

PC-cillin™ Internet Security 2005

Superior protection for your PC and home network

Quick Start Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Quick Start Guide, which are available from the Trend Micro Web site at:

<http://www.trendmicro.com/download/>

A Maintenance Agreement is a contract between you or your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Note: The Maintenance Agreement expires. Your License Agreement does not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro. If not renewed, you will not receive Maintenance.

You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

<https://olr.trendmicro.com/registration/>

Trend Micro, the Trend Micro t-ball logo, PC-cillin, MacroTrap, ScriptTrap, and TrendLabs are trademarks or registered trademarks of Trend Micro,

Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 1995 - 2004 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. PCEM22032/40920

Release Date: October 2004

Protected by U.S. Patent No. 5,951,698

The Quick Start Guide for Trend Micro PC-cillin Internet Security™ 2005 is intended to introduce the main features of the software and installation instructions for your computer. Read it before installing or using the software.

Detailed information about how to use specific features within the software is available in the online help file and Trend Micro's Web-based Knowledge Base.

At Trend Micro, we are always interested in improving our documentation. If you have questions, comments, or suggestions about any Trend Micro document, please contact us at docs@trendmicro.com. Your feedback is welcome.

Contents

Chapter 1: Welcome to Trend Micro™ PC-cillin™ Internet Security 2005

Hit the Ground Running...	1-2
What Trend Micro PC-cillin Internet Security does right from the outset	1-3
What you can do with the click of a button:	1-3
What's New in PC-cillin Internet Security	1-4
Minimum System Requirements	1-6
Essential Getting Started Tasks	1-7
Installing Your Software	1-8
Registering PC-cillin Internet Security	1-9
Updating PC-cillin Internet Security	1-10
Upgrading Trial Version Software	1-11
Safer Computing Practices	1-12

Chapter 2: Getting to Know Trend Micro PC-cillin Internet Security

How Trend Micro PC-cillin Internet Security Protects Your Computer	2-2
Opening the Trend Micro PC-cillin Internet Security Main Window	2-4
Using Trend Micro PC-cillin Internet Security	2-4
Using the Task Tray Icon	2-6
Identifying program icons	2-7
Viewing System Information	2-7
Viewing product information	2-7
Viewing Internet Security status	2-8
Viewing Antivirus status	2-9
Viewing Event logs	2-9
Introducing the Outbreak Warning System	2-11
Accessing Online Help	2-12

Chapter 3: Protecting Your Files and Data

Confirming Real-time Scan is Enabled	3-1
--------------------------------------	-----

Confirming Mail Scan is Enabled	3-2
Scanning Your Entire Computer	3-3
Scanning a Folder or File	3-3
Running Scan Tasks	3-4
Detecting Spyware and Additional Internet Threats	3-5
Searching For and Cleaning Trojans	3-6
Checking for Known Security Vulnerabilities	3-6
Protecting Your Private Data	3-7
Reducing Spam	3-9
Anti-Spam for Outlook™	3-10

Chapter 4: Dealing with Viruses

Understanding Viruses	4-1
What to Do When a Virus is Detected	4-2
Actions On Uncleanable Files	4-2
Cleaning Boot Viruses	4-3

Chapter 5: Guarding Your Internet Connection

Introducing the Personal Firewall	5-1
Enabling the Personal Firewall	5-2
Understanding Personal Firewall profiles	5-3
Halting Internet Traffic	5-3
Blocking Network Viruses	5-4
Filtering Inappropriate Web Content	5-5
Blocking predefined Web site categories	5-7

Chapter 6: Getting Support

Before Contacting Technical Support	6-1
Visiting the Customer Care Center	6-2
Visiting the Technical Support Web Site	6-2
Contacting Technical Support	6-2
TrendLabs™	6-3
Sending Your Infected Files to Trend Micro	6-3

Appendix

Working With Rescue Disks	A-1
Enabling and Configuring Proxy Settings	A-3



Welcome to Trend Micro™ PC-cillin™ Internet Security 2005

Trend Micro PC-cillin Internet Security protects your computer against Internet threats such as viruses, spyware, hackers, and spam. In addition, PC-cillin Internet Security secures your personal information, blocks unwanted Web sites, checks your computer for known Microsoft security vulnerabilities, and checks email for viruses. This program provides a simple interface to access powerful functionality. New features help ensure that all areas of your Internet and network connection are secure.

Unsolicited commercial email, also known as spam, is a costly and annoying problem. PC-cillin Internet Security contains a powerful anti-spam feature that lets you filter unwanted email.

PC-cillin Internet Security is designed to detect and block spyware, adware, and additional Internet threats. Spyware is often installed alongside programs downloaded from the Internet, and may track information such as the Web sites you visit and the purchases you make from the Internet.

Private Data Protection allows you to specify important personal information, such as your credit card number, home address, or telephone number that you do not want sent over the Web or in messages. Trend Micro PC-cillin Internet Security will block and log any attempts to send this data.

Additionally, PC-cillin Internet Security includes outgoing (SMTP) email scanning, which protects other users from being infected by an email

message from your machine. PC-cillin Internet Security scans all messages and attachments before they leave your computer.

You can even remotely control PC-cillin Internet Security on other computers on your home network and detect intruders into your network, using the new Home Network Control and Wi-Fi Detection features.

The innovative Outbreak Warning System protects your computer against the latest virus outbreaks and security threats. The Outbreak Warning System warns you in advance of new network virus infections and prompts you to update your software to prevent infection.

This chapter contains the following sections:

- Hit the Ground Running... on page 1-2
- What's New in PC-cillin Internet Security on page 1-4
- Minimum System Requirements on page 1-6
- Essential Getting Started Tasks on page 1-7
- Installing Your Software on page 1-8
- Registering PC-cillin Internet Security on page 1-9
- Updating PC-cillin Internet Security on page 1-10
- Safer Computing Practices on page 1-12
- Upgrading Trial Version Software on page 1-11

Hit the Ground Running...

Even before you completely install Trend Micro PC-cillin Internet Security, it checks your main operating system files for viruses and Trojan horse programs. Then after it is installed, PC-cillin Internet Security helps keep your computer free from infection with a series of pre-defined automated tasks.

What Trend Micro PC-cillin Internet Security does right from the outset

Without having to configure anything, PC-cillin Internet Security will do the following:

- Check for viruses every time you open, copy, move, or save a file
- Protect against downloading infected files
- Detect and clean Trojans
- Block spyware
- Scan your email messages and attachments as they are being downloaded from the POP3 email server or sent via an SMTP server, and scan webmail attachments as they are being downloaded from a Webmail server. See Minimum System Requirements on page 1-6 for a list of supported email applications.
- Protect your computer against attacks from the Internet using the Personal Firewall
- Monitor your Microsoft Word™ and Excel™ sessions for macro viruses, using MacroTrap™, a system that detects macro viruses through heuristics, rule-based methods, rather than through pattern matching
- Check for unknown viruses based on their “behavior”, using advanced heuristic technology
- Scan all files on your hard drive according to a default scheduled scan task
- Scan all program files for viruses according to a default scheduled scan task

What you can do with the click of a button:

- Scan every file on your computer
- Scan any file from Windows Explorer or My Computer by right-clicking the file icon
- Scan floppy disks
- Check all Word or Excel documents for macro viruses
- Scan your computer for spyware, adware, and additional Internet threats

What's New in PC-cillin Internet Security

As viruses and other malicious programs become stronger and cleverer, Trend Micro PC-cillin Internet Security also continues to become more powerful to provide complete personal virus protection and Internet security.

