

About Standard mode
Viewing the Simple mode System Status

Scan Now

Use Scan Now to quickly select the drives or folders you want to scan for viruses. PC-cillin scans the drives or folders and executes the necessary virus actions according to the settings you have configured for Manual Scan.

To perform a manual scan using Scan Now:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. Click the Scan Now link. The Scan Now screen appears.
3. Under Manual Scan, select the drives or folders you want to scan.
4. Click Scan. The Scan files dialog box appears.

See also:

Running scan tasks
About Manual Scan

Running scan tasks

Scan tasks are a quick and easy way to perform a variety of scans. You can execute any scan task you have previously defined.

To run a scan task:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. Click the Scan Now link. The Scan Virus screen appears.
3. Under Scan tasks, select the task you want to execute.
4. Click Execute. The Scan Files dialog box appears and PC-cillin begins scanning.

PC-cillin 2002 includes a number of scan tasks that have been pre-defined. In addition to running these scan tasks, you can also view them to give you hints about how to create your own effective scan tasks.

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A1>**Scan for macro viruses**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A2>**Scan C:\ drive weekly**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A3>**Scan everything monthly**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A4>**Scan floppy A:**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A5>**Scan Internet related files**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A6>**Scan all Word documents**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A7>**Scan all Excel documents**

= 4) && (typeof(BSPSPopupOnMouseOver) == 'function')) BSPSPopupOnMouseOver(event)" id=A8>**Scan Program files**

See also:

Scan Now

About scan tasks

About PC-cillin for Wireless

As PDAs and other handheld computing devices increase the number of ways for communicating with other devices, from infrared transmitters, to mobile phone interfaces (high-end PDAs even feature Internet connectivity), the chances of becoming infected by viruses also increase.

With features like real-time launch scanning (for Palm PDAs), PC-cillin for Wireless prevents viruses from entering every possible entry point--beaming, synchronizing, email, and Internet downloading.

Note: The real-time launch scanning for Palm PDAs is activated when you tap the Virus Application.

See also:

About Intelligent Update

Updating PC-cillin for Wireless

Selecting PDA OS type

About quarantined files

PC-cillin 2002 can safely quarantine files that cannot be cleaned or suspicious files that may contain new, unknown viruses. Quarantined files will not spread and may be sent to Trend Micro's eDoctor Lab, deleted, or held for further analysis and repair.

You should quarantine files that can't be cleaned. Although you could delete the file, if you quarantine it, you have a lot more options. For example, perhaps after the next pattern file update you can clean the file. You can also restore it, send it to Trend Micro for analysis and manually cleaning, or ultimately you can still delete it if you choose.

However, infected files placed in quarantine are not immediately cleaned and the file remains infected until cleaned. For maximum protection against the latest viruses, remember to have the latest virus pattern files and scan engine updates installed on your computer.

Note: *Infected files that are part of a compressed file are not automatically quarantined -- you must first decompress the file to have PC-cillin take the action specified.*

See also:

Adding files to the Quarantine folder

Cleaning quarantined files

Deleting quarantined files

Restoring quarantined files

Sending quarantined files to Trend Micro

What happens if a virus is detected

Adding files to the Quarantine folder

You can manually add files to the Quarantine folder. Perform this action if you suspect a file is infected and the scan engine is unable to clean the file. For example, if you received an email with an attachment from someone you don't know and accidentally saved the attachment to your computer.

To add a file to the Quarantine folder:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Quarantine link. The Quarantine screen appears.
3. Click Add. The Open dialog box appears.
4. Browse to the location of the file.
5. Select the file and click Open. A confirmation message box appears.
6. Click Yes. The file appears in the Quarantine List.

See also:

About quarantined files
Cleaning quarantined files
Deleting quarantined files
Restoring quarantined files
Sending quarantined files to Trend Micro
What happens if a virus is detected

Cleaning quarantined files

Files moved to the Quarantine folder may still contain a virus. Every time you update your pattern files or any other PC-cillin program files, try to clean quarantined files.

To clean a quarantined file:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Quarantine link. The Quarantine screen appears.
3. In the Quarantine List, select the file you want to clean.
4. Click Clean to attempt to clean the file.

See also:

About quarantined files

Adding files to the Quarantine folder

Deleting quarantined files

Restoring quarantined files

Sending quarantined files to Trend Micro

What happens if a virus is detected

Deleting quarantined files

Since files moved to the Quarantine folder may still be infected, it may be necessary to delete the files if the file cannot be cleaned even after using the latest pattern files and scan engines.

To delete a quarantined file:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Quarantine link. The Quarantine screen appears.
3. In the Quarantine List, select the file you want to delete.
4. Click Delete. A confirmation message box appears.
5. Click Yes to delete the file.

See also:

About quarantined files
Adding files to the Quarantine folder
Cleaning quarantined files
Restoring quarantined files
Sending quarantined files to Trend Micro
What happens if a virus is detected

Restoring quarantined files

After a file in the Quarantine folder has been cleaned you can restore it to its original location. In addition, there may be times when files moved to the Quarantine folder may cause an application or even your operating system to stop functioning properly. In this situation, you may need to restore quarantined files to their original location.

To restore a quarantined file:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Quarantine link. The Quarantine screen appears.
3. In the Quarantine List, select the file you want to restore.
4. Click Restore. A confirmation message box appears.
5. Click Yes to restore the file to its original location.

See also:

About quarantined files
Adding files to the Quarantine folder
Cleaning quarantined files
Deleting quarantined files
Sending quarantined files to Trend Micro
What happens if a virus is detected

Sending quarantined files to Trend Micro

If the file cannot be cleaned even after using the latest pattern files and scan engines, you can send it to Trend Micro for further analysis. The infected file is automatically routed to the Trend Micro virus expert on duty. Because we have offices around the world, virus experts are on duty around the clock. If it's night time in the United States, for example, the file is routed to our virus analysis lab in Asia.

To send a quarantined file to Trend Micro:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the Quarantine link. The Quarantine screen appears.
3. In the Quarantine List, select the file you want to sent to Trend Micro.
4. Click Send to Trend. A message box appears.
5. Click OK. The quarantined file is sent to Trend Micro for analysis.

See also:

About quarantined files

Adding files to the Quarantine folder

Cleaning quarantined files

Deleting quarantined files

Restoring quarantined files

What happens if a virus is detected

About logs

PC-cillin keeps running logs of all update, virus, Site filter, and Personal Firewall activity. These logs can be viewed from the View Logs screen and provide a valuable source of information.

In addition to displaying the date and the time of each recorded log, the various log types provide log-specific information:

Update Logs: PC-cillin keeps a running record of each time it contacts Trend Micro to update the virus pattern file or program files. New logs are created when a download is performed. Update log entries also contain: the time the virus was detected; what file(s) were downloaded and installed from Trend Micro; the status--Success or Failure--of the download.

Virus Logs: PC-cillin keeps a record of all the viruses it detects and the actions performed on them. New logs are created when a virus is detected. Virus log entries also contain: the time the virus was detected; the type of scan--Real-time or a Scan Task--that detected the virus; the source type of the virus; the name of the virus; the name of the actual file that contains the virus; the success or failure the first action took on the infected file; and the success or failure the second action took on the infected file.

Site Filter Logs: PC-cillin records its Web Security activity. New logs are created when a Web site is blocked or harmful Web content encountered. Site filter log entries also contain: the time access to a restricted site was attempted; the URL, or Web address, that was blocked; the Action the Web filter took; and either Deny Access or Warn.

Personal Firewall Logs: PC-cillin logs all of its Internet activity. New logs are created when your computer is attacked from someone using the Internet. Personal Firewall log entries also contain: the time of the attack; the direction of the network traffic (IN/OUT); the type of protocol used; the IP address of the source; the port number of the source; the IP address of the destination; the port number of the destination; the name of the attack type.

See also:

Viewing logs
Exporting logs
Deleting logs

Viewing logs

You can view the following types of logs: Update, Virus, Site Filter, and Personal Firewall. The log entries are grouped according to the date the event occurred.

To view a log:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the View Logs link. The View Logs screen appears.
3. Under Log Type, click the type of log you want to view (for example: Update, Virus, Site Filter, and Personal Firewall Logs).
4. Click the View Logs button. The log dialog box appears.
5. Select the date of the log you want to view. The log entries for that date appear.
6. To sort the logs (ascending or descending) by column header (for example: Time), click the column title for the desired display.

See also:

About logs
Exporting logs
Deleting logs

Exporting logs

You can save log entries and print them out or examine them in detail. Save log entries as a comma-separated value (CSV) file (files are text with each of the fields separated by a comma) or as a plain text file. The default file format is CSV.

To export a log entry:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the View Logs link. The View Logs screen appears.
3. Under Log Type, click the type of log you want to export.
4. Click the View Logs button. The log dialog box appears.
5. Under Log Date, select the date of the log entries you want to export. The log entries for that date appear.
6. Click Export. The Save As dialog box appears.
7. Browse to the desired location and type a name for the log entry. To save as a plain text file: in the Save as type list, choose text file.
8. Click Save.

See also:

About logs
Viewing logs
Deleting logs

Deleting logs

Delete log entries if the information they provide is no longer useful. If the number of logs is taking up too much disk space you may also want to delete log entries for certain dates.

To delete a log entry:

1. On the PC-cillin window, click the Standard tab. The Standard mode menu appears.
2. On the Standard mode menu, click the View Logs link. The View Logs screen appears.
3. Under Log Type, click the type of log you want to delete.
4. Click the View Logs button. The log dialog box appears.
5. Under Log date, select the date of the log entry you want to delete. The log entries for that date appear.
6. Click Delete. The Delete logs dialog box appears.
7. From the *Delete logs before and including the date* list, select a date.
8. Click OK. A confirmation message box appears.
9. Click Yes to delete the log entries.

See also:

About logs
Viewing logs
Exporting logs

About the Real-time Monitor

The Real-time Monitor is the quickest way to access certain functions, for example to display the PC-cillin or Settings windows. With the Real-time Monitor, you know at a glance if real-time scanning is enabled (the lightning streak icon is red) or disabled (the lightning streak icon is grey).


The Emergency Lock is activated. All incoming and outgoing Internet traffic is halted.


PC-cillin is connecting to the Trend Micro server to download the latest updates.


Your computer is currently under attack.


The real-time scanning function is enabled.


The real-time scanning function is disabled.

The Real-time Monitor can help you perform the following:

- Open the PC-cillin window
- Enable the Emergency Lock
- Enable real-time scanning
- Open the Settings window
- View the real-time status
- Exit the Real-time Monitor

See also:

Starting the Real-time Monitor
Opening the PC-cillin window
Opening the Settings window
Viewing Real-time Satus

Starting the Real-time Monitor

When the PC-cillin program loads, the Real-time Monitor should automatically launch and appears in your system tray. However, if you do not see the Real-time Monitor in your system tray, we recommend you launch it.

To start the Real-time Monitor, click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor. The Real-time Monitor icon appears in the system tray.

See also:

About the Real-time Monitor

Opening the PC-cillin window

Opening the Settings window

Viewing Real-time Satus

Opening the PC-cillin window

Use the Real-time Monitor to quickly open the PC-cillin window.

To open the PC-cillin window:

1. Make sure the Real-time Monitor is displayed in the system tray. If not, click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor.
2. Do one of the following:

- Double-click the Real-time Monitor.
- Right-click the Real-time Monitor and click Startup PC-cillin.

The PC-cillin window appears.

See also:

[About the Real-time Monitor]
[Starting the Real-time Monitor]
[Opening the Settings window]
[Viewing Real-time Satus]

Opening the Settings window

Use the Real-time Monitor to quickly open the Settings window.

To open the Settings window:

1. Make sure the Real-time Monitor is displayed in the system tray. If not, click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor.
2. Right-click the Real-time Monitor and click Configuration. The Settings window appears.

See also:

About the Real-time Monitor

Starting the Real-time Monitor

Opening the PC-cillin window

Viewing Real-time Satus

Viewing Real-time Status

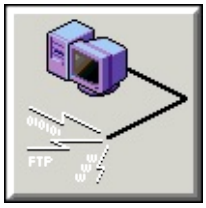
View the Real-time status to display the pattern file version you are currently using and the name of the last file scanned. It also displays Firewall traffic information and the status of the Emergency Lock.

In addition, you can activate the Internet Emergency Lock function to immediately halt all network activity. Activating the Emergency Lock function immediately stops all traffic to and from the Internet.

To view the Real-time Status:

1. Make sure the Real-time Monitor is displayed in the system tray. If not, click Start > Programs > Trend Micro PC-cillin 2002 > Real-time Monitor.
2. In the system tray, right-click the Real-time Monitor icon and click Real-time Status. The Real-time Scan Monitor dialog box appears.