Feature	Description
Home Network Control	Home Network Control enables you to control supported Trend Micro software installed on other computers on your local area network (LAN). You can scan other computers on the network for viruses, update their program components, and check them for known Microsoft security vulnerabilities. You can also configure and view the properties and logs of the Trend Micro software on other networked computers.
Wi-Fi Detection	Wi-Fi Detection monitors your network and warns you of unwanted intrusions. Since accessing a wireless network is much easier than making a physical connection, network intrusion has become a serious security problem. PC-cillin Internet Security will scan your network at the interval you specify, and warn you when new computers connect.
Spyware scan and clean	Many Internet threats are not viruses or other inherently malicious code. Rather, they are applications that compromise your privacy, allow hackers to take control of your computer without your knowledge, or annoy you. They are frequently unknowingly downloaded along with desired applications. These threats include spyware, adware, dialers, joke programs, hack tools, remote access tools, password cracking applications, and other uncategorized software. PC-cillin Internet Security can scan for and clean these threats manually, or as a part of a Real-time Scan.
Lightweight installation mode	The Lightweight installation mode allows you to install PC-cillin Internet Security with only Real-time Scan enabled, for users who desire only virus and spyware protection, with very little user interaction.

<p>Security vulnerability check</p>	<p>Security Check inspects your computer for vulnerabilities that Trend Micro has identified as presenting a significant risk. These vulnerabilities or “security holes” make it easy for attackers, network viruses, or other Internet threats to harm your computer. Microsoft has publicly identified these vulnerabilities as issues that exist in their software. Patching security holes helps significantly reduce the chance your computer will be attacked or infected by viruses.</p>
<p>Turbo Scan</p>	<p>Turbo Scan allows you to speed up Manual Scan by skipping files that have already been scanned. When Turbo Scan is enabled, PC-cillin Internet Security keeps a record of files that have been scanned. If there have been no changes to the file since it was last scanned, it is not scanned again. This can substantially reduce the time required for a Manual Scan.</p>

Minimum System Requirements

The following are the minimum software and hardware requirements to run Trend Micro PC-cillin Internet Security.

Operating System:

- Microsoft™ Windows™ XP Home or Professional with Service Pack 1 or 2, 2000 Professional with Service Pack 4, Me, 98SE, 98

CPU:

- Intel™ Pentium™ 233MHz or equivalent processor for Windows 98, 98SE, Me
- Intel Pentium 300MHz or equivalent processor for Windows 2000, XP

Memory:

- 64MB of RAM (128MB or more recommended) for Windows 98, 98SE, Me, 2000
- 128MB of RAM for Windows XP

For all installations:

- Internet Explorer 6.0 with Service Pack 1
- 100MB of available hard disk space for installation
- Supported email clients for Mail Scan, Anti-spam, and Private Data Protection: Microsoft Outlook™ Express™ 6.0, Microsoft Outlook 2000–2003, Netscape™ Mail 7.1, Eudora™ Pro 6.0, Becky!™ Internet Mail version 2.
- Webmail Scan supported webmail accounts: MSN Hotmail, Yahoo! Mail, AOL Mail
- Private Data Protection supported instant messaging applications: Windows Messenger 4.7 and 5.0, MSN Messenger 6.2, ICQ Lite

Note: An Internet connection is required to perform online registration, update, and other online services.

Essential Getting Started Tasks

This section provides a list of the most important tasks you have to complete to get up and running with Trend Micro PC-cillin Internet Security. To effectively use this program and start protecting your computer, Trend Micro strongly recommends that you perform all of these tasks.

Task	Topic
Install the software	See Installing Your Software on page 1-8 .
Register the software	See Registering PC-cillin Internet Security on page 1-9 . Register your software to enable updates. PC-cillin Internet Security needs to regularly update component files to stop the latest viruses.
Perform a Manual Update	See Updating PC-cillin Internet Security on page 1-10 . As people constantly unleash new viruses, Trend Micro strongly recommends that you perform regular component updates. Enable the Intelligent Update option to let PC-cillin Internet Security automatically update itself.
Manually Scan all files	See Scanning Your Entire Computer on page 3-3 . Perform a complete scan of your computer to ensure there are no viruses or other malicious programs hiding on your computer

Installing Your Software

Installing Trend Micro PC-cillin Internet Security is simple and only takes a few minutes.

Important: Before installation, remove any existing antivirus software including previous versions of any Trend Micro antivirus software except PC-cillin Internet Security 2004 or PC-cillin Antivirus 2004.

To install PC-cillin Internet Security:

1. Insert the PC-cillin Internet Security program CD into your CD-ROM drive, and do the following:
 - If the menu automatically appears, click **Install Program**, and then click **Next**.
 - If the installation program does not automatically start, from the Windows Taskbar click **Start > Run**. In the **Open** field, type `D:\Setup\setup.exe` and click **OK** (where D:\ is the drive letter of your CD-ROM). Click **Next**.
2. Read the license agreement, then click **I accept the terms in the license agreement** to continue installing PC-cillin Internet Security. The installation procedure will quit if you do not accept the terms.
3. Click **Next**. PC-cillin Internet Security scans your computer's memory, boot sector, and critical files before installing the program files. If PC-cillin Internet Security finds an infected file, it cleans or deletes it. The **Registration Information** screen appears. Do the following:
 - In **User name**, type a user name. A user name is required to continue installation.
 - In **Organization**, type the name of your organization.
 - In **Serial number**, type your serial number. If you are upgrading from Trend Micro Internet Security 2004 or Antivirus 2004, use your existing serial number.
4. Click **Next**. The **Installation Location** screen appears. You can choose where PC-cillin Internet Security will be installed or use the default location. To change the location click **Change**, and then browse to the desired location.

5. Click **Next**. The **Installation Type** screen appears. You can install the full version of PC-cillin Internet Security, or only the antivirus functions. If you select **Antivirus Only**, network control and security features such as Personal Firewall, Wi-Fi Detection, and Emergency Center will not be installed. Trend Micro recommends that you select this option only if you are using other firewall software.
6. Click **Next**. The **Configuration Type** screen appears. Choose to install with the recommended default, or select the **Lightweight** mode to enable only Real-time Scan and Intelligent Update. You can change your settings at any time after installation.
7. Click **Next**. If you are satisfied with the selections you have made, click **Install** to begin installation.
8. After installation, the wizard informs you that the installation is successful, and PC-cillin Internet Security has been started. Click **Finish** to exit the installer.

If the installer needs to restart the computer, close all running programs and click **Yes** to restart.

Registering PC-cillin Internet Security

Take a few minutes to register your software online. Registration enables component updating.

Important: Register your software to enable component updates. Regularly update to keep your computer protected.

To register Trend Micro PC-cillin Internet Security:

1. Make sure you are connected to the Internet.
2. On the PC-cillin Internet Security main window, click **Updates and Registration > Registration**.
3. Confirm that your serial number displays correctly, and then click **Register Now**.
4. In the appropriate fields on the **Register** Web page, type your name, email address, and other required information.

5. Click **Preview**. Confirm that the information you entered is correct.
6. Click **Submit**. Make sure the email address for your User ID is correct and then type a password.
7. Confirm the password is correct, and then click **Submit**. Your license key is displayed, and a confirmation email message is sent to the User ID email address.

You have registered your software and are a Trend Micro Customer Care Center member. You can now download updates to PC-cillin Internet Security.

Note: If you have trouble viewing the Registration page, you may need to configure your proxy settings. Refer to *Enabling and Configuring Proxy Settings* on page A-3 in the Appendix for instructions.

Updating PC-cillin Internet Security

To protect your computer against the latest threats, regularly update your program files, scan engine, virus pattern files, and other components. Updated pattern files are released by Trend Micro on at least a weekly basis. Updating your pattern file provides you with the most up-to-date protection and lets Trend Micro PC-cillin Internet Security scan for the latest viruses or other malicious programs.

Important: Since Trend Micro virus experts discover hundreds of new viruses every month, Trend Micro strongly recommends you regularly update PC-cillin Internet Security.

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 Internet Security can act on the new instructions in the virus pattern to detect and remove viruses.

Note: Register your software to enable component updates.

To update the virus pattern file and scan engine manually:

1. On the PC-cillin Internet Security Main window, click **Update Components**. The **Update** screen appears. If the update process does not begin, click **Update**. The meter displays the update progress.
2. To halt the update, click **Stop**. To resume updating, click **Update**.

To automatically search for and download the latest pattern and program files from the Trend Micro ActiveUpdate server, Trend Micro recommends you schedule the Intelligent Update function. This powerful function keeps PC-cillin Internet Security and all its components updated to offer you maximum protection with minimum user intervention.

To regularly schedule program component updates:

1. On the PC-cillin Internet Security main window, click **Updates and Registration > Update Settings**.
2. Make sure **Enable Intelligent Update...** is selected, and select how often you want PC-cillin Internet Security to check for updates.
3. Click **Apply**.

Upgrading Trial Version Software

Upgrade your software and register online to take full advantage of Trend Micro PC-cillin Internet Security. Upgrading your software to the registered version enables you to continue using all PC-cillin Internet Security functions.

A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at the then-current Maintenance fees.

If you are using a trial version, click **Buy Now** on the splash screen that appears when you start PC-cillin Internet Security 2005, and follow the on-screen instructions.

Safer Computing Practices

Take the following proactive measures to help prevent your computer from becoming infected.



Make sure Real-time Scan is enabled – Real-time Scan provides constant protection against viruses. With Real-time Scan enabled, you significantly reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), Trend Micro recommends that you always keep Real-time Scan enabled.



Update Trend Micro PC-cillin Internet Security – Register your software and download the latest versions of the pattern files, scan engine, and program components to ensure PC-cillin Internet Security uses the latest protection technology. Also, schedule PC-cillin Internet Security to automatically perform updates using Intelligent Update.



Beware of suspicious email attachments – Email is the most common way viruses and malicious code spread. If you receive an email message from someone you do not know, you should not save or run any files attached to the message. Also, regardless of who sent you the message, be suspicious of email attachments that contain executable files (.exe, .com).



Set scheduled scan tasks – Scan tasks are a quick and easy way to schedule a variety of scans. Using scan tasks lets you configure the type of files to search and how often to perform the scan. For example, you could set a scan task to scan all types of files on your computer, every Friday night at 10:00 PM.



Keep informed – Regularly visit the Trend Micro Web site (www.trendmicro.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.



Update Microsoft Windows – Microsoft responds to security issues in their software by releasing patches and other updates on their Web site. Microsoft Windows operating systems provide a Windows update function that allows you to easily download and update these files. Use Security Check to determine if your computer is up-to-date.



Getting to Know Trend Micro PC-cillin Internet Security

This chapter contains sections that help you become familiar with PC-cillin Internet Security. In addition, it introduces Outbreak Warnings and describes how to access the PC-cillin Internet Security online help.

Included in this chapter are the following sections:

- How Trend Micro PC-cillin Internet Security Protects Your Computer on page 2-2
- Opening the Trend Micro PC-cillin Internet Security Main Window on page 2-4
- Using the Task Tray Icon on page 2-6
- Viewing System Information on page 2-7
- Introducing the Outbreak Warning System on page 2-11
- Accessing Online Help on page 2-12

How Trend Micro PC-cillin Internet Security Protects Your Computer

PC-cillin Internet Security is designed to protect your computer from both external and internal threats.

Threat	PC-cillin Internet Security Protection
External (incoming) – viruses and other malicious programs, such as Trojans and worms, and infected email or attachments	<p>Real-time Scan is designed to detect and scan any file downloaded, copied, or moved to your computer.</p> <p>Mail Scan checks incoming (POP3) and outgoing (SMTP) mail for viruses. Webmail Scan provides protection from infected webmail attachments.</p>
Internal (local machine) – viruses and other malicious programs (for example, Trojans, worms)	<p>Manual Scan (on-demand) and Scheduled Scan tasks check your local machine.</p> <p>PC-cillin Internet Security is designed to detect the activity of Trojan horse programs, recover operating system files modified by Trojans, stop their processes, and delete the files Trojans drop.</p>
Virus Outbreaks	<p>Outbreak Warning System proactively warns you of virus outbreaks or other high-risk situations and advises you to update PC-cillin Internet Security.</p> <p>Instantly halt all Internet traffic if you suspect an outbreak or other suspicious activity.</p>
Malicious hackers	<p>Personal Firewall helps provide protection from external attacks. Exception lists let you configure Personal Firewall to your needs.</p>
Inappropriate Web sites	<p>URL Filter lets you block inappropriate Web sites from loading. You can define lists of Approved or Blocked sites, or select predefined categories to filter out.</p>

<p>Spam email messages</p>	<p>The PC-cillin Internet Security anti-spam engine identifies spam email messages and tags them so they can be filtered.</p>
<p>Private data collection</p>	<p>Private Data Protection allows you to specify personal information (such as your credit card number, or your home address) that PC-cillin Internet Security will block from being transmitted over the Web or in messages.</p>
<p>Wireless Ethernet (Wi-Fi) network intrusion</p>	<p>Wi-Fi Detection scans your network to determine who is connected to it. Firewall profiles give you the flexibility to change Personal Firewall settings depending on your computing environment. For example, you can configure a Wi-Fi Protection profile to help secure your computer when accessing an untrusted wireless LAN environment.</p>
<p>Known Microsoft security vulnerabilities</p>	<p>Security Check inspects your computer for vulnerabilities that make it easy for attackers, viruses, or other Internet threats to harm your computer. Microsoft has publicly identified these vulnerabilities as issues that exist in their software.</p>
<p>Spyware and additional Internet threats</p>	<p>PC-cillin Internet Security detects and removes spyware, adware and additional Internet threats, which are often installed secretly with legitimate programs downloaded from the Internet. Spyware tracks and reports your personal data, such as the Web sites you view and what you purchase online. Other applications in this category allow hackers to take control of your computer without your knowledge, or annoy you.</p>


Opening the Trend Micro PC-cillin Internet Security Main Window

The tab interface of PC-cillin Internet Security provides quick access to all areas of your antivirus and Internet security settings.

To view the PC-cillin Internet Security Main window:

- From the Windows Taskbar, click **Start > Programs > Trend Micro PC-cillin > Trend Micro PC-cillin Internet Security 2005**.

or

In the system tray, right-click the PC-cillin Internet Security icon  and click **Open Main**. (The system tray is next to the clock, on the bottom right hand side of your screen.)







- The PC-cillin Internet Security Main window appears.

Using Trend Micro PC-cillin Internet Security

The redesigned interface gives you quick access to Trend Micro PC-cillin Internet Security settings and summary information. There are buttons at the top of the Main window for frequently accessed functions:

Quick Link	Description
Scan for Viruses	Scans your computer, according to your specified Manual Scan settings.
Update Components	Checks for the latest virus pattern file and program components on the Trend Micro ActiveUpdate server, the Internet server where updates for all Trend Micro products are located. Internet access is required.
Scan for Spyware	Scans your computer for Spyware, adware, and additional Internet threats.
Help	Provides quick access to the online help file, product information, Customer Care Center, and other online resources including the Technical Support Web site, Virus Information Center, and the Virus Encyclopedia.