Note: In the Real-time Scan Monitor dialog box, you can click the Emergency button to activate the Emergency Lock.



See also:

About the Real-time Monitor
Starting the Real-time Monitor
Opening the PC-cillin window
Opening the Settings window

PDA viruses

The increasing power of PDAs has spawned a new breed of viruses. Maliciously creative programmers have leveraged the PDA's ability to communicate with other devices and run programs, to cause digital mayhem.

The blissfully safe world where users of these devices could synchronize and download with impunity came to an end in August 2000 with the discovery of the Palm Liberty.A virus. Since then, many more viruses have been discovered.

Though not yet as harmful as their PC-based cousins, these viruses still pose a threat to unsuspecting users. Their effects vary from the harmless flashing of an unwanted message or an increase in power consumption, to the deletion of all installed programs. But the threat is growing, and the destructiveness of these viruses is expected to parallel the development of the devices they attack.

See also:

Scanning for PDA viruses

Dealing with PDA viruses

Getting PDA virus information

PC-cillin for Wireless System Requirements

System Requirements

Your PDA requires the following to run PC-cillin for Wireless.

Palm

- Palm® OS 3.1 or above
- 2MB of memory or more
- Minimum 100KB of free memory for program installation
- Desktop computer must have Palm Desktop and HotSync® applications

EPOC

- Psion Revo™ or Revo Plus
- 8MB of RAM or more
- Minimum 200KB of free memory for program installation.
- Desktop computer must have PsiWin application

Pocket PC

- Windows CE® 3.0
- 16MB of RAM or more
- Minimum 1MB of free memory for program installation
- Desktop computer must have Microsoft ActiveSync application

Installing PC-cillin for Wireless

Previous versions of PC-cillin for Wireless are not supported for Program update and unlike the PC-cillin 2002 main program, PC-cillin for Wireless is not overwritten during installation. If you have a PDA connected to your computer, during initial installation of PC-cillin 2002 there are additional installation procedures you need to follow based on your PDA OS type. Even if you installed PC-cillin 2002 and then added a PDA to your computer, PC-cillin detects the PDA type and lets you select your PDA type in the Update PDA screen of the Settings window. However, if your PDA is not a Palm PDA, you need to perform the following additional procedure to synchronize your PDA.

Note: To install PC-cillin for Wireless while installing the PC-cillin 2002 main program, it is necessary to have PDA synchronization software for your PDA installed on your PC, and the PDA device must be connected to the PC before running the installation program.

For EPOC and Pocket PC PDAs:

You have to perform the following procedure only if you installed an EPOC or Pocket PC PDA after you installed PC-cillin 2002.

To manually install synchronize files:

1. Insert the PC-cillin 2002 CD into the appropriate drive.
2. On the CD, navigate to the Wireless folder (PCC9\program files\Trend Micro\PC-cillin). Do one of the following:

- For EPOC PDAs: Double-click the PcciEpoc.sis file.
- For Pocket PC PDAs: Double-click the PocketPC.exe file.

Follow the onscreen instructions.

Dealing with PDA viruses

There are two actions available if a virus is detected: bypass or delete.

- To take no action against the detected viruses, tap the Back button to return to the program's entry screen.
- To delete all detected viruses, tap the Delete All button. To delete only selected viruses, choose the target virus on the list of detected viruses, and tap the Delete button.

See also:

About PDA viruses
Scanning for PDA viruses
Getting PDA virus information

Getting PDA virus information

Virus information can be viewed either from the main screen, or on the scan results screen.

From the Main Screen:

1. Tap the Virus Info button. This opens the virus encyclopedia.
2. Select the virus you wish to inquire about.
3. Tap the Description button to view the virus description.

From the Scan Results Screen:

1. Select the virus you want to know more about from the list of detected viruses.
2. Tap the Description button to view the virus description.

See also:

About PDA viruses
Scanning for PDA viruses
Dealing with PDA viruses

Using the PC-cillin for Wireless Virus Log

The virus log stores information about viruses detected during previous scans and the action taken against them.

To view the log, tap the Log button on the main screen.

The Virus Scan Log screen shows the detected viruses as well as the size of the log in bytes. Tap on Back to return to the main screen, or Clear Log to delete the log entries. In the latter option, a dialog box appears for you to confirm log deletion. Tap on Yes to continue, or No to abort the operation.

Uninstalling PC-cillin for Wireless from your PDA

To uninstall PC-cillin for Wireless from your Palm:

1. Select Delete from the Palm system menu to bring up the Delete list.
2. Remove the following files:

- PC-cillin - the main program file
- PATTERN.xxx - the pattern file
- Pccillin.log - the log file; this contains log information
- Realtime - the real-time scanning module

3. Tap Done to return to the main screen. After you remove the Realtime file, the system restarts.

To uninstall PC-cillin for Wireless from your EPOC:

1. Close the PC-cillin for EPOC program by clicking the ESC button.
2. Click Control Panel on the right-hand side bar.
3. Double-tap the Add/Remove icon to open the Installed Programs dialog box.
4. Select the PC-cillin for EPOC item, then tap Remove. A confirmation dialog box opens.
5. Tap Yes to remove the program.

To uninstall PC-cillin for Wireless from your PocketPC:

1. Close PC-cillin for Pocket PC by tapping the OK button at the top-right corner of the screen.
2. Click Start > Settings to open the Settings dialog.
3. Select the System tab and then tap the Remove Programs icon.
4. Select the Trend Micro PC-cillin for Pocket PC item, then click Remove. The Remove Program dialog box opens.
5. Tap Yes to remove the program.

Uninstalling PC-cillin

Before uninstalling PC-cillin, you must stop Real-time scanning. You can do this by right-clicking the PC-cillin icon in the system tray and then clicking Real-time Monitor to clear the check, if any. The lightning bolt icon turns grey when real-time scanning is disabled.

During uninstallation, PC-cillin deletes all quarantined files. These files may contain "live" viruses and should not be left on your computer. If you must preserve them, we suggest that you copy the entire directory to a safe location such as a specially marked floppy disk.

To uninstall PC-cillin, do one of the following:

- Click Start > Programs > Trend Micro PC-cillin 2002 > Uninstall. A confirmation dialog box appears. Click Yes to uninstall PC-cillin.
- Click Start > Settings > Control Panel. Double-click Add/Remove Programs and select PC-cillin 2002. Click Add/Remove. A confirmation dialog box appears. Click Yes to uninstall PC-cillin.

Maintaining constant protection from viruses

Real-time scanning provides constant protection against viruses. With Real-time scanning turned on, you can significantly reduce the chances of your computer becoming infected.

The real-time scanner checks files for viruses whenever they are used for example, each time a file is: opened, copied, moved, saved, compressed or decompressed, downloaded from the Internet, and, in the case of email attachments, read.

Because it is so powerful and operates in the background, we recommend you keep Real-time scanning enabled.

To maintain constant protection from viruses:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Quick Access link. The Quick Access screen appears.
3. Select the *Enable Real-time Scan* check box.
4. Click Apply.

See also:

About Real-time Scan

Protecting against email threats

PC-cillin can scan data packets as you download mail messages from an Internet (POP3) mail server. This makes sure infected attachments don't infect your computer. Some examples of mail clients that use POP3 mail servers include: Microsoft Outlook, Outlook Express, Eudora Pro, and Netscape Messenger.

To protect against email threats:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Quick Access link. The Quick Access screen appears.
3. Select the *Enable Internet mail scan* check box.
4. Click Apply.

See also:

About Internet mail scan

Preventing Internet programs from harming your computer

WebTrap protects against malicious Java and ActiveX applets. Although most Web sites are completely harmless, it is possible for someone to create a small program and set it to run, invisibly, whenever their Web page is accessed. These programs may destroy data, steal your passwords, financial data, etc.

PC-cillin's WebTrap protects you against malicious Java and ActiveX programs while allowing harmless ones to safely pass through.

To prevent Internet programs from harming your computer:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Quick Access link. The Quick Access screen appears.
3. Select the *Enable WebTrap* check box.
4. Click Apply. A message box appears notifying you that the change will not take effect until you restart your computer or log off and log on again.
5. Click OK.
6. Restart your computer or log on again to immediately enable the function.

See also:

About WebTrap

Filtering unwanted Web content

For protection against offensive Web content, PC-cillin offers the Site filter. This utility lets you set whatever Web sites you want "off-limits" to other users of the computer. This function is especially useful for families where many family members share one computer.

To filter unwanted Web content:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Quick Access link. The Quick Access screen appears.
3. Select the *Enable Site filter* check box.
4. Click Apply. A message box appears notifying you that the change will not take effect until you restart your computer or log off and log on again.
5. Click OK.
6. Restart your computer or log on again to immediately enable the function.

Note: If you have password-protected your Site filter screen and try to enable the Site filter on the Quick Access screen, you must supply your password.

See also:

About the Site Filter

Blocking harmful Internet connections

The PC-cillin 2002 Personal Firewall protects your computer against attacks from the Internet. A firewall creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters the incoming and outgoing Internet traffic. By filtering Internet traffic, the firewall prevents malicious programs or files from entering your computer.

To block harmful Internet connections:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Quick Access link. The Quick Access screen appears.
3. Select the *Enable Personal Firewall* check box.
4. Click Apply.

See also:

About the Personal Firewall

About virus scan actions

What happens when PC-cillin detects a virus? It depends on the action that is configured in the Settings window. For both Manual Scan and Real-time Scan, you can set actions PC-cillin executes when it detects a virus. You can also set actions PC-cillin will perform, if for some reason, PC-cillin is unable to clean a virus. Any action PC-cillin takes is recorded as a log entry in the Virus log.

For a Real-time Scan, these virus scan actions include the following:

- **Deny Access**- Deny the user access to the infected file.
- **Rename**- Modify the file's extension to prevent opening or execution.
- **Quarantine**- Move infected or malicious files to a restricted access folder.
- **Clean**- Remove virus code from infected files.
- **Delete**- Remove the infected or malicious files (e.g., Trojans, worms, etc.).

For a Manual Scan, all the virus actions are the same as a Real-time Scan with the exception of **Deny Access**. Instead the Manual Scan action is: **Pass -** Record virus infection or malicious files in the Virus log but take no action.

See also:

Setting virus scan actions

Setting virus scan actions if unable to clean file

Cleaning compressed files

Backing up files before cleaning

Setting virus scan actions

For both Manual Scan and Real-time Scan, you can set actions PC-cillin executes when it detects a virus. We recommend you use the default scan action setting, *Clean*. Any virus scan action PC-cillin executes is recorded as a log entry in the Virus log.

To set a virus scan action:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands. Do one of the following:

- To set Manual Scan virus scan actions, click the Manual Scan link.
- To set Real-time Scan virus scan actions, click the Real-time Scan link.

Depending on the link you clicked, the Manual Scan or Real-time Scan screen appears.

3. On the Manual Scan or Real-time Scan screen, under Scan action, select one of the following virus scan actions from the *Action when virus found* list:

- **Deny Access**- Deny the user access to the infected file (Real-time Scan only).
- **Pass**- Record virus infection or malicious files in the Virus log, but take no action (Manual Scan only).
- **Rename**- Modify the file's extension to prevent opening or execution.
- **Quarantine**- Move infected or malicious files to a restricted access folder.
- **Clean**- (Default) Remove virus code from infected files.
- **Delete**- Remove the infected or malicious files (e.g., Trojans, worms, etc.).

4. Click Apply.

See also:

About virus scan actions
Setting virus scan actions if unable to clean file

Setting virus scan actions if unable to clean file

You can also set actions PC-cillin will execute if a file cannot be cleaned. If a file can't be cleaned, you should quarantine the file. Therefore, we recommend you use the default scan action setting, *Quarantine*.

Although you could delete the file, if you quarantine it, you have a lot more options. For example, perhaps after the next pattern file update you can clean the file. You can also restore it, send it to Trend Micro for analysis, or ultimately you can still delete it if you choose. Any virus scan action PC-cillin executes is recorded as a log entry in the Virus log.

To set a virus scan action if unable to clean a file:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands. Do one of the following:

- To set Manual Scan virus scan actions if unable to clean a file, click the Manual Scan link.
- To set Real-time Scan virus scan actions if unable to clean a file, click the Real-time Scan link.

Depending on the link you clicked, the Manual Scan or Real-time Scan screen appears.