Each of the buttons on the left hand side of the interface lets you manage the functions for a specific security area.

To perform the following actions:	Click:
View a summary of your antivirus and security status, and event logs.	 Summary
Configure scan settings and quarantine files, perform a scan task, or check for spyware or security vulnerabilities.	 System
Configure Mail Scan, Web Scan, and Anti-spam settings.	 Email
Configure the URL Filter, Private Data Protection, Home Network Control, and Password settings.	 Network Control
Configure the Personal Firewall and Wi-Fi Detection, and view the Emergency Center.	 Network Security
View your update settings, perform a manual update, and register your software.	 Updates and Registration





Using the Task Tray Icon

Using the Trend Micro PC-cillin Internet Security icon in the task tray is the quickest way to access certain functions, for example, displaying the Main window. It also lets you know at a glance if Real-time Scan is enabled or disabled.

To:	Do the following:
Open the Main window	Right-click the Task tray icon and click Open Main .
Exit PC-cillin Internet Security	Right-click the task tray icon and click Exit .
Halt all Internet Traffic	Right-click the task tray icon and click Halt Internet Traffic .
Perform an update	Right-click the task tray icon and click Update Components .
Scan your computer for viruses	Right-click the task tray icon and click Scan for Viruses .
Check your computer for known Microsoft security vulnerabilities	Right-click the task tray icon and click Check Security .
Change your Personal Firewall profile	Right-click the task tray icon and click User Profile , then select the new profile to use.
Enable or disable Real-time Scan	Right-click the task tray icon and click Real-time Scan .

Identifying program icons

Use the table below to learn the meanings of Trend Micro PC-cillin Internet Security task tray icons.

Icon	Description
	All incoming and outgoing Internet traffic has been stopped (to enable Internet traffic, refer to Halting Internet Traffic on page 5-3)
	Connecting to the Trend Micro server to download the latest updates
	Real-time Scan is enabled (red lightning bolt).
	Real-time Scan is disabled (gray lightning bolt). To enable Real-time Scan, refer to Confirming Real-time Scan is Enabled on page 3-1

Viewing System Information

Both summary and detailed information about your antivirus and Internet security is available through Trend Micro PC-cillin Internet Security. You can view summary information to quickly check which settings are enabled, or you can view the logs for details of security, antivirus, and program events.

Viewing product information

It is important to make sure your pattern files and scan engine are kept up to date. Using the latest version of these components ensures you have the most updated virus protection Trend Micro can offer. To confirm you have the

latest updates, you can view your current pattern file and scan engine version.

To view important product information:

- Click **Help > About**.

Your serial number is also displayed. If you contact technical support or an authorized reseller for help with an issue or to re-install Trend Micro PC-cillin Internet Security, you need your serial number.

You can check the latest available pattern file and scan engine versions by visiting the Trend Micro Virus Information Center.

To visit the Trend Micro Virus Information Center:

- Click **Help > Virus Information Center**.

Viewing Internet Security status

The Internet Security status window provides a quick overview of the status of your Internet security. It allows you to quickly assess whether your computer is secure in the following areas: Personal Firewall, URL Filter, Private Data Protection, Wi-Fi Detection, and Anti-spam.

To view Internet Security status:

- Click **Summary > Internet Security Status**.

The **Last attack information** box shows the most recent attempt to attack or scan your computer. This information is only applicable if your Personal Firewall is enabled.

The **Internet security settings** box shows the current enabled/disabled status of the Internet security settings. Click the link to display the configuration window for each setting.

The **Internet traffic monitoring** box displays the total amount of traffic received and sent. An increase in sent or received traffic when you are not using any Internet services may indicate Trojan or virus activity.

Viewing Antivirus status

The Antivirus status window provides a summary of your antivirus scanning and update settings. Use this page to check the overall status of your antivirus settings, and to view antivirus statistics.

To view the Antivirus status:

- Click **Summary > Antivirus Status**.

The **Scan and virus status** box shows information about the last virus and infected file found, the last file scanned, and the times of your last manual and scheduled scans.

The **Update and scan settings** box shows the current enabled/disabled status of the antivirus security settings. Click the link to display the configuration window for each setting.

Viewing Event logs

Trend Micro PC-cillin Internet Security keeps logs for all update, virus, URL filter, Trojan Cleanup Service, Private Data Filter, Anti-spam, and Personal Firewall events. These logs can be viewed from the Event logs screen and provide a valuable source of information. For example, you can view the virus type to learn if it is a Trojan or a worm and should be deleted rather than quarantined.

To view event logs:

1. Click **Summary > Event Logs**.
2. Select the type of log you would like to view from the drop-down list, then click **View Logs**.

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

Log	Entries are created when:
Virus	A virus or other malicious program is detected. Virus log entries also contain the time the virus was detected; the type of scan—Real-time or Manual—that detected the virus, the source type of the virus, the name of the virus, the name of the file that contains the virus, the status of the first action, and if applicable the status of the second action.
Update	You try to download the latest components. Update log entries also contain what file(s) were downloaded and installed from Trend Micro and the status—Successful or Unsuccessful—of the download.
Personal Firewall	Your computer experiences an attack from the Internet. Personal Firewall log entries also contain the type of firewall defense, time of the attack, type of protocol used, source IP address, source port number, destination IP address, destination port number, the reason traffic was blocked, and the path and name of the application involved.
Anti-spam	Spam is identified and tagged. Anti-spam logs contain the time of the detection, the subject of the email message, and the sender.
URL Filter	A Web site is blocked or harmful Web content is encountered. URL filter log entries contain the time at which access to a restricted site was attempted, the filter setting in use, the URL that was blocked, and the filter category applicable to the URL .
Trojan Cleanup	A Trojan is detected by the Trend Micro Trojan Cleanup (DCS). DCS detects and cleans Trojan horse viruses. DCS log entries contain the time the Trojan was detected, the name of the Trojan, and the result of the cleaning action.

Private Data Protection	Your computer attempts to send your private data over the Internet. Private Data Protection log entries contain the time of the attempt to send private data, the type of data, and the Web site or the email address of where the data was being sent.
Spyware	Entries are created whenever spyware or other Internet threats are detected. Spyware log entries contain the time the threat was detected, the name of the spyware or other threat, and the result of the cleaning action.
Security Check	Entries are created whenever known Microsoft security vulnerabilities are detected. Security check log entries contain the time the vulnerability was detected, the name of the related Microsoft security bulletin, the risk rating, and the name of potential threats that are known to exploit this vulnerability.

To check your logs:

1. On the Main window, click **Summary > Event Logs**.
2. Click the type of log you want to view.
3. Click **View Logs**.
4. Select the date of the log you want to view.

Note: To sort the logs (ascending or descending) by column header (for example: Time), click the column title.

Introducing the Outbreak Warning System

Trend Micro PC-cillin Internet Security includes an innovative service to prevent the latest virus outbreaks or other malicious threats. By leveraging the research and knowledge of TrendLabs, PC-cillin Internet Security can proactively warn you of threats so you have time to update your software to prevent infection.

Enable the Outbreak Warning system to receive Outbreak Warnings.

To enable the Outbreak Warning System:

1. From the PC-cillin Internet Security main window, click **Updates and Registration > Outbreak Warning Settings**.
2. Select **Enable Outbreak Alert**.
3. To view the most recent Outbreak Warning, click **View Alert**.
4. Click **Apply**.

Outbreak Warnings are classified as Red and Yellow Alerts. Red Alerts correspond to the TrendLabs High-Risk ranking and Yellow Alerts to the Medium-Risk ranking.


Important: If you receive an Outbreak Warning, immediately update your virus pattern file and scan engine, and then run a scan on your entire computer.

Accessing Online Help

The Trend Micro PC-cillin Internet Security online help provides comprehensive coverage of all the functions and features of PC-cillin Internet Security. Use the online help to find the answers for your PC-cillin Internet Security questions.

To access online help:

- On the PC-cillin Internet Security Main window, click **Help > Contents and Index**. The online help appears.

When you are using the program you will also see context-sensitive help buttons . Click these buttons to view relevant help information based on the screen you are currently viewing.



Protecting Your Files and Data

This chapter contains information about basic tasks you can perform to protect your computer. It includes the following sections:

- Confirming Real-time Scan is Enabled on page 3-1
- Confirming Mail Scan is Enabled on page 3-2
- Scanning Your Entire Computer on page 3-3
- Scanning a Folder or File on page 3-3
- Running Scan Tasks on page 3-4
- Detecting Spyware and Additional Internet Threats on page 3-5
- Searching For and Cleaning Trojans on page 3-6
- Checking for Known Security Vulnerabilities on page 3-6
- Protecting Your Private Data on page 3-7
- Reducing Spam on page 3-9

Confirming Real-time Scan is Enabled

Real-time Scan provides constant protection against viruses by scanning files that are copied, downloaded, or moved to your computer. Real-time scanning takes place in the background and requires no user intervention, so you do not really have to do anything to "use" Real-time Scan—just be sure it is enabled.

To verify Real-time Scan is enabled, check the PC-cillin Internet Security icon in the Windows system tray.



Enabled (default) – red lightning bolt



Disabled – gray lightning bolt

To enable Real-time Scan:

- In the system tray, right-click the PC-cillin Internet Security icon, and then click **Real-time Scan**.

Confirming Mail Scan is Enabled

Email is the most common way for viruses and other malicious programs to spread, and opening an infected email message or attachments is the primary means of virus infection. Due to the popularity of email communication, virus writers create viruses that exploit the vulnerabilities of email client software.

Mail Scan is designed to check email messages and attachments as they are downloaded and sent from an Internet (POP3/SMTP) mail server. Supported email clients are:

- Microsoft Outlook 2000 and above
- Outlook Express 6.0 Service Pack 1 and above
- Eudora Pro 6.1 and above
- Netscape Mail 7.1 and above

Mail Scan can also scan mail attachments downloaded from a webmail account (email stored on a server and accessed by a Web browser). Supported webmail accounts are:

- MSN Hotmail
- Yahoo! Mail
- AOL Mail

Enable Mail Scan to begin scanning your email messages.

To confirm Mail Scan is enabled:

1. On the Main window, click **Email > Mail Scan**.
2. Click **Incoming Mail**. Ensure **Enable incoming mail scanning** is selected.
3. Click **Outgoing Mail**. Ensure **Enable outgoing mail scanning** is selected.
4. Click **Apply**.

Scanning Your Entire Computer

Scan all drives to check if your computer is infected. With one click, Trend Micro PC-cillin Internet Security provides a fast and easy way to scan all drives connected to your computer for infected files.

To scan your entire computer:

- On the Main window, click **Scan for Viruses**. The Scan Files dialog box appears and PC-cillin Internet Security begins scanning. To stop scanning, click **Stop**. A confirmation message box appears. Click **Yes** to confirm and then click **OK**.

Note: PC-cillin Internet Security scans the file types and executes the necessary scan actions according to the Manual Scan settings. To change these settings, refer to the online help under the book “Protecting Against Viruses and other Threats > Configuring Scan settings”.

Scanning a Folder or File

With Trend Micro PC-cillin Internet Security, you can scan the entire contents of a folder, including subfolders, or you can scan a single file. PC-cillin Internet Security scans the file types and executes the necessary virus actions according to the Manual Scan settings.

To scan a folder:

- Right-click the folder, and then click **Scan for Viruses**.

Tip: You can also drag the folder onto the PC-cillin Internet Security Main window.

To scan a single file:

- Right-click the file, and then click **Scan for Viruses**.

Tip: You can also right-click the file, select **Properties**, then click the **Virus Property** tab; or you can drag the file onto the PC-cillin Internet Security Main window.

Running Scan Tasks

Scan tasks let you schedule a variety of scans to automatically run at the specified time. In addition, at any time you can manually execute previously defined scan tasks.

PC-cillin Internet Security provides a number of pre-defined scan tasks. 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.

To run a scan task:

1. On the Main window, click **System > Manual Scan**.
2. Select the task you want to execute.
3. Click **Scan**. To stop scanning, click **Stop**. A confirmation dialog box appears. Click **Yes** to confirm and then click **OK**.

Note: To learn more about scan tasks, refer to the online help under the book “Protecting Against Viruses and Other Threats > Managing Scan Tasks”.

Detecting Spyware and Additional Internet Threats

Many Internet threats are not viruses or other inherently malicious code. Rather, they are applications that compromise your privacy, allow hackers to take control of your computer without your knowledge, or annoy you. They are frequently unknowingly downloaded along with desired applications. These threats include spyware, adware, dialers, joke programs, hack tools, remote access tools, password cracking applications, and other uncategorized software.

Trend Micro PC-cillin Internet Security detects these threats during Real-time Scan, and can also perform a Manual Scan specifically for spyware and additional Internet threats.

To enable Real-time scanning for spyware and additional Internet threats:

1. On the PC-cillin Internet Security main window, click **System > Scan Settings**.
2. Click the **Real-time Scan** tab.
3. Ensure **Enable Real-time Scan** is selected.
4. Click the **Spyware** tab.
5. Select **Enable for spyware and additional Internet threats**.
6. Select individual threats to scan for.
7. Click **Apply**.

To manually scan for spyware and additional Internet threats:

1. On the PC-cillin Internet Security main window, click **Scan for Spyware**.
2. The **Spyware Scan Results** screen appears, listing all threats found.
3. For details on a listed item, click **More Information...**
4. Select the items to remove
5. Click **Remove**.

Note: Not all applications identified are necessarily harmful to your computer. Before removing potential threats, verify they are not desired programs.

Searching For and Cleaning Trojans

Trend Micro PC-cillin Internet Security detects Trojan activity, recovers files modified by the Trojan, stops Trojan processes, and deletes files left behind.

Trojans, or Trojan horses, are small, seemingly harmless programs. To cause any damage, these programs must be installed onto your computer. Once a Trojan is installed, it has all the same privileges as the user of the computer and can exploit the computer 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.

PC-cillin Internet Security searches for Trojans during initial installation, and you can configure PC-cillin Internet Security to automatically search for Trojans during manual scans and every time Real-time Scan starts.

To automatically search for and delete Trojans during scans:

1. On the PC-cillin Internet Security main window, click **System > Scan Settings**.
2. Click **Manual Scan** or **Real-time Scan**, depending on which scan you also want to include searches for Trojans. Trend Micro recommends including searches for Trojans for both Manual and Real-time Scan.
3. Select **Search for and clean Trojans**.
4. Click **Apply**.

To manually search for and delete Trojans:

1. Locate the folder where you installed PC-cillin Internet Security (for example, the default location is `C:\Program Files\Trend Micro\Internet Security 2005`).
2. Double-click **Tsc.exe**.
3. A command console window displays the progress of the scan.

Checking for Known Security Vulnerabilities

Vulnerabilities or “security holes” make it easy for attackers, viruses, or other Internet threats to harm your computer. Microsoft has publicly identified these vulnerabilities as issues that exist in their software. Patching

security holes helps significantly reduce the chance your computer will be attacked or infected by viruses.