3. On the Manual Scan or Real-time Scan screen, under Scan action, select one of the following virus scan actions from the *Action on uncleanable files* list:

- **Deny Access**- Deny the user access to the infected file (Real-time Scan only).
- **Pass**- Record virus infection or malicious files in the Virus log, but take no action (Manual Scan only).
- **Rename**- Modify the file's extension to prevent opening or execution.
- **Quarantine**- (Default) Move infected or malicious files to a restricted access folder.
- **Delete**- Remove infected or malicious files (e.g., Trojans, worms, etc.).

4. Click Apply.

See also:

About virus scan actions
Setting virus scan actions
Cleaning compressed files
Backing up files before cleaning

Cleaning compressed files

File compression involves shrinking the size of a file or files using a data compression format. One of the most popular is the Zip format. Compressed files are useful for transferring information over networks because of the smaller file size.

For example, let's say there are five files, *A.doc*, *B.doc*, *C.*doc, *D.doc*, and *E.doc: C.doc* is infected with a macro virus, and they are all packed into a single compressed file called *docs.zip*: [*docs.zip*(*A.doc*, *B.doc*, ***C.doc***, *D.doc*, *E.doc*)]. You can set PC-cillin to detect the virus in *C.doc*, issue an alert, and write the event to the Virus log. Because *C.doc* is in the first layer, PC-cillin will automatically execute the action you have specified when PC-cillin detects a virus up to the second layer. If you have selected the *Clean viruses in compressed files* check box. PC-cillin is able to carry out this action only if the infected file is contained in the second layer or less of the compressed file.

However, if *C.doc* was located in a deeper layer of compression, for example, {*docs1.zip*[*docs.zip*(*A.doc*, *B.doc*, ***C.doc***, *D.doc*, *E.doc*)]}. Although PC-cillin could detect it (if you have set your scan compression layers to a number greater than three) it is unable to perform any scan action. Therefore, if you want to clean *C.doc*, use WinZip, or another compression program to decompress the compressed file. When the individual files have been decompressed, right-click *C.doc* and click PC-cillin. PC-cillin will perform the scan action you have set for Manual Scans.

To clean a compressed file:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands. Do one of the following:

- To set Manual Scan virus scan actions, click the Manual Scan link.
- To set Real-time Scan virus scan actions, click the Real-time Scan link.

Depending on the link you clicked, the Manual Scan or Real-time Scan screen appears.

3. On the Manual Scan or Real-time Scan screen, under Scan action make sure

Clean is selected from the *Action when virus found* list and select the *Clean viruses in compressed files* check box.

4. Click Apply.

See also:

[About virus scan actions]
[Setting virus scan actions]
[Setting virus scan actions if unable to clean file]
[Backing up files before cleaning]

Backing up files before cleaning

During the clean process it is possible the file being cleaned may suffer some damage. You can set PC-cillin to rename and back up the files to the Backup folder (located in the Quarantine folder) before cleaning the original files. This is a safety precaution in case the original file is critical and becomes damaged while being cleaned.

Backed up files should be quickly deleted once you've determined whether the original file is usable after being cleaned. If not, and the file is mission critical, you can send it to Trend Micro for further analysis. (Even if the virus itself can be completely removed, i.e., the file cleaned, some viruses can damage the original file code beyond repair.)

To back up files before cleaning:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands. Do one of the following:

- To set Manual Scan virus scan actions if unable to clean a file, click the Manual Scan link.
- To set Real-time Scan virus scan actions if unable to clean a file, click the Real-time Scan link.

Depending on the link you clicked, the Manual Scan or Real-time Scan screen appears.

3. On the Manual or Real-time Scan screen, under Scan action select the *Back up files before cleaning* check box.
4. Click Apply.

See also:

[About virus scan actions]
[Setting virus scan actions]
[Setting virus scan actions if unable to clean file]
[Cleaning compressed files]

About Manual Scan

A Scan Now (Manual Scan) occurs immediately after you choose your scan target and run the function. Scan Now is an effective way to check a file, folder, or drive that you suspect has been infected and you want immediate confirmation about the status. When PC-cillin detects a virus or other malicious code, it performs the necessary actions according to the settings you have configured for Manual Scan.

See also:

About virus scan actions

Selecting Manual Scan file types

Adding Manual Scan file types

Setting Manual Scan compression layers

Including the boot sector

Selecting Manual Scan file types

The PC-cillin 2002 Manual Scan only examines those file types configured in the Settings window. The following is a list of options you can set to select Manual Scan file types:

- **All file types-** Examine all files no matter what type--the highest level of security. However, there is a trade off between speed and safety. Scanning all files takes longer than scanning only specified files types. However, most file types, for example .TXT, .JPG, .AVI, .HLP, .PDF, etc., are not known to host or spread viruses and probably do not require scanning. But then again until August 1995, document files (.DOC, .XLS, etc.) had never been known to carry viruses either. And now macro viruses are the most prevalent.
- **Recommendation-** Examine only those file types recommended by Trend Micro virus analysts. These recommended file types are known to have a higher risk of containing viruses. Any files whose extension does not appear on the list will not be scanned. "Zip" and other compressed file types must be specified to be included in the scan.
- **Selected Files-** Examine the file types you set. Using this option you can customize the types of files PC-cillin will examine. Any files whose extension is not specified will not be scanned. "Zip" and other compressed file types must be specified to be included in the Manual Scan.

To select Manual Scan file types:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Manual Scan link. The Manual Scan screen appears.
4. Under Scan file types, click one of the following:

- **All file types-** The button becomes disabled.
- **Recommendation-** The button caption becomes *View File Types*. Click View File Types to see a list of Trend Micro recommended higher-risk file types.
- **Selected Files-** The button caption becomes *Select File Types*.

5. Click Apply.

See also:

About virus scan actions
About Manual Scan
Adding Manual Scan file types
Setting Manual Scan compression layers
Including the boot sector

Adding Manual Scan file types

Define your own file types to scan for high-risk files that are not included in the recommended file list. This increases the scanning speed because you don't scan all file types. However, when you select this option, PC-cillin will only scan for selected file types during a Manual Scan.

To add a file type, you simply provide the file type or extension (three letter "suffix" that identifies the type of file) that you want PC-cillin to examine. Examples of file types or extensions include: annual report.**doc**, 4th quarter sales.**xls**, win.**com**, calculator.**exe**. You can add compressed file types to the list of those scanned or remove unnecessary file types.

To add a Manual Scan file type:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Manual Scan link. The Manual Scan screen appears.
4. Under Scan file types click Selected Files. The button caption becomes *Select File Types*.
5. Click Select File Types. The File Types dialog box appears.
6. Click Add. The Add File Type(s) dialog box appears.
7. In the Extension box, type your file extension. You can just type the letters of your file type, it is unncessary to include a "." before the file type or to type in upper-case.
8. Click OK. You can also do the following:

- To delete a file type, select it and click Delete. The file type is removed from the list.
- To add compressed file types (ARJ, CAB, CO_, DO_, EX_, LZH, XL_ and ZIP), click Compressed. The compressed file types are added to the list.
- To restore a list of the default file types, click Default. The original default file types are added to the list.

9. Click OK.

10. Click Apply.

See also:

About virus scan actions
About Manual Scan
Selecting Manual Scan file types
Setting Manual Scan compression layers
Including the boot sector

Setting Manual Scan compression layers

PC-cillin recognizes many types of file compression including PK-ZIP and LZEXE, and four types of file encoding, including UUencode and MIME. *File compression* involves shrinking the size of a file or files using a data compression format. One of the most popular is the Zip format. Compressed files are useful for transferring information over networks because of the smaller file size.

PC-cillin will check the contents of a compressed file for viruses based on the number of *layers* you have set. Usually when files are compressed they are only compressed to the first layer: [*docs.zip*(*A.doc*, *B.doc*, *C.doc*, *D.doc*, *E.doc*)] i.e., the compressed file [*docs.zip*] contains the files (*A.doc*, *B.doc*, *C.doc*, *D.doc*, *E.doc*) which are located in the first layer. If the *docs.zip* file was compressed again, {*docs+1.zip*[*docs.zip*(*A.doc, B.doc, C.doc*, *D.doc*, *E.doc*)]} the original files are now located in the second layer.

When multiple layers of compression are encountered, PC-cillin recursively decompresses each, up to the limit you set. In other words, if an archive contains .cab files that have been compressed using PK-ZIP, and LZEXE, PK-LITE, Microsoft Compress, etc., PC-cillin will decompress each layer until no more compressed files are found or the limit of you have specified is reached.

To set Manual Scan compression layers:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Manual Scan link. The Manual Scan screen appears.
4. Under Scan file types, select the number of compression layers from the Compression Layer list. The default number of layers is five.
5. Click Apply.

Note: When detecting infected files that are part of a compressed file, PC-cillin can automatically execute the *Clean* action only if the following conditions are met:

- You have selected the *Clean viruses in compressed files* check box.
- The file or files are located in the second layer.

To perform a *Clean* scan action for a compressed file for files beyond the second layer, you must decompress it first. If you have Real-time Scan enabled, decompressing the file will trigger the action.

If you're not using Real-time Scan, right-click the infected file after it is decompressed, select Properties from the pop-up menu and then choose Virus Properties.

Important: Be sure to delete the compressed file (for example the .ZIP file), because it will still contain a copy of the infected item.

See also:

About virus scan actions

About Manual Scan

Selecting Manual Scan file types

Adding Manual Scan file types

Including the boot sector

Including the boot sector

The boot sector is critical to the proper start up of your computer. On startup, the computer checks the master boot record (MBR) for instructions on how to start the operating system and loads much of this data into memory. The boot sector is special, and usually off-limits to most programs--they can't touch it. Nor can you see the boot sector using Explorer, for example.

Any boot viruses that are infecting the computer are loaded into memory along with the valid data during boot up (system start-up). It's from their perch in memory that they infect files on the hard drive whenever they are opened, closed, etc.

What makes boot viruses especially nasty is that even if all the files on the system are cleaned, and the memory is cleaned, the next time the computer is restarted, the whole infection will come back -- unless and until the boot sector itself has been cleaned. And besides cleaning the c:\ boot sector, if you ever have a boot virus, be sure to clean every floppy, ZIP, and other removable, bootable disk that you have.

You may also want to run a quick scan of the boot sector of any floppies or disks before using them to start your computer (including game disks!).

To include the boot sector in a Manual Scan:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Manual Scan link. The Manual Scan screen appears.
4. Under Scan file types , select the *Include boot sector* check box.
5. Click Apply.

See also:

About virus scan actions
About Manual Scan
Selecting Manual Scan file types
Adding Manual Scan file types
Setting Manual Scan compression layers

About Real-time Scan

Real-time scanning provides constant protection against viruses. With real-time scanning turned on, you reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), we recommend you always keep real-time scanning enabled.

The real-time scanner checks files for viruses whenever they are used, for example each time a file is opened, copied, moved, saved, compressed or decompressed, downloaded from the Internet, and, in the case of email attachments, read.

See also:

[About virus scan actions]

[Enabling Real-time Scan]

[Selecting Real-time Scan file types]

[Adding Real-time Scan tile types]

[Setting Real-time Scan compression layers]

[About Exception files]

Enabling Real-time Scan

When enabled, PC-cillin's Real-time Scan provides constant protection against viruses. Real-time scanning takes place in the background and requires no user intervention, so you don't really have to do anything to "use" Real-time Scan--just be sure it is enabled.

To enable Real-time Scan:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Select the *Enable Real-time Scan* check box.
5. Click Apply.

See also:

About virus scan actions
About Real-time Scan
Selecting Real-time Scan file types
Adding Real-time Scan tile types
Setting Real-time Scan compression layers
About Exception files

Selecting Real-time Scan file types

Real-time Scan only examines those file types set in the Settings window. The following is a list of options you can set to select Real-time Scan file types:

- **All file types-** Examine all files no matter what type--the highest level of security. However, there is some trade off between speed and safety. On the one hand scanning all files takes longer than scanning only specified files types. On the other hand, most file types, for example .TXT, .JPG, .AVI, .HLP, .PDF, etc., are not known to host or spread viruses and probably do not require scanning. But then again until August 1995, document files (.doc, .xls, etc.) had never been known to carry viruses either. And now macro viruses are the most prevalent.
- **Recommendation-** Examine only those file types recommended by Trend Micro virus analysts. These recommended file types are known to have a higher risk of containing viruses.
- **Selected Files-** Examine the file types you set. Using this option you can customize the types of files PC-cillin will examine. Any files whose extension is not specified will not be scanned. "Zip" and other compressed file types must be specified to be included in the Real-time Scan.

To select Real-time Scan file types:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Under Scan action, click one of the following:

- **All file types-** The button becomes disabled.
- **Recommendation-** The button caption becomes *View File Types*. Click View File Types to see a list of Trend Micro recommended higher-risk file types.
- **Selected Files-** The button caption becomes *Select File Types*.