PC-cillin Internet Security checks your computer for vulnerabilities that Trend Micro has identified as presenting a significant risk. When security vulnerabilities are found, their risk level, potential threat, and the related bulletin are displayed.

Risk Level represents how great a threat this vulnerability represents. The levels, in order of decreasing danger, are:

- Critical
- Very High
- High
- Moderate
- Low

Potential Threat lists known viruses or other threats that exploit this vulnerability. For more information about a potential threat, consult the Trend Micro Virus Encyclopedia.

Related Bulletin gives the reference number of the Microsoft security bulletin that describes this vulnerability. To view the bulletin, go to the Microsoft Web site.

To check your computer for known Microsoft security vulnerabilities:

1. On the PC-cillin Internet Security main window, click **System > Security Check**.
2. Click **Check**.
3. The **Security Check results** area displays your results.

Protecting Your Private Data

Private Data Protection allows you to define certain types of information (for example, your name, address, or credit card number), which will then be blocked from being sent over the Web, or by email or instant messaging.

Note: Private Data Protection cannot guard your private data until you define the data items. See the online help under the book “Guarding Against Internet Attacks > Protecting private data” for more information.

To confirm Private Data Protection is enabled:

1. On the Main window, click **Network Control > Private Data Protection**.
2. Ensure that **Enable Private Data Protection** is selected.
3. Click **Apply**.

To add or edit a Private Data Protection item:

1. On the Main window, click **Network Control > Private Data Protection**.
2. Ensure that **Enable Private Data Protection** is selected.
3. Choose one of the following:
 - To add a new item, click **Add**.
 - To edit an existing item, select the existing item, and then click **Edit**.
4. Type a name and description for the item in the **Item name** and **Description** boxes.
5. Type your private data in the **Data** box. PC-cillin Internet Security will match the data exactly as you type it. Note that the information you enter is case-sensitive, so *trend*, *TREND*, and *tReNd* are all considered different.
6. Choose one or more of the following:
 - To protect this item from being sent over the Web, select **Check Web protocol**.
 - To protect this item from being sent via email, select **Check mail protocol**.
 - To protect this item from being sent via instant message, select **Check Instant Messenger protocol**.
7. Click **OK**.
8. Click **Apply**. The item is saved.

Reducing Spam

Spam email messages (also known as junk email) are an expensive and annoying problem on the Internet. The PC-cillin Internet Security Anti-spam engine identifies spam email messages and adds an identifier tag so they can be easily identified or filtered.

Enable Anti-spam to begin filtering your email messages.

To confirm Anti-spam is enabled:

1. On the PC-cillin Internet Security main window, click **Email > Anti-spam**.
2. Ensure **Enable Anti-spam** is selected.

You can configure PC-cillin Internet Security Anti-spam to operate on three different levels. On the highest level, the anti-spam rules are very strict. This leads to more spam being correctly identified, however legitimate email messages are more likely to be incorrectly tagged. The lowest level has much looser anti-spam rules. This leads to more spam getting through, but less chance of legitimate email messages being falsely tagged.

When an email message is identified as spam, the Subject line will be modified with "SPAM: " at the front. Set up a rule in your email client to filter these messages to a special "spam" folder, where you can periodically check for any legitimate email that was incorrectly tagged. (See your email client documentation for information on setting up rules.)

Anti-spam also has an Approved Senders list, and a Blocked Senders list. Any email messages originating from an email address on the Approved Senders list will never be tagged as spam. Messages from an address on the Blocked Senders list will always be tagged as spam.

To configure Anti-spam settings:

1. On the Main window, click **Email > Anti-spam**.
2. Select **Enable Anti-spam**.
3. Choose a setting from the **Anti-spam level** slider.
4. To add email addresses to your Approved Senders or Blocked Senders list, click **Edit Approved/Blocked Senders**
5. Follow the instructions on the screens that appear.

6. Click **OK** to return to the **Anti-spam** screen.
7. Click **Apply**.

Note: Email messages larger than the limit specified for the incoming (POP3) mail scan will not be filtered for spam.

Anti-Spam for Outlook™

Trend Micro Anti-Spam for Outlook is also included on the PC-cillin Internet Security CD. This personal anti-spam tool is installed as an add-in to Microsoft Outlook. Anti-Spam for Outlook provides spam filtering of email messages based on heuristic scanning, a spam signature database, and user-defined Approved and Blocked Senders lists.

Anti-Spam for Outlook offers the following features:

- A powerful and customizable anti-spam engine built into a personal Microsoft Outlook add-in
- Automatic quarantine of filtered messages for easy review and confirmation
- User-defined Approved and Blocked Senders list
- Spam and false positive reporting
- Filtering statistics for processed and quarantined email messages
- Support for manual and automatic updating of program components

To install Anti-Spam for Outlook:

1. Insert the Trend Micro PC-cillin Internet Security CD into your CD-ROM drive and do the following:
2. If the menu automatically appears, click **Install Anti-Spam for Outlook**, and then click **Next**.
3. If the installation program does not automatically start, from the Windows Taskbar click **Start > Run**. In the **Open** field, type `D:\Antispam\setup.exe` and click **OK** (where D:\ is the drive letter of your CD-ROM). Click **Next**.
4. Click **Yes** to accept and continue installing Anti-Spam for Outlook. The installation procedure will quit if you do not accept the terms.

Note: To prevent unnecessary duplication of resources, Trend Micro recommends disabling the Anti-spam feature of PC-cillin Internet Security when using Anti-Spam for Outlook.



Dealing with Viruses

With the number of viruses already “in-the-wild” and the number of viruses created and released, it is likely you will encounter a virus at some point. This chapter contains the following sections:

- Understanding Viruses on page 4-1
- What to Do When a Virus is Detected on page 4-2
- Actions On Uncleanable Files on page 4-2
- Cleaning Boot Viruses on page 4-3

Understanding Viruses

Simply put, a computer virus is a program that replicates. To do so, it attaches itself to other program files (for example, .exe, .com, .dll) and executes whenever the host program executes. Beyond simple replication, a virus usually 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 stored on your hard disk's partition table to scrambling the numbers in your spreadsheets to just taunting you with sounds, pictures, or obnoxious effects.

To learn more about any particular virus, or about viruses in general, you can access the Trend Micro online Virus Encyclopedia or visit the Web site at:

<http://www.trendmicro.com>.

What to Do When a Virus is Detected

First, do not panic. When Trend Micro PC-cillin Internet Security detects a virus either by Real-time, Manual, or Mail Scan, it notifies you of the virus and the scan action performed.

For Real-time and Mail Scan a message box is displayed describing the infected file and the scan action performed.

The scan actions for Real-time, Manual, or Mail Scan depend on the settings you have configured for each scan. However, the default action for all scans is Clean.

This simply means if a file becomes infected, PC-cillin Internet Security first attempts to clean the file. The default secondary action for Real-time and Manual Scan is Quarantine.

PC-cillin Internet Security may detect a malicious program which cannot be cleaned. Some malicious programs (such as Trojans and worms) do not infect files, so therefore cannot be cleaned. In addition, certain types of viruses overwrite existing data, making cleaning impossible. By default, PC-cillin Internet Security moves these “uncleanable” files to the Quarantine folder. (The default secondary action for Mail Scan is Delete.)

Actions On Uncleanable Files

Quarantined malicious programs cannot be cleaned, as they are programs. No virus is infecting a file; rather the entire program itself requires “cleaning.” Delete any quarantined malicious programs

For more information about how to handle files in the Quarantine Folder, view the interactive Quarantine Guide.

To view the Quarantine Guide:

1. On the Main window, click **System > Quarantine**.
2. Click **View Quarantine Guide** and follow the instructions.

You can learn the virus type by viewing the Virus logs. The following provides further information about how to identify different types of viruses and other threats based on their names.

Type of malicious program	Name prefix	Example
Trojan horses	TROJ_<name>	TROJ_QAZ.A
Worms	WORM_<name>	WORM_KLEZ
Script viruses	VBS_<name> JS_<name>	VBS_BRITNEYPIC.A
File infecting viruses	PE_<name>	PE_VETIKINS.A
Spyware	SPYW_<name>	SPYW_NARGON.A

Cleaning Boot Viruses

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

Trend Micro PC-cillin Internet Security automatically scans for boot sector viruses during a manual or scheduled scan. If a boot sector virus is found, Trend Micro PC-cillin Internet Security performs the action specified for the current scan.

Note: Boot viruses spread easily. If Trend Micro PC-cillin Internet Security detects 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.



Guarding Your Internet Connection

This chapter includes instructions on how to secure your Internet connection from malicious hackers. It also describes how you can prevent Web sites from being viewed using the URL Filter.

This chapter contains the following sections:

- Introducing the Personal Firewall on page 5-1
- Halting Internet Traffic on page 5-3
- Blocking Network Viruses on page 5-4
- Filtering Inappropriate Web Content on page 5-5

Introducing the Personal Firewall

The Trend Micro PC-cillin Internet Security 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 helps prevent malicious hackers from invading your computer and causing mischief.

The PC-cillin Internet Security firewall is a “stateful inspection” firewall, which means it tracks and monitors the state of each connection to make sure nothing strange is going on. For example, stateful inspection detects if something other than HTTP is running over port 80. A stateful inspection

firewall keeps track of each “session” and knows if the session is already active. The firewall uses this information plus a list of rules to determine if a packet (which is the basic unit of data transferred across a network) is blocked or forwarded.

Filtering decisions are based not only on defined rules, but also on context that has been established by prior packets that have already passed through the firewall.

The Personal Firewall includes the following features:

- Flexibility to create and apply different firewall profiles that provide an appropriate balance of security and access depending on the environment
- Allow, deny, or warn of traffic based on a specified port, protocol or target application
- When using the High security level, an outgoing access warning appears when an application tries to connect to the Internet, and the user is asked if the connection should be allowed.
- Intrusion Detection System prevents known firewall attacks (such as Too big fragment, Overlapping fragment attack, Tiny fragment attack)
- Prevents Trojan damage by closing particular ports that are known to be used in attacks
- Provides updateable firewall and IDS rules
- Ability to filter HTTP strings from server-to-server to prevent network viruses such as NIMDA and Code Red
- Automatic profile switching when the network environment changes

Enabling the 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 against hackers trying to damage files, steal personal information, or create mischief.

To confirm the Personal Firewall is enabled:

1. On the PC-cillin Internet Security Main window, click **Network Security > Personal Firewall**.
2. Ensure **Enable Personal Firewall** is selected.
3. Click **Apply**.

Understanding Personal Firewall profiles

Trend Micro PC-cillin Internet Security allows you to configure different Personal Firewall profiles for different situations. Depending on your computer and network settings, you may require certain ports or services enabled in some situations. By using Personal Firewall profiles, you can easily switch profiles between, for example, a home network and a wireless LAN, thereby keeping your security as tight as possible. The Personal Firewall comes configured with a variety of common network configurations. You can use one of these configurations without modification, or you can create and customize your own profile.

Note: See the online help under “Guarding Against Internet Attacks > Securing Internet connections with Personal Firewall > Managing Personal Firewall profiles” for more information.

Halting Internet Traffic

Complete control over your Internet traffic is vital for virus outbreaks or other intrusion attacks. The Emergency Lock immediately stops all incoming and outgoing Internet traffic and is particularly useful during times when someone is trying to remotely break into your computer or there is a virus outbreak.

To activate the Emergency Lock:

- On the Main window, click **Summary > Internet Security Status**, and then click **Halt Internet Traffic!**. All Internet traffic is now halted, so you will not be able to browse the Web or check your email messages until the Emergency Lock is deactivated.

To re-enable Internet Traffic:

- Click **Halt Internet Traffic** again.

Tip: In the system tray, right-click the PC-cillin Internet Security icon and click **Halt Internet Traffic** or when Real-time Scan detects a virus click **Halt Internet Traffic** on the message box that appears.

Blocking Network Viruses

Network viruses such as NIMDA spread rapidly through the Internet and local networks. Trend Micro PC-cillin Internet Security helps prevent your computer from being infected by network viruses, and prevents your computer from infecting other computers. PC-cillin Internet Security can do the following upon detection of a network virus:

- Halt all Internet traffic immediately
- Pop-up a Red Alert message

To view information about network viruses:

1. On the PC-cillin Internet Security Main window, click **Network Security > Network Virus Emergency Center**.
2. Click the link for more information about a particular network virus.

To change network virus settings:

1. On the PC-cillin Internet Security Main window, click **Network Security > Network Virus Emergency Center**.
2. Do one of the following:
 - To immediately halt Internet traffic when a network virus is detected, click **Halt all Internet traffic when network virus detected**.
 - To display an alert when a network virus is detected, select **Display Red Alert pop-up**.
3. Click **Apply**.

Filtering Inappropriate Web Content

For protection against offensive Web content, Trend Micro PC-cillin Internet Security offers the URL Filter. This feature lets you set whatever Web sites you want “off-limits” to other users of the computer.

The URL Filter can work in the following modes:

- Disable access to all Web sites by default. You then specify a list of sites you want access to. This list of URLs is known as the Approved URLs List.
- Enable access to all Web sites by default. You then specify a list of sites you do NOT want access to. This list of URLs is known as the Blocked URLs List.
- Enable access to all Web sites except those in specific content categories. These categories are predefined and determined by the Trend Micro Rating Server.

To filter unwanted Web content:

1. On the PC-cillin Internet Security Main window, click **Network Control > URL Filter**
2. Select **Enable URL filtering**.
3. Select the default filtering action.
4. Click **Apply**.

A message will be displayed when someone attempts to access a blocked Web site.

To add or edit an exception list URL:

1. On the PC-cillin Internet Security main window, click **Network Control > URL Filter**.
2. Ensure **Enable URL filtering** is selected.
3. Choose one of the following:
 - To add to or edit the Approved URLs List, click **Block access to....**
Your Approved URLs List is now operational.
 - To add to or edit the Blocked URLs List, click **Allow access to....**
Your Blocked URLs List is now operational.

4. Click **View Exceptions**.

5. Do one of the following:

To add Web site addresses:

a. Click **Add**.

b. On the **Add/Edit site** window, select **Add URL** and type the address, or to import URLs from your Internet Explorer cache, select **Import recently accessed URLs** and select the URL or URLs to add.

c. If desired, click **Include all sub-pages under these URLs**. This will add all sub-pages of the URL to the list. For example, if you added www.somewebpage.com, this would also allow or block access to www.somewebpage.com/pageone and www.somewebpage.com/pagetwo.

d. Click **OK** to return to the URL Filter Exceptions screen.

To edit Web site addresses:

a. Select the address you want to edit.

b. Click **Edit**.

c. On the **Add/Edit site** window, edit the address as required.

d. Click **OK** to return to the URL Filter Exceptions screen.

To delete Web site addresses:

a. Select the URL(s) you want to delete.

b. Click **Delete**. The URL(s) are removed from the list.

6. Click **OK** to return to the URL Filter screen. If you selected **Include all sub-pages...**, a small cross appears on the URL icon.