5. Click Apply.

See also:

About virus scan actions

About Real-time Scan

Enabling Real-time Scan

Adding Real-time Scan tile types

Setting Real-time Scan compression layers

About Exception files

Adding Real-time Scan file types

Define your own file types to scan for high-risk files that are not included in the recommended file list. This increases the scanning speed because you don't scan all file types. However, when you select this option, PC-cillin will only scan for selected file types during a Real-time Scan.

You simply provide the file type or extension (three letter "suffix" that identifies the the type of file) that you want PC-cillin to examine. Examples of file types or extensions include: annual report.**doc**, 4th quarter sales.**xls**, win.**com**, calculator.**exe**. You can add compressed file types to the list of those scanned or remove unnecessary file types.

To add Real-time Scan file types:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Under Scan file types, click Selected Files. The button caption becomes *Select File Types*.
5. Click Select File Types. The File Types dialog box appears.
6. Click Add. The Add File Type(s) dialog box appears.
7. In the Extension box, type your file extension. You can just type the letters of your file type, it is unncessary to include a "." before the file type or to type in upper-case.
8. Click OK. You can also do the following:

- To delete a file type, select it and click Delete. The file type is removed from the list.
- To add compressed file types (ARJ, CAB, CO_, DO_, EX_, LZH, XL_ and ZIP), click Compressed. The compressed file types are added to the list.
- To restore a list of the default file types, click Default. The original default file types are added to the list.

9. Click OK.

10. Click Apply.

See also:

About virus scan actions
About Real-time Scan
Enabling Real-time Scan
Selecting Real-time Scan file types
Setting Real-time Scan compression layers
About Exception files

Setting Real-time Scan compression layers

PC-cillin recognizes many types of file compression including PK-ZIP and LZEXE, and four types of file encoding, including UUencode and MIME. *File compression* involves shrinking the size of a file or files using a data compression format. One of the most popular is the Zip format. Compressed files are useful for transferring information over networks because of the smaller file size.

PC-cillin will check the contents of a compressed file for viruses based on the number of *layers* you have set. Usually when files are compressed they are only compressed to the first layer: (*docs.zip*{*A.doc, B.doc, C.doc, D.doc, E.doc*}) i.e., the compressed file (*docs.zip*) contains the files (*A.doc, B.doc, C.doc, D.doc, E.doc*) which are located in the first layer. If the *docs.zip* file was compressed again [*docs+1.zip*(*docs.zip*{*A.doc, B.doc, C.doc, D.doc, E.doc*})], the original files are now located in the second layer.

When multiple layers of compression are encountered, PC-cillin recursively decompresses each, up to the limit you set. In other words, if an archive contains .cab files that have been compressed using PK-ZIP, and LZEXE, PK-LITE, Microsoft Compress, etc., PC-cillin will decompress each layer until no more compressed files are found or the limit of you have specified is reached.

To set Real-time Scan compression layers:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Under Scan file types, select the number of compression layers from the Compression Layer list. The default number of layers is one.
5. Click Apply.

Note: When detecting infected files that are part of a compressed file, PC-cillin can automatically execute the *Clean* action only if the following conditions are met:

- You have selected the *Clean viruses in compressed files* check box.
- The file or files are located in the second layer.

To perform a *Clean* scan action for a compressed file for files beyond the second layer, you must decompress it first. If you have Real-time Scan enabled, decompressing the file will trigger the action.

If you're not using Real-time Scan, right-click the infected file after it is decompressed, select Properties from the pop-up menu and then choose Virus Properties.

Important: Be sure to delete the compressed file (for example the .ZIP file), because it will still contain a copy of the infected item.

See also:

About virus scan actions

About Real-time Scan

Enabling Real-time Scan

Selecting Real-time Scan file types

Adding Real-time Scan tile types

About Exception files

About Exception files

Occasionally antivirus programs detect a file as being infected with a virus when in fact there is no virus. This is because the binary pattern of the file is sufficiently similar to a real virus that the scan engine cannot distinguish the difference. This sometimes happens in Microsoft Word or Excel documents with complex macros.

In order to prevent false alarms or speed up the scanning process, you can configure PC-cillin to avoid scanning certain files. These are called *scan exceptions*.

See also:

About virus scan actions

About Real-time Scan

Adding Exception files

Adding Exception folders

Adding Exception files

You can set exceptions to PC-cillin's Real-time Scan so that certain files are ignored. For example, Quarantined files are never included in real-time scanning (you know they're infected, that's why they've been quarantined). You may have other files that you don't want real-time scanning to examine.

To add an exception file:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Under Scan file types, click Exception files. The Set Real-time Exception dialog box appears.
5. Click Add File. The Open dialog box appears.
6. Browse to and select the file you want to exclude from scanning.
7. Click Open. The file appears in the Real-time Scan exceptions list. To remove a file from the list, under Real-time Scan exceptions select the file, and then click Delete.
8. Click OK.
9. Click Apply.

See also:

About virus scan actions
About Real-time Scan
About Exception files
Adding Exception folders

Adding Exception folders

You can add folders to a Scan Exceptions list, which PC-cillin uses to determine what folders should be skipped when running a real-time scan.

To add an exception folder:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Real-time Scan link. The Real-time Scan screen appears.
4. Click Exception files. The Set Real-time Exception dialog box appears.
5. Click Add Folder. The Browse for Computer dialog box appears.
6. Browse to and select the folder you want to exclude from scanning.
7. Click OK. The folder appears in the Real-time Scan exceptions list. To remove a folder from the list, under Real-time Scan exceptions select the folder, and then click Delete.
8. Click OK.
9. Click Apply.

See also:

About virus scan actions
About Real-time Scan
About Exception files
Adding Exception files

About Internet mail scan

PC-cillin can scan data packets as you download mail messages from an Internet (POP3) mail server making sure infected attachments don't invade your computer. Examples of mail clients that use POP3 mail servers include: Microsoft Outlook, Outlook Express, Eudora Pro, and Netscape Messenger.

The email client retrieves messages from the mail server. These messages are analyzed and any viruses are detected. However, Internet mail scan does not scan message attachments that are already in folders on your computer.

Post Office Protocol 3 (POP3) is the most recent standard protocol for receiving email, whereby a server receives mail on your behalf and stores it until you check your mailbox and download the messages. If you are a home user who connects to a mail server hosted by your ISP or a Web-based email service, you are probably using a POP3 server. If your computer is connected to a local area network (LAN), you might be using a POP3 mail server. Check with your network administrator about how mail is handled on your company's network.

See also:

Enabling Internet mail scan

Setting Internet mail scan actions

Setting Internet mail scan actions if unable to clean file

Cleaning compressed mail files

Enabling Internet mail scan

Infected email attachments are now the primary means of virus infection. Due to the ubiquity of email communication, many virus writers are now writing viruses that exploit the vulnerabilities of email clients. The Internet mail scan feature must be enabled on the computer before accessing the email server.

To enable Internet mail scan:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click Internet Mail Scan. The Internet mail scan screen appears.
4. Select the *Enable Internet mail (POP3 mail) scan* check box.
5. Click Apply.

Note: A Notification screen briefly appears to inform you the POP3 scan is working correctly. To prevent this screen from displaying, clear the *Display Notification when Internet mail scan checks for viruses* check box.

See also:

[About Internet mail scan]
[Setting Internet mail scan actions]
[Setting Internet mail scan actions if unable to clean file]
[Cleaning compressed mail files]

Setting Internet mail scan actions

For the Internet mail scan, you can set actions PC-cillin executes when it detects a virus. We recommend you use the default mail scan action setting, *Clean*. This lets PC-cillin clean any infected files--effectively keeping the file intact while destroying the virus. Any virus scan action PC-cillin executes is recorded as a log entry in the Virus log.

To set an Internet mail scan action:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Internet Mail Scan link. The Internet Mail Scan screen appears.
4. On Internet Mail Scan screen, under Scan action, select one of the following virus scan actions from the *Action when virus found* list:

- **Pass**- Record virus infection or malicious files in the Virus log, but take no action.
- **Delete**- Remove infected or malicious files (e.g., Trojans, worms, etc.).
- **Clean**- (Default) Removes virus code from infected files.

5. Click Apply.

See also:

[About Internet mail scan]
[Enabling Internet mail scan]
[Setting Internet mail scan actions if unable to clean file]
[Cleaning compressed mail files]

Setting Internet mail scan actions if unable to clean file

You can also set actions PC-cillin will execute, if for some reason a file cannot be cleaned. Any virus scan action PC-cillin executes is recorded as a log entry in the Virus log.

To set an Internet mail scan action if unable to clean file:

1. Under Scan action, select one of the following virus scan actions from the *Action on uncleanable files* list:

- **Pass**- (Default) Record virus infection or malicious files in the Virus log, but take no action.
- **Delete**- Remove infected or malicious files (e.g., Trojans, worms, etc.).

2. Click Apply.

See also:

[About Internet mail scan]
[Enabling Internet mail scan]
[Setting Internet mail scan actions]
[Cleaning compressed mail files]

Cleaning compressed mail files

File compression involves shrinking the size of a file or files using a data compression format. One of the most popular is the Zip format. Compressed files are useful for transferring information over networks because of the smaller file size.

For example, let's say there are five files, *A.doc*, *B.doc*, *C.*doc, *D.doc*, and *E.doc: C.doc* is infected with a macro virus, and they are all packed into a single compressed file called *docs.zip*: [*docs.zip*(*A.doc*, *B.doc*, ***C.doc***, *D.doc*, *E.doc*)]. You can set PC-cillin to detect the virus in *C.doc*, issue an alert, and write the event to the Virus log. Because *C.doc* is in the first layer, PC-cillin will automatically execute the action you have specified when PC-cillin detects a virus up to the second layer. if you have selected the *Clean viruses in compressed files* check box. PC-cillin is able to carry out this action only if the infected file is contained in the second layer or less of the compressed file.

However, if *C.doc* was located in a deeper layer of compression, for example {*docs1.zip*[*docs.zip*(*A.doc*, *B.doc*, ***C.doc***, *D.doc*, *E.doc*)]}. Although PC-cillin could detect it (if you have set your scan compression layers to a number greater than three) it is unable to perform any scan action. Therefore, if you want to clean *C.doc*, use WinZip, or another compression program to decompress the compressed file. When the individual files have been decompressed, right-click *C.doc* and click PC-cillin. PC-cillin will perform the scan action you have set for Internet mail scans.

To clean a compressed mail file:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Internet Mail Scan link. The Internet Mail Scan screen appears.
4. Under Scan action, make sure Clean is selected from the *Action when virus found* list, and then select the *Clean viruses in compressed files* check box.
5. Click Apply.

See also:

[About Internet mail scan]
[Enabling Internet mail scan]

About scan tasks

Scan tasks are a quick and easy way to perform a variety of scans. Using scan tasks automates routine antivirus maintenance procedures on your desktop and improves antivirus management efficiency and control over antivirus policy.

You can "set and forget" as many tasks as you see fit. For each task, you can select the file types you want to scan for viruses, the action PC-cillin will take upon finding a virus, and other program details.

To create a scan task, you must specify a target, configure scan options, and set a schedule.

See also:

Specifying scan task target

Configuring scan task options

Scheduling scan tasks

Editing scan tasks

Deleting scan tasks

Specifying scan task target

Use PC-cillin to create any number of scan tasks designed according to your specific needs. For example, you can specify scan tasks to scan only compressed files, all files on a removable disk drive, or only files located in a particular folder.

To specify a scan task target:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Scan Tasks link. The Scan Tasks screen appears.
4. Click Add. The Task Configuration dialog box appears.
5. Click the Scan Target tab.
6. In the Task name (or description) box, type a descriptive name for the task.
7. From the Target list, select a target of your scan task:

   - **All drives**- scan all drives (including mapped network drives).
   - **Selected drive(s)**- scan a single drive from the Drive list.
   - **Selected file/folder**- choose to scan individual files or folders then do the following:

   - **To set up a routine check of an individual file**- Click Add File, and then in the Open dialog box select the file you want scanned, and then click Open.
   - **To set up a routine check of an individual drive or folder**- Click Add Folder, and then in the Open dialog box select the folders you want scanned, and then click OK.
   - **To remove a drive, folder, or file from the list**- From the list, select the item, and then click Delete.

8. Click OK.

See also:

About scan tasks

Configuring scan task options

Configuring scan task options

Configure your scan task options including, file types, and scan actions. Scan tasks only examine those file types configured. The following is a list of options you can set to select file types:

- **All file types-** Examine all files no matter what type--the highest level of security. However, there is some trade off between speed and safety. On the one hand scanning all files takes longer than scanning only specified files types. On the other hand, most file types, for example, .TXT, .JPG, .AVI, .HLP, .PDF, etc., are not known to host or spread viruses and probably do not require scanning. But then until August 1995, document files (for example, .doc, .xls) had never been known to carry viruses either. And now macro viruses are the most prevalent.
- **Recommendation-** Examine only those file types recommended by Trend Micro virus analysts. These recommended file types are known to have a higher risk of containing viruses. Any files whose extension does not appear on the list will not be scanned. "Zip" and other compressed file types must be specified to be included in the scan.
- **Selected Files-** Examine the file types you set. Using this option you can customize the types of files PC-cillin will examine. Any files whose extension is not specified will not be scanned. "Zip" and other compressed file types must be specified to be included in the scan.

Any action PC-cillin takes is recorded as a log entry in the Virus log. The virus scan actions you can set include the following:

- **Pass**- Record virus infection or malicious files in the Virus log but take no action.
- **Rename**- Modify the file's extension to prevent opening or execution.
- **Quarantine**- Move infected or malicious files to a restricted access folder.
- **Clean**- Remove virus code from infected files.
- **Delete**- Remove the infected or malicious files (e.g., Trojans, worms, etc.).

To configure scan task options:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Scan Tasks link. The Scan Tasks screen appears.
4. Click Add. The Task Configuration dialog box appears.
5. Click the Scan Options tab. The Scan Options property sheet appears.
6. Under Scan file types, click one of the following:

- **All file types-** The button becomes disabled.
- **Recommendation-** The button caption becomes *View File Types*. Click View File Types to see a list of Trend Micro recommended higher-risk file types.
- **Selected Files-** The button caption becomes *Select File Types*. To add file types:

a. Click Select File Types. The File Types dialog box appears.

b. Click Add. The Add File Type(s) dialog box appears.

c. In the Extension box, type your file extension. You can just type the letters of your file type, it is unncessary to include a "." before the file type or to type in upper case.

d. Click OK.

e. You can also do the following:

- To delete a file type, select it and click Delete. The file type is removed from the list.
- To add compressed file types (ARJ, CAB, CO_, DO_, EX_, LZH, XL_ and ZIP), click Compressed. The compressed file types are added to the list.
- To restore a list of the default file types, click Default. The original default file types are added to the list.

f. Click OK.

7. Do the following:

- To set the number of compression layers, from the Compression Layers list, select the number of compression layers. The default number of layers is five.
- To include the boot sector, select the *Include boot sector* check box.

8. Under Scan action, do the following:

- To set a scan action, from the *Action when virus found* list select an action.
- To set a scan action if the file cannot be cleaned, from the *Action on uncleanable files* list select an action.

9. Do the following:

- To clean viruses in compressed files, select the *Clean viruses in compressed files* check box.
- To back up files before cleaning, select the *Back up file before cleaning* check box.

10. Click OK.

See also:

[About scan tasks]
[Specifying scan task target]
[Scheduling scan tasks]
[Editing scan tasks]
[Deleting scan tasks]

Scheduling scan tasks

You can configure PC-cillin to automatically run the tasks you create at the frequency you specify. Setting a schedule for your tasks ensures that what you want scanned happens when you want it.

To schedule a scan task:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Scan Tasks link. The Scan Tasks screen appears.
4. Click Add. The Task Configuration dialog box appears.
5. Click the Schedule The Task tab. The Schedule The Task property sheet appears.
6. From the Frequency list, select how often you want to execute the task:

- If you chose *Daily*, in the Time box enter a time (time is in 24 hour clock format).
- If you chose *Weekly*, in the Time box enter a time, and then from the Day of Week list, select a day.
- If you chose *Monthly*, in the Time box enter a time, and then enter a date.

7. Click OK.

See also:

[About scan tasks]
[Specifying scan task target]
[Configuring scan task options]
[Editing scan tasks]
[Deleting scan tasks]

Editing scan tasks

You can edit a scan task including modifying the scan target, file types, scan actions and the frequency that the task executes.

To edit a scan task:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Scan Tasks link. The Scan Tasks screen appears.
4. In the Task List, select the scan task you want to edit.
5. Click Edit. The Task Configuration dialog box appears. Do one of the following:

- To edit the scan target, click the Scan Target tab, and then make your edits.
- To edit the scan options (file types, scan actions), click the Scan Options tab, and then make your edits.
- To edit the frequency, click the Schedule The Task tab, and then make your edits.

6. Click OK.

See also:

[About scan tasks]
[Specifying scan task target]
[Configuring scan task options]
[Scheduling scan tasks]
[Deleting scan tasks]

Deleting scan tasks

You can delete scan tasks if the tasks are no longer useful.

To delete a scan task:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Scan Tasks link. The Scan Tasks screen appears.
4. From the Task List, select the scan task you want to delete.
5. Click Delete. A confirmation message box appears.
6. Click Yes to delete the task.

See also:

About scan tasks
Specifying scan task target
Configuring scan task options
Scheduling scan tasks
Editing scan tasks

Enabling Intelligent Update

Enable Intelligent Update so you never miss the latest PC-cillin update (including: virus pattern files, scan engine, other program files, and Personal Firewall rules). Using the latest updates provides you with the most protection and ensures PC-cillin 2002 is kept current to catch the newest viruses and prevent the latest hacker attacks.

To enable Intelligent Update:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Program Update link. The menu expands.
3. Click Intelligent Update. The Intelligent Update screen appears.
4. Select the *Enable Intelligent Update* check box.
5. Click Apply.

See also:

About Virus Pattern Files
Viewing pattern file and scan engine information
Updating PC-cillin 2002
Updating PC-cillin for Wireless
About Intelligent Update
Scheduling Intelligent Update

Scheduling Intelligent Update

You can configure PC-cillin 2002 to automatically search for updates at the frequency you specify. Setting a schedule for updates ensures PC-cillin has installed the latest components and offers the best protection. You can also set the connection time period for PC-cillin to search for updates.

To schedule Intelligent Update:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Program Update link. The menu expands.
3. Click Intelligent Update. The Intelligent Update screen appears.
4. Make sure the *Enable Intelligent Update* check box is selected and do the following:

   - From the *Update every* list select, how often you want PC-cillin to check for updates.
   - To set a connection time period that restricts PC-cillin from connecting during any other time, select the *Connect only during the specified time period* check box, and then in the From and To boxes enter a time (time is in 24 hour clock format).

5. Click Apply.

See also:

About Virus Pattern Files
Viewing pattern file and scan engine information
Updating PC-cillin 2002
Updating PC-cillin for Wireless
About Intelligent Update
Enabling Intelligent Update

Selecting PDA OS type

Before you update your PC-cillin for Wireless files, you must set the operating system of your PDA.

To select the PDA OS type:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Program Update link. The menu expands.
3. Click the Update PDA link. The Update PDA screen appears.
4. Select your PDA OS type.
5. Click Apply.

See also:

About Intelligent Update
Updating PC-cillin for Wireless
Selecting PDA OS type

About proxy servers

A proxy server is an intermediate server that typically sits between the user and the main server. It can be used to provide security and to speed download times.

Most home users do not use a proxy server, but many offices, schools, and Internet Service Providers do. If you are having trouble downloading virus pattern files or program updates, it may be because you use a proxy server but it has not been identified or there is an error in the address/credentials.

If there is a proxy server between your computer and the Internet, your Web browser is probably configured to use it. Check the online help of your Web browser to find out if you are connected to the Internet using a proxy server. In many cases, you can check whether you have a proxy server connection by checking the Advanced, or Options settings of your Web browser.

See also:

Enabling proxy settings

Entering proxy settings

Enabling proxy settings

If you've determined that you do use a proxy server, you must enable the proxy settings.

To enable proxy settings:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Program Update link. The menu expands.
3. Click the Proxy Settings link. The Proxy Settings screen appears.
4. Select the *Enable proxy setting* check box.
5. Click Apply.

See also:

About proxy servers
Entering proxy settings

Entering proxy settings

If you use a proxy server on your network (for example, you use PC-cillin in an office, school, or your Internet Service Provider requires a proxy server) you need to enter the IP address (number) and port of this proxy server.

In addition, if you use a proxy server and users are required to log on, you need to supply the appropriate logon credentials.

To enter proxy settings:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Program Update link. The menu expands.
3. Click the Proxy Settings link. The Proxy Settings screen appears.
4. Make sure the *Enable proxy setting* check box is selected and do the following:

   - In the Proxy address and Port box, type the IP address and port number of the proxy server.
   - In the User Name and Password boxes, type your proxy server logon credentials.

5. Click Apply.

See also:

[About proxy servers]
[Enabling proxy settings]

About WebTrap

WebTrap protects against malicious Java and ActiveX applets. Although most Web sites are completely harmless, it is possible for someone to create a small program and set it to run, invisibly, whenever their Web page is accessed. These programs may destroy data, steal your passwords or financial data, etc.

PC-cillin's WebTrap protects you against malicious Java and ActiveX programs while allowing harmless ones to pass safely through.

See also:

Enabling WebTrap

Setting WebTrap actions

Enabling WebTrap

With WebTrap enabled, PC-cillin 2002 monitors all Java and ActiveX applets that are silently downloaded to your computer when you are surfing the Web.

To enable WebTrap:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Web Trap link. The WebTrap screen appears.
4. Select the *Enable WebTrap* check box.
5. Click Apply. A message box appears notifying you that the change will not take effect until you restart your computer or log off and log on again.
6. Click Yes.
7. Restart your computer or log on again to immediately enable the function.

Note: A Notification screen briefly appears when you open your browser to inform you WebTrap is enabled. To prevent this screen from displaying, clear the *Display Notification when you open your browser* check box.

See also:

About WebTrap
Setting WebTrap actions

Setting WebTrap actions

You can set different WebTrap actions PC-cillin 2002 will perform when malicious programs are found.

To set a WebTrap action:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Web Trap link. The WebTrap screen appears.
4. Make sure the *Enable WebTrap* check box is selected, and click one of the following:

- **Prompt for action**- PC-cillin informs you of the potentially harmful program and prompts you to specify an action.
- **Block the malicious program**- PC-cillin automatically blocks the harmful program without any user intervention.

5. Click Apply. A message box appears notifying you that the change will not take effect until you restart your computer or log off and log on again.
6. Click OK.
7. Restart your computer or log on again to immediately enable the function.

Note: A Notification screen briefly appears when you open your browser to inform you WebTrap is enabled. To prevent this screen from displaying, clear the *Display Notification when you open your browser* check box.

See also:

About WebTrap

Enabling WebTrap

About the Site filter

For protection against offensive Web content, PC-cillin offers Site filter. This configurable utility lets you make whatever Web sites you want "off limits" to other users of the computer. This function is especially useful for families where many family members use the same computer.

Web sites restricted by the Site filter are listed in the Restricted site list. The Restricted site list displays an icon with the uniform resource locator (URL) of the Web site.

In addition, you can specify the Site filter to allow access to a restricted site, but only after a prompt appears reminding the user you have flagged the site as objectionable.

Note: *Web sites that are completely restricted including all sub-pages have a small cross on the URL icon.*

See also:

Enabling the Site filter
Protecting the Site filter screen
Adding URLs to the Site filter
Editing Site filter URLs
Deleting Site filter URLs

Enabling the Site filter

Enable the Site filter to control access to offensive Web sites.

To enable the Site filter:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Site Filter link. The Site Filter screen appears.
4. Select the *Enable Site filter* check box.
5. If you only want Site filter to warn someone trying to retrieve a restricted site but then allow entry to restricted sites, select the *Permit access to the restricted sites...* check box. If this check box is clear, any Web site in the Restricted sites list will not be loaded and a message will appear in the browser notifying the user they are trying to access a restricted site.
6. Click Apply. A message box appears notifying you that the change will not take effect until you restart your computer or log off and log on again.
7. Click OK.
8. Restart your computer or log on again to immediately enable the function.

See also:

About the Site filter
Protecting the Site filter screen
Adding URLs to the Site filter
Editing Site filter URLs
Deleting Site filter URLs

Protecting the Site filter screen

You can password-protect the list of Web sites you want to restrict. This prevents unauthorized users from viewing or modifying the Site list. After you have enabled the password protection, you should immediately set your password.

Passwords are case-sensitive so *trend*, *Trend*, *TrEnD* are all considered different. The next time and every time you try to view the Site Filter screen, you must provide your password.

If you have password-protected your Site filter screen and try to enable the Site filter on the Quick Access screen, you must supply your password.

To protect your Site filter screen:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Site Filter link. The Site Filter screen appears.
4. Select the *Password required to access this feature* check box. The Set Password button becomes enabled.
5. Click Set Password. The Set Password dialog box appears. Do the following:

   - In the Enter password box, type your password.
   - In the Confirm password box, type the same password.

6. Click OK.
7. Click Apply.

See also:

[About the Site filter]
[Enabling the Site filter]
[Adding URLs to the Site filter]
[Editing Site filter URLs]
[Deleting Site filter URLs]

Adding URLs to the Site filter

You can add the URLs of Web sites that you want to restrict the access.

To add a URL to the Site filter:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Site Filter link. The Site Filter screen appears.
4. Make sure the *Enable Site filter* check box is selected and click Add. The Add Site To Restricted List dialog box appears.
5. In the text box, type the URL of the restricted Web site (for example, www.anywebsite.com). To block the entire Web site including all sub-pages, select the *Extend to all sub-pages* check box.
6. Click OK. The URL appears in the Restricted site list. If you selected the *Extend to all sub-pages* check box, a small cross appears on the URL icon.
7. If you only want Site filter to warn someone trying to retrieve a restricted site but then allow entry to restricted sites, select the *Permit access to the restricted sites...* check box. If this check box is not selected, any Web site in the Restricted sites list will not be loaded and a message will appear in the browser notifying the user they are trying to access a restricted site.
8. Click Apply.

See also:

About the Site filter
Enabling the Site filter
Protecting the Site filter screen
Editing Site filter URLs
Deleting Site filter URLs

Editing Site filter URLs

You can edit the URLs of Web sites you have added to the Restricted Site list.

To edit a Site filter URL:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Site Filter link. The Site Filter screen appears.
4. In the Restricted site list, select the URL you want to edit.
5. Click Edit. The Add Site To Restricted List dialog box appears.
6. In the text box, edit the URL of the restricted Web site. To block the entire Web site, select the *Extend to all sub-pages* check box.
7. Click OK. The modified URL appears in the Restricted site list. If you selected the *Extend to all sub-pages* check box, a small cross appears on the URL icon.
8. To allow a Web site to be viewed after being prompted, select the *Permit access to the restricted sites...* check box.
9. Click Apply.

See also:

About the Site filter
Enabling the Site filter
Protecting the Site filter screen
Adding URLs to the Site filter
Deleting Site filter URLs

Deleting Site filter URLs

You can remove the URLs of Web sites from the Restricted Site list. Once a URL of a Web site is removed from the Restricted Site list, it can readily be accessed.

To delete a Site filter URL:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Internet Security link. The menu expands.
3. Click the Site Filter link. The Site Filter screen appears.
4. In the Restricted site list, select the URL you want to delete.
5. Click Delete. The URL is removed from the list.
6. Click Apply.

See also:

About the Site filter
Enabling the Site filter
Protecting the Site filter screen
Adding URLs to the Site filter
Editing Site filter URLs

About Personal Firewalls

The Trend Micro PC-cillin 2002 Personal Firewall protects your computer against attacks from the Internet. A *firewall* creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic to your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer.

With the PC-cillin 2002 Personal Firewall, you can also control the security level, create a list of sites you know can be trusted, and view a list of blocked ports. The Personal Firewall is actually composed of the following components:

- **Cloaking:** Prevents your computer from being found. Cloaking hides the entry points (ports) of your computer making it appear to be disconnected from a network. Hackers using techniques like NetBIOS browsing, port scanning, or ICMP packet special processing will be unable to locate your computer.
- **Firewall:** Provides a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic coming into your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer. The firewall protects against attacks hackers commonly use including: *Ping of Death, IP conflict*, *SYN flooding*, and others.
- **Trojan Backdoor Blocking:** If a hacker has already broken into your system, he or she could have installed a Trojan (small hidden program) onto your computer (unlike viruses, Trojans do not replicate themselves, but can still wreak havoc on your system). To avoid being traced, the hacker can then use your computer to attack other computers. The Trojan Backdoor Blocking function prevents hackers from using your computer by blocking *Back Orifice*, *Back Orifice 2000*, *Net Bus*, *Deep Throat* and other known back door programs.

There is also an Internet Emergency Lock feature that lets you immediately disable all Internet activity if you suspect you are under attack. Enabling this feature immediately stops all traffic to and from the Internet.

See also:

Enabling your Personal Firewall

About the Personal Firewall security level settings

Anytime your computer connects to another computer the threat of invasion by an outside intruder exists. The more computers connected to your computer, the greater the threat and the higher the probability your computer will be singled out for an attack. Each time you connect to the Internet, there are millions of computers that can also connect to your computer.

Since different users have different needs, PC-cillin provides three levels of security. The High Security level offers maximum protection from outside attacks, while the Low Security level offers minimum protection. Unless you use your computer as a server (Medium), we recommend you use the default setting: *High*.

High (Default): Cloaking, Trojan backdoor blocking, and Firewall all enabled. This is the default and most secure setting. At this security level, your computer's entry points are invisible, and Trojan backdoor programs are blocked. In addition, a barrier filters and examines both incoming and outgoing Internet traffic. This setting is recommended for the expert Internet user that frequently visits many different Web sites, often transfers files online, and receives a lot of email from numerous accounts. Also recommended for users with always-on Internet connections. Do not use this security level if you use your computer as a server; choose the Medium security level.

Medium: Trojan backdoor blocking and Firewall enabled. Use this setting if you use your computer as a server. At this security level, Trojan backdoor programs are blocked, and a barrier filters and examines both incoming and outgoing Internet traffic. However, your computer’s entry points are visible and server-functions will function normally. These settings are also recommended for the casual Internet user who spends less time online, doesn't often transfer files, and only uses one email account.

Low: Firewall enabled. At this security level, a barrier filters and examines both incoming and outgoing Internet traffic. This level is recommended for users that rarely go online, don't transfer files over the Internet, and don't use email on their computer.

See also:

[About Personal Firewalls]
[Enabling your Personal Firewall]

Adjusting the Personal Firewall security level settings

Depending on your needs you can adjust the Personal Firewall security level.

To adjust the Personal Firewall security level settings:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Security Level link. The Security Level screen appears.
4. Make sure the *Enable Personal Firewall* check box is selected and Under Security Level, choose the level of security:

- **High** (Default): Cloaking, Trojan backdoor blocking, and Firewall all enabled.
- **Medium**: Trojan backdoor blocking and Firewall enabled. (Recommended security level if computer functions as a server.)
- **Low**: Firewall enabled.

5. Click Apply.

See also:

About Personal Firewalls
Enabling your Personal Firewall
About the Personal Firewall security settings
About trusted sites
About blocked ports
Activating the Emergency Lock
About Trojans
How Trojans cause damage

About trusted sites

There may be Web sites that you know are safe and will not attack your computer. The Personal Firewall lets you add these trusted sites to a list. You should be absolutely sure a Web site can be trusted before adding it to this Trusted Site list. The Personal Firewall ignores all sites on the Trusted Site list so they can freely connect to your computer.

See also:

About Personal Firewalls

Enabling your Personal Firewall

About the Personal Firewall security settings

Adding trusted sites

Editing trusted sites

Deleting trusted sites

About blocked ports

Activating the Emergency Lock

About Trojans

How Trojans cause damage

Adding trusted sites

You can add Web sites you know to be safe to the Trusted Site list and the Personal Firewall will not block these.

To permit other users to access your computer over a network (typically a LAN), on the Trusted Sites List, select the check box of your network adapter card, and then click Apply.

To add a trusted site:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Trusted Sites link. The Trusted Sites screen appears.
4. Click Add. The IP Settings dialog box appears.
5. In the Description box, type a description of the trusted site you are adding.
6. In the Type box, select a definition type, and do the following:

- **HostName**: in the HostName box type the host name of the trusted site, and then click Resolve to view the IP address.
- **IPAddress**: in the IPAddress box type the IP address of the trusted site.
- **IPRange**: in the IPAddrFrom and IPAddrTo boxes, type the range of IP addresses that are considered safe.
- **Subnet**: in the IPAddress box type the IP address and in the Netmask box type the subnet address for the safe site.

7. Click OK. If you select the check box next to the trusted site, the site is "trusted" and considered safe. If you clear the check box the site is not "trusted".
8. Click Apply.

Note: If you have trouble using resources on a network, (printer or other computers), add the subnet mask to the Trusted Sites List.

See also:

About Personal Firewalls

Enabling your Personal Firewall

Editing trusted sites

You can edit a trusted site including modifying the host name, IP address, IP address range, and the subnet.

To edit a trusted site:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Trusted Sites link. The Trusted Sites screen appears.
4. On the Trusted Sites List, select the site you want to edit.
5. Click Edit. The IP Setting dialog box appears. Do the following:

   - To edit the type of IP setting, select the type from the Type list: HostName, IPAddress, IPRange, and Subnet and make your changes.
   - To edit the description, type your new description in the Description box.

6. Click OK. If you select the check box next to the trusted site, the site is "trusted" and considered safe. If you clear the check box the site is not "trusted".
7. Click Apply.

See also:

About Personal Firewalls

Enabling your Personal Firewall

About the Personal Firewall security settings

About trusted sites

Adding trusted sites

Deleting trusted sites

About blocked ports

Activating the Emergency Lock

About Trojans

How Trojans cause damage

Deleting trusted sites

You can remove sites you no longer trust from the Trusted Sites List.

To delete a trusted site:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Trusted Sites link. The Trusted Sites screen appears.
4. On the Trusted Sites List, select the site you want to delete.
5. Click Delete. A confirmation message appears.
6. Click Yes to remove the trusted site from the Trusted Site list.

If you want to keep the site in the list, but you no longer trust the site, you can clear the site check box.

See also:

About Personal Firewalls
Enabling your Personal Firewall
About the Personal Firewall security settings
About trusted sites
Adding trusted sites
Editing trusted sites
About blocked ports
Activating the Emergency Lock
About Trojans
How Trojans cause damage

About blocked ports

By default, the Personal Firewall blocks a list of ports used by Trojan attacks when malicious individuals try to gain access to your computer. Many network attacks can be avoided by preventing access to these ports.

A *port* is an entry point computers use to connect to networks or to other computers to exchange information. Every port has a unique number and based on this number, the receiving computer determines which application to send received data.

To view the list of blocked ports:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Personal Firewall link. The menu expands.
3. Click the Blocked Ports link. The Blocked Ports screen appears.
4. Under the Port list, you can view the Trojan name, protocol, and the number of the port the Trojan tries to access when attacking.

See also:

About Personal Firewalls

Enabling your Personal Firewall

About the Personal Firewall security settings

About trusted sites

Activating the Emergency Lock

About Trojans

How Trojans cause damage

About viruses

A computer virus is a program that replicates. To do so, it needs to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes. Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage.

Called the damage routine, or payload, the destructive portion of a virus can range from overwriting critical information kept on your hard disk's partition table to scrambling the numbers in your spreadsheets to just taunting you with sounds, pictures, or obnoxious effects.

It’s worth bearing in mind, however, that even without a "damage routine," viruses allowed to run unabated will continue to propagate--consuming system memory, disk space, slowing network traffic and generally degrading performance. Besides, virus code is often buggy and can also be the source of mysterious system problems that take weeks to understand. So, whether a virus is harmful or not, its presence on your system can lead to instability and should not be tolerated.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate--until the preordained trigger day or event when they unleash their damage routines on the host system or across a network.

To learn more about any particular virus, or about viruses in general, you can access Trend Micro's online Virus Encyclopedia at: www.antivirus.com/.

How viruses are created

Until a few years ago, creating a virus required knowledge of a computer programming language. Today anyone with even a little programming knowledge can create a virus. Usually, though, misguided individuals who want to cause widespread, random damage to computers create viruses.

In the typical scenario, it is an individual, working alone, who writes a virus program and then introduces it onto a single computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations. Recently, do-it-yourself "virus kits" have been popping up on the Internet, and macro scripts are becoming both easier to learn and more powerful, putting the capacity to engineer viruses in the hands of nearly everyone. In other words, no single, likely profile exists by which virus writers can be described or understood.

So whatever the reason one may have for writing a virus, the important thing is to make certain your company is not victimized, that data you are responsible for is safe, and that precious time is not wasted hunting down (and cleaning up after) viruses.

Test virus

The European Institute for Computer Anti-Virus Research (EICAR), along with antivirus software vendors, has developed a test file that can be used in checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose "signature " has been included in the Trend Micro virus pattern file and as such, can be detected by the virus scan engine.

You can download this file from:

www.antivirus.com/vinfo/testfiles/

Alternatively, copy the following text into a text editor and then save the file with a *.COM extension.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

You may need to disable real-time scanning before downloading the file and make sure no other antivirus products are running. Once on your machine, you can use the test virus to see for yourself how PC-cillin's various scanning features work.

Accessing the Trend Micro Virus Encyclopedia

PC-cillin includes access to the online Trend Micro virus encyclopedia, organized by name and virus type. Use it to find out about tens of thousands of individual viruses, including the typical symptoms of a given virus, its infection procedure, and the damage routine.

With the growing prevalence of Macro viruses, we've bolstered the number of Macro virus descriptions included in the encyclopedia to well over 2000.

Of course, PC-cillin, which uses Trend's award-winning, 32-bit, multi-threading scan engine, is capable of detecting all viruses that are known to be in circulation, plus the many thousands more that exist as "proof of concept" only in researcher's virus labs and on hacker's computers.

To access the Trend Micro Virus Encyclopedia, on the PC-cillin menu bar, click Security Info > Encyclopedia..

Viewing the Trend Micro Virus list

The Virus Information Center contains a list of the Real-time top ten viruses. In addition, you can view updated Security Alerts and Virus Advisories.

To access the Trend Micro Virus list, on the PC-cillin menu bar click, Security Info > Virus List.

How viruses spread

The most likely virus entry points are email, Internet and network connections, floppy disk drives, and modems or other serial or parallel port connections. In today's increasingly interconnected workplace (Internet, intranet, shared drives, removable drives, and email), virus outbreaks now can spread faster and wider than ever before.

The following are some common ways for a virus to enter your system:

- Email attachments
- World Wide Web (WWW) sites
- FTP traffic from the Internet (file downloads)
- Shared network files & network traffic in general
- Demonstration software
- Pirated software
- Shrink-wrapped, production programs (rare)
- Computer labs
- Electronic bulletin boards (BBS)
- Diskette swapping (using other people’s diskettes for carrying data and programs back and forth)

High risk files

The most dangerous files types are:

.EXE, .COM, .XLS, .DOC, .MDB

Because they don't need any special conversion to infect a computer -- all they've got to do is run, or be opened, and the virus spreads. Trend Micro virus doctors estimate that 99% of all viruses are written for these file formats.

A list of possible virus carriers include:

EXE - (Executable file)

SYS - (Executable file)

COM - (Executable file)

DOC - (Microsoft Word)

DOT - (Microsoft Word)

XLS - (Microsoft Excel)

XLA - (Microsoft Excel)

XLT - (Microsoft Excel)

MDB - (Microsoft Access)

ZIP - (Compressed file, common in the USA)

ARJ - (Compressed file, common in the USA)

DRV - (Device driver)

0VL - (Windows overlay file)

BIN - (Common boot sector image file)

SCR - (Microsoft screen saver)

Most of these file formats, .drv, .ovl, and .bin, for example, are not dangerous in and of themselves; they must be converted in order to be executed.

Boot viruses

Until the mid-1990s, boot sector viruses were the most prevalent virus type, spreading primarily in the 16-bit DOS world via floppy disk. Boot sector viruses infect the boot sector on a floppy disk and spread to a user's hard disk, and can also infect the master boot record (MBR) on a user's hard drive. Once the MBR or boot sector on the hard drive is infected, the virus attempts to infect the boot sector of every floppy disk that is inserted into the computer and accessed.

Boot sector viruses work like this: by hiding on the first sector of a disk, the virus is loaded into memory before the system files are loaded. This allows it to gain complete control of DOS interrupts so that it can spread and cause damage.

These viruses often replace the original contents of the MBR or DOS boot sector with their own contents and move the sector to another area on the disk. Cleaning up a boot sector virus can be performed by booting the machine from an uninfected floppy system disk rather than from the hard drive, or by finding the original boot sector and replacing it in the correct location on the disk.

Direct action virus

A Direct Action virus loads itself into memory to infect other files and then unloads itself, while a companion virus acts to fool an executable file into executing from a .com file. For example, a companion virus might create a hidden pgm.com file so that when pgm command is executed, the fake pgm.com runs first. The .com file invokes its virus code before going on to start the real pgm.exe file.

Macro viruses

Macro viruses currently account for about 80 percent of all viruses, according to the International Computer Security Association (ICSA), and are the fastest growing viruses in computer history. Unlike other virus types, macro viruses aren’t specific to an operating system and spread with ease via email attachments, floppy disks, Web downloads, file transfers, and cooperative applications.

Macro viruses are, however, application-specific. They infect macro utilities that accompany such applications as Microsoft Word and Excel, which means a Word macro virus cannot infect an Excel document and vice versa. Instead, macro viruses travel between data files in the application and can eventually infect hundreds of files if undeterred.

Macro viruses are written in "every man's programming language" -- Visual Basic -- and are relatively easy to create. They can infect at different points during a file's use, for example, when it is opened, saved, closed, or deleted.

Multi-partite viruses

Multi-partite viruses share some of the characteristics of boot sector viruses and file viruses: They can infect .com files, .exe files, and the boot sector of the computer’s hard drive.

On a computer booted up with an infected diskette, the typical multi-partite virus will first make itself resident in memory then infect the boot sector of the hard drive. From there, the virus may infect a PC's entire environment. Not many forms of this virus class actually exist. However, they do account for a disproportionately large percentage of all infections.

Polymorphic or mutation viruses

Polymorphic (mutation) viruses are unique in that they are designed to elude detection by changing their structure after each execution--with some polymorphic viruses, millions of permutations are possible. Of course, this makes it harder for normal antivirus programs to detect or intercept them. It should be noted that polymorphic viruses do not, strictly speaking, constitute a separate category of virus; they usually belong to one of the categories described above.

Stealth viruses

Stealth viruses, or Interrupt Interceptors, as they are sometimes called, take control of key DOS-level instructions by intercepting the interrupt table, which is located at the beginning of memory. This gives the virus the ability to do two important things: 1) gain control of the system by re-directing the interrupt calls, and 2) hide itself to prevent detection.

File infecting viruses

File infectors, also known as parasitic viruses, operate in memory and usually infect executable files with the following extensions: *.COM, *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS. They activate every time the infected file is executed by copying themselves into other executable files and can remain in memory long after the virus has activated.

Thousands of different file infecting viruses exist, but similar to boot sector viruses, the vast majority operate in a DOS 16-bit environment. Some, however, have successfully infected the Microsoft Windows, IBM OS/2, and Apple Computer Macintosh environments.

Methods of virus detection

Three main methods exist for detecting viruses: integrity checking (also known as checksumming), behavior monitoring, and pattern matching (scanning). PC-cillin is scanning based, with further buttressing from Trend Micro's MacroTrap, WebTrap, and ScriptTrap technologies.

Integrity checking

Antivirus programs that use integrity checking start by building an initial record of the status (size, time, date, etc.) of every application file on the hard drive. Using this data, checksumming programs then monitor the files to see if changes have been made. If the status changes, the integrity checker warns the user of a possible virus.

However, this method has several disadvantages, the biggest being that false alarms are altogether too common. The records used by checksumming programs are often rendered obsolete by legitimate programs, which, in their normal course of operations, make changes to files that appear to the Integrity checker to be viral activity. Another weakness of integrity checking is that it can only alert the user after a virus has infected the system.

Behavior monitoring

Behavior Monitoring programs are usually *terminate and stay resident* (TSR) and constantly monitor requests that are passed to the interrupt table. These programs are on the lookout for activities that a virus might engage in--requests to write to a boot sector, opening an executable program for writing, or placing itself resident in memory. The behavior these programs monitor is derived from a user-configurable set of rules.

Pattern matching

Using a process called "pattern matching," PC-cillin draws upon an extensive database of virus patterns to identify known virus signatures, or telltale snippets of virus code. Key areas of each scanned file are compared against the list of thousands of virus signatures that Trend Micro has on record.

Whenever a match occurs, PC-cillin takes the action you have configured: Clean, Delete, Quarantine, Pass (Deny Access for Real-time Scan), or Rename.

About Trojans

Trojans, or Trojan horses, are small seemingly harmless programs. To cause any damage, these programs must be installed onto your system. Once a Trojan is installed, it has all the same privileges as the user of the computer and can exploits the system to do something the user did not intend. The main difference between Trojans and viruses is that Trojans cannot replicate or spread on their own.

See also:

How Trojans cause damage

Trojan System Cleaner

Running the Trojan System Cleaner

Activating the Emergency Lock

How Trojans cause damage

Although a Trojan seems like a harmless program, it actually contains malicious code. Trojans trick your system into accepting them as useful programs. Once a Trojan is installed onto your system this program has the same privileges as you have and can:

- Delete files
- Transmit to the intruder any files you can read
- Change any files you can modify
- Install other programs with your privileges
- Execute privilege-elevation attacks—the Trojan can attempt to exploit a weakness to raise the level of access beyond the user running the Trojan. If successful, the Trojan can operate with increased privileges.
- Install viruses
- Install other Trojans

During installation and every time the Real-time Monitor runs, PC-cillin's Trojan System Cleaner (TSC) scans your system for any Trojans on your system.

See also:

[How Trojans cause damage]
[Trojan System Cleaner]
[Running the Trojan System Cleaner]
[Activating the Emergency Lock]

Contacting Technical Support

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

Send an email to our highly trained technical support staff or visit our Web site to receive technical support.

Trend Micro Technical Support

Email: support@trendmicro.com

URL: www.antivirus.com

To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- PC-cillin program, scan engine, pattern file, version number
- OS name and version
- Internet connection type
- Exact text of any error message given
- Steps to reproduce the problem

See also:

Before Contacting Technical Support
Visiting the Trend Micro User's page
Visiting the Technical Support Web site

Before Contacting Technical Support

While our technical support staff is always pleased to handle your inquiries, there are a couple things you can do to quickly find the answer you are seeking.

- **Check the documentation:** the manual and online help provide comprehensive information about PC-cillin. Search both documents to see if they contain your solution.
- **Visit our technical support Web site:** our technical support Web site contains the most up-to-date information about all Trend Micro products. Other inquiries that were already answered are also posted on the support Web site.

See also:

Contacting Technical Support
Visiting the Trend Micro User's page
Visiting the Technical Support Web site

Visiting the Trend Micro User's page

Visit the Trend Micro user's page to receive the latest news about PC-cillin. As a registered user, you can access information that cannot be found on other Web sites.

To visit the Trend Micro User's page, on the PC-cillin menu bar, click Support > Trend Micro User Home Page.

See also:

Contacting Technical Support

Before Contacting Technical Support

Visiting the Technical Support Web site

Visiting the Technical Support Web site

Visit the Trend Micro Technical Support Web site to find answers to your questions. The Trend Micro Technical Support Web site contains the latest virus and product information.

To visit the Technical Support Web site, on the PC-cillin menu bar, click Support > Technical Support Home Page.

See also:

Contacting Technical Support

Before Contacting Technical Support

Visiting the Trend Micro User's page

How do I reinstall PC-cillin 2002?

The procedure for reinstalling PC-cillin 2002 is the same procedure you used to originally install PC-cillin. When you reinstall PC-cillin on the same computer with the original operating system (i.e., you did not reformat your hard drive or install a different operating system), it is unnecessary to re-register your software.

This procedure is also documented in the Quick Start Guide that came bundled inside the CD case. However, if you cannot find your Quick Start Guide we recommend you print out these instructions so you can refer to them during the installation process.

To reinstall PC-cillin 2002:

1. Insert the PC-cillin program CD into your CD-ROM drive and do the following:

- If the installation program automatically starts. Click Next.
- If the installation program doesn't automatically start, click Start > Run. In the Open box, type d:\setup.exe and click OK (where d:\ is the drive letter of your CD-ROM). Click Next.

2. Click *I accept the terms of the license agreement* to accept and continue installing PC-cillin. The installation procedure will be aborted if you do not accept the terms.
3. Click Next. PC-cillin scans your system memory, boot sector, and critical files before installing the program files. If PC-cillin finds a virus-infected file, PC-cillin either cleans or deletes it. Do the following:

- In the User Name box, type a user name. You must provide a user name to continue installation.
- In the Organization box, type the name of your organization.
- In the Serial Key boxes, type your serial key. If you do not have a serial key, you can continue installation and install a 30-day trial version.
- If you are installing the trial version an additional screen appears when you click Next asking if you want to install the trial version. Select the *I wish to install as trial version* check box and click Next.

4. Click Next. The Destination Folder screen appears. You can choose where PC-cillin is installed or just use the default location. To change the location PC-cillin is installed, click Change and browse to a different folder.
5. Click Next. If you are ready to complete installation, click Install.

Can I install PC-cillin 2002 on another computer?

If you install PC-cillin on another computer, it is necessary to re-register your software after you install PC-cillin. You must perform the *Registering your software* procedure and enter your new License Key. Any previously obtained License Keys are invalid and will not work correctly on another computer.

See also:

New product registration method

Registering your software

What if I lost my serial number?

What happens to my License Key if I reinstall my operating system?

What if I lost my serial number?

Contact your regional Trend Micro technical support representative.

Trend Micro Technical Support

Email: Support@trendmicro.com

URL: www.antivirus.com

See also:

New product registration method

Registering your software

Can I install PC-cillin 2002 on another computer?

What happens to my License Key if I reinstall my operating system?

What happens to my License Key if I reinstall my operating system?

If you reinstall your operating system, it is necessary to re-register your software after you install PC-cillin. You must perform the *Registering your software* procedure and enter your new License Key. Any previously obtained License Keys are invalid and will not work correctly.

See also:

New product registration method

Registering your software

Can I install PC-cillin 2002 on another computer?

What if I lost my serial number?

License Key error... can't register PC-cillin 2002

When you register you software and receive a License Key from the Trend Micro Web site, an error message may appear:

This may have occurred for the following reasons:

- If you accessed the online registration site from a different computer, please try registering again from your own computer. A License Key is created using a combination of your computer information and your PC-cillin serial number.
- You may have mistyped your License Key. Type your License Key exactly as it appears. License Keys are case sensitive.
- If you re-installed your operating system, you must re-register PC-cillin. You have to get a new License Key from the online registration site.

Does PC-cillin 2002 automatically change a user's mail account?

Yes the account name and the name of the incoming POP3 mail server changes. However, if you are using a supported Internet mail client, like Outlook 98 or above, Outlook Express, Netscape Messenger, or Eudora, PC-cillin will automatically make these changes and will not affect you receiving mail.

If you are using an unsupported Internet mail client, modify the mail configuration settings (refer to the documentation of your mail client) by manually changing the incoming server to *localhost* and changing the account name to *name/pop3server* (where *name* is your account name and *pop3server* is the name of your POP3 mail server).

How to set multiple mail accounts?

If you are using a PC-cillin 2002-supported Internet mail client like Outlook 98 or above, Outlook Express, Netscape Messenger, or Eudora, you do not have to perform any special modifications to create multiple mail accounts (refer to your respective mail client documentation for the exact procedures for creating multiple mail accounts).

However, if you are using an unsupported Internet mail client, **for each mail account** modify the mail configuration settings (refer to your mail client documentation) by manually changing the incoming server to *localhost* and changing the account name to *name/pop3server* (where *name* is your account name and *pop3server* is the name of your POP3 mail server).

When virus detected in files with ".RB" extension

When PC-cillin cleans a virus, it creates a backup file before the process. Backup infected files have the extension "RB0", or "RB1"~"RB8". The backup files are created in the same folder as the infected files. When virus clean process succeeds you can delete these backup .RB files.

PC-cillin cannot clean or quarantine viruses from backup .RB files. Therefore, when .RB files are detected during a Manual Scan, PC-cillin cannot clean, quarantine or delete the file. If PC-cillin is configured to quarantine the file when the clean process fails, it cannot quarantine the file, but the file name appears on Quarantined files list. You can delete this .RB file from Quarantined files list but actually it isn't deleted. When you perform a Manual Scan the .RB file will be detected again.

To delete .RB files:

1. On the PC-cillin window, click Settings. The Settings window appears.
2. On the Settings menu, click the Virus Scan link. The menu expands.
3. Click the Manual Scan link. The Manual Scan screen appears.
4. Under Scan action, select Pass from the *Action when virus found* list.
5. Scan all drives manually.
6. When the .RB file is detected, select the file from the list in the Scan Files dialog box.
7. Click Delete. A confirmation message appears.
8. Click Yes to delete the file.

After detecting "MBX" file, can't open received email

PC-cillin with VSAPI 5.400 (or above) can scan "MBX" files (files used by Outlook Express 4.x for mailbox files). Outlook Express 4.x combines multiple mails in one "MBX" file. The VSAPI 5.400 scan engine can scan this "MBX" file and check for viruses. If a virus is detected, PC-cillin can detect the virus but cannot clean the file.

The default setting for a file that cannot be cleaned is "quarantine". Therefore, the "MBX" file will be moved to the Quarantine folder and you cannot access incoming emails. If the "MBX" file is quarantined please restore the quarantined file to original directory to access your email.

Note: Don't delete an "MBX" file. If you delete it, you will lose not only infected email but also all email. Please delete infected email using your email reader. Check the infected file name and then search for the each email's attached file name, and delete the file manually.

What's the difference between WebTrap and the Personal Firewall?

PC-cillin's WebTrap protects you against malicious Java and ActiveX programs while still allowing the harmless ones to pass through safely. WebTrap only scans Java and ActiveX programs. The Personal Firewall makes your computer's entry points invisible to snooping intruders and creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic to your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer.

What do the Personal Firewall log symbols mean?

A packet (information transmitted across a network) was identified as part of an attack and blocked trying to pass the Personal Firewall.

An unauthorized individual tried to connect to your computer (probably using a packet sniffer or other tool). This request was rejected and your computer remains hidden from other computers.

A Trojan horse program (e.g., Back Orifice) attempted to access a computer port that matched a port listed in the Trojan database. Traffic trying to access this computer port was blocked.

Burning a CD-ROM while running PC-cillin 2002

Before burning a CD-ROM, we recommend you exit PC-cillin and turn off real-time scanning. This is to prevent any interference with the CD-ROM burning software. Also make sure you haven’t scheduled a task to occur at the same time you want to burn the CD-ROM.

Reinstalling your operating system

If you reinstall your operating system, you must also reinstall PC-cillin, and re-register your software after installation. You must perform the *Registering your software* procedure and enter your new License Key. Any previously obtained License Keys are invalid and will not function correctly on another computer.

Using a dual boot machine

You must use different serial numbers when you install PC-cillin into dual boot machine.

If you installed both Windows 98 and Windows 2000 using dual boot machine and want to use PC-cillin for your machine, you have to buy 2 license of PC-cillin. In this case, you have to repeat the same installation processes for each OS. You must perform on-line registration once for each OS. Since you use different serial number, you will get different license key for each OS. Please keep registration date.

License key is issued using your serial number and OS information. If you get 2 license keys using different OSs, one license key may be invalid.

Intelligent Update

To receive the latest pattern file and program updates, PC-cillin 2002 detects the computer's Internet connection. If the computer is online and this feature is enabled, PC-cillin automatically connects to the Trend Micro server to check if the latest pattern file or scan engine is available. If a newer component available, a pop-up window appears requesting permission to start downloading. If you choose not to download now, the pop-up window will re-appear 10 minutes later.

With this feature, you do not have to be involved when or how often you update your software. As long as you use your computer and the Internet, PC-cillin always informs you when you can update your software.

License Key

You need the License Key to complete the registration process. When you register your software online, you receive a License Key from Trend Micro via email. After you enter this License Key into the correct field on the PC-cillin window and click Finish, the product is officially registered and you receive the following benefits: a year of virus pattern file updates, technical support, and information about future updates and the latest virus threats.

When you reinstall PC-cillin on the same computer with the original operating system (i.e., you did not reformat your hard drive or install a different operating system), it is unnecessary to re-register your software.

However, if you install PC-cillin on another computer or reinstall your operating system, it is necessary to re-register your software and obtain a new License Key. You must perform the Registering your software procedure and enter your new License Key. Any previously obtained License Keys are invalid and will not work correctly on another computer.

log

PC-cillin keeps running logs of all update, virus, Site filter, and Personal Firewall activity. These logs can be viewed from the View Logs screen and provide a valuable source of information. You can export these logs to print them or examine them in more detail. You can also delete them if they begin to take up too much space on your hard disk.

In addition to displaying the date and the time of each recorded log, the various log types provide log-specific information.

Internet mail scan

PC-cillin can scan email attachments retrieved from a POP3 mail server (supported POP3 mail clients include: Microsoft Outlook 98 and above, Microsoft Outlook Express 4 and above, Netscape Messenger, and Eudora Pro 4.0 and above).

Virus-infected email attachments are now the primary means of virus infection. Due to the ubiquity of email communication, many virus writers are now writing viruses that exploit the vulnerabilities of email clients.

MacroTrap

Trend Micro's MacroTrap performs a rules-based, line-by-line examination of all macro code that is saved in association with a document. This code analysis is called a "heuristic," or "intelligent" search because it allows the virus engine to detect new viruses that have not been included in the virus pattern file.

Macro virus code is typically contained as a part of the invisible template (.dot, for example, in Microsoft Word) that travels with many documents. MacroTrap checks the template for signs of a Macro virus by seeking out key instructions that perform virus-like activities--instructions to copy parts of the template to other templates (replication) or to execute potentially harmful commands (destruction).

Macro viruses are the most common type of viruses, responsible for the greatest number of infections. This is because macro viruses are relatively easy to produce, spread easily (for example via email attachments), and are platform independent. Any computer running Word, for example, can become infected with the Concept virus -- regardless of whether the Word document is opened on a PC, an iMac, or on another platform.

PDA

A small handheld computing device, a personal digital assistant (PDA), provides computing, storage, retrieval, and networking. Manufacturers have provided PDAs with a number of methods for communicating with other devices, from infrared transmitters to mobile phones. High-end PDAs also feature Internet connectivity.

Pattern file

A pattern file, or virus pattern file, is a database of the known virus binary patterns. These binary patterns or signatures serve as a "fingerprint" the PC-cillin scan engine uses to detect viruses in email, FTP, and Web traffic. As new viruses are written and released out into the public, Trend Micro collects their tell-tale signatures and incorporates the information into the pattern file.

Updated pattern files are available every week or so and you should make sure your pattern files are the latest version Trend Micro has released. Updates are available for one year to registered PC-cillin users.

Rescue Disks

A "rescue disk" is a bootable floppy disk that PC-cillin can create if you are running Windows 95/98/Me. Rescue disks should be checked for viruses and write-protected. In addition to this disk, PC-cillin backs up some critical system files and copies them to other floppy disks. You need multiple disks for the complete set of rescue disks.

Personal Firewall

The Trend Micro PC-cillin 2002 Personal Firewall protects your computer against attacks from the Internet. A *firewall* creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic to your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer.

Actually composed of three components (cloaking, firewall, Trojan backdoor blocking), the Personal Firewall lets you control the security level, create a list of sites you know can be trusted, and view a list of blocked ports.

Real-time Scan

Real-time scanning provides constant protection against viruses. With real-time scanning enabled, you reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), we recommend that you always keep real-time scanning enabled.

The real-time scanner checks files for viruses whenever they are used, for example each time a file is opened, copied, moved, saved, compressed or decompressed, downloaded from the Internet, and in the case of email attachments, read.

Besides monitoring file operations, real-time scanning offers protection against viruses entering your system from the Internet via file downloads (HTTP and FTP) and through infected email attachments. It even monitors compressed files such as ZIP files as they are decompressed.

Real-time Monitor

The Real-time Monitor is located in the system tray and is used to quickly perform commonly used functions. For example, you know at a glance if real-time scanning is enabled (the lightning streak icon is red) or disabled (the lightning streak icon is grey).

The Emergency Lock is activated. All incoming and outgoing Internet traffic is halted.

PC-cillin is connecting to the Trend Micro server to download the latest updates.

Your computer is currently under attack.

The real-time scanning function is enabled.

The real-time scanning function is disabled.

The Real-time Monitor is also a useful tool for doing the following:

- Opening the PC-cillin window
- Enabling the Emergency Lock
- Enabling real-time scanning
- Opening the Settings window
- Viewing the real-time status
- Exiting the Real-time monitor

Scan Now (Manual Scan)

If you suspect that a file, folder, or drive has been infected and you want immediate confirmation about the status, run Scan Now (Manual Scan). If during Scan Now, PC-cillin detects a virus, PC-cillin takes the action you have specified in your Scan Now settings.

Scan tasks

For a quick and convenient way to perform a variety of virus scanning, use scan tasks. Scan tasks automates routine antivirus maintenance procedures on your desktop and improves antivirus management efficiency.

Site Filter

Site Filter offers customized protection against offensive Web content. Trend Micro's user-configurable Site Filter function lets you specify whatever Web sites you want "off limits" to other users of the computer. This function is especially useful for families where family members, including children, share one computer.

WebTrap

Although most Web sites are harmless, it is possible for someone to create a small program and configure it to run invisibly whenever a Web page is accessed. These types of programs can destroy data, steal your passwords or financial data, etc.

WebTrap protects your computer against malicious Java and ActiveX applets while allowing harmless ones to pass safely through.