7. Click **Apply**.

Blocking predefined Web site categories

Trend Micro PC-cillin Internet Security can block Web sites based upon content categories you select. The categories available are:

Adult	Games
Sex	Web Communica- tions
Alcohol/Tobacco	Personal/Dating
Illegal Drugs	Chat/Instant Mes- saging
Gambling	Email
Crime	Newsgroups
Violence/Hate/Rac- ism	Shopping/Auctions
Hacking/Proxy Avoidance	Software Downloads
Cult/Occult	Streaming Media/MP3
Weapons/Military	Job Search



Getting Support

Trend Micro is committed to providing service and support that exceeds our users' expectations regardless of their location. This chapter contains information on how to get technical support. Register your product to be eligible for support.

The following topics are discussed in this section:

- Before Contacting Technical Support on page 6-1
- Visiting the Customer Care Center on page 6-2
- Visiting the Technical Support Web Site on page 6-2
- Contacting Technical Support on page 6-2
- TrendLabs™ on page 6-3
- Sending Your Infected Files to Trend Micro on page 6-3

Before Contacting Technical Support

Check your documentation: the manual and online help provide comprehensive information about Trend Micro PC-cillin Internet Security. Search both documents to see if they contain the solution to your problem.

Visit our Technical Support Web site: our Technical Support Web site contains the latest information about all Trend Micro products. Previous user inquiries that have been answered are posted on the support Web site.

Visiting the Customer Care Center

The Customer Care Center contains the latest news about Trend Micro PC-cillin Internet Security. As a registered user, you can access information that is not available outside this Web site.

To visit the Trend Micro Customer Care Center:

- On the Main window, click **Help > Customer Care Center**.

Visiting the Technical Support Web Site

Visit the Trend Micro Technical Support Web site to find answers to your inquiries. The Technical Support Web site contains the latest updated information about our products. New solutions are added daily. However, if you do not find the answer you seek, you can submit your question on-line, where the experts at TrendLabs will provide you with an answer or contact you for more information.

To visit the Technical Support Web site:

- On the Main window, click **Help > Technical Support Home Page**.

Contacting Technical Support

A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

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
- Trend Micro PC-cillin Internet Security program, scan engine, pattern file, version number
- Operating System name and version and Internet connection type
- Exact text of any error message given
- Steps to reproduce the problem

The best way to receive support is to send an email message to our highly trained Technical Support staff or visit our Web site.

Email: support@trendmicro.com

For other ways to contact Technical Support, check the "Support" section of our Web site at:

<http://www.trendmicro.com>

TrendLabs™

TrendLabs is a global network of antivirus research and product support centers that provide continuous coverage to Trend Micro customers around the world, 24 hours a day, seven days a week.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA, ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. For more information about TrendLabs, please visit:

<http://www.trendmicro.com/en/security/trendlabs/overview.htm>

Sending Your Infected Files to Trend Micro

You can send your viruses to Trend Micro via the Web. More specifically, if you have a file that you think is infected with a virus but our scan engine does not detect it or cannot clean it, submit the suspicious file to us at the following Web address:

<http://subwiz.trendmicro.com>

Please include in the message text a brief description of the symptoms you are experiencing. The Trend Micro team of virus engineers will “dissect” the file to identify and characterize any virus(es) it may contain and return the cleaned file to you—usually within 48 hours.



Appendix

This appendix contains information that may not be applicable for all users. It includes the following sections:

- Working With Rescue Disks on page A-1
- Enabling and Configuring Proxy Settings on page A-3

Working With Rescue Disks

Certain types of boot viruses can prevent your computer from booting normally. To clean these viruses, start your computer from a clean disk, not the infected hard drive. A “rescue disk” is a bootable floppy disk that Trend Micro PC-cillin Internet Security can create if you are running Microsoft Windows 98 or Windows Me.

The PC-cillin Internet Security rescue disks require a “pure DOS” environment to operate correctly, however Windows 2000 and XP no longer support a pure DOS environment.

For Windows 2000 and XP, Trend Micro recommends you create an Emergency Repair Disk. Refer to the Microsoft Windows documentation for instructions.

You need multiple disks to create the complete set of rescue disks.

Note: Write protect rescue disks after they are created. A disk is write protected when you can see through both squares in the upper corners.

- Emergency Boot Disk (Disk 1): 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.
- PCSCAN Files Disk (Disk 2): Contains the scan engine. Use with the Pattern File disks to detect and clean viruses located in the boot sector of your computer.
- Pattern File Disks (Disks 3 and others): Contains pattern files to detect the latest viruses. Use with the PCSCAN Files disk to detect and clean viruses located in the boot sector of your computer.

Note: Do not restart your computer using rescue disks that were created for an earlier version of Trend Micro PC-cillin Internet Security—this can result in data loss.

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

Even if you already have a set of rescue disks from a previous version of Trend Micro software, create a new set after installing PC-cillin Internet Security. Likewise, if you created your rescue disks under Windows 98 and have upgraded to Windows Me, 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 rescue disks:

1. Obtain some disks and insert one into the floppy drive of your computer.
2. From the Windows Taskbar, click **Start > Programs > Trend Micro PC-cillin > Create the Rescue Disks**. The Create Emergency Rescue Disks window appears.
3. Click **Complete Rescue Disk set**, and then **Click Next**.
4. Make sure the Target drive is correct and click **Next**. The Format dialog box appears.
5. Choose your format type (Trend Micro recommends Full) and click **Start**. The disk starts formatting.

6. When the formatting is finished, click **Close**. The Format dialog box closes and PC-cillin Internet Security starts copying the files to the disk.
7. As each floppy is finished, remove it and immediately label it. Slide up the plastic button in the upper left hand corner of the back of the disk to write protect it. The disk is write-protected when you can see through both squares in the upper corners. Creating the rescue disks takes about 10 minutes.
8. Repeat the procedure for each disk, starting from the formatting step.
9. Click **Finish**.

Note: 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.

Enabling and Configuring Proxy Settings

A proxy server is used to provide security and increase efficient use of network bandwidth. Most home users do not use a proxy server, but many offices and schools do. If you are having trouble connecting to the Internet to register, or download 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 you use a proxy server on your network, type 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, type the appropriate logon credentials.

To enable and configure proxy settings for downloading updates:

1. On the Main window, click **Updates and Registration > Update Settings**.
2. Under **Proxy information**, select **Use a proxy server...**

3. Click **Proxy Settings**, and then do the following:
 - In **Proxy address**, type the IP address of the proxy server or domain name (for example, proxy.yourcompany.com).
 - In **Port**, type the port number of the proxy server (for example, 80).
 - In **User name** and **Password**, type your proxy server logon credentials, if required.
4. Click **OK**.
5. Click **Apply**.

Note: The procedure for configuring a proxy server for use with the Personal Firewall is similar. For detailed instructions, refer to the online help under the book "Guarding Against Internet Attacks > Managing Personal Firewall Profiles > Configuring a proxy server."

Index

A

Activation 1-9
Anti-spam 3-9
Anti-Spam for Outlook 3-10

B

Blocking Web sites 5-5
Boot viruses 4-3, A-1

C

Checking 3-6

E

Event logs 2-9

F

Filtering Web content 5-5
Firewall 5-1, 5-3
Firewall profiles 5-3

G

Getting started 1-7

I

Icons 2-6–2-7
Installing 1-8

L

Logs 2-9

M

Mail clients supported 3-2
Mail scan 3-2
Main window 2-4
Maintenance Agreement
 expiration 1-1
 renewal 1-1
Minimum system requirements 1-6

N

Network viruses 2-11, 5-4

O

Online help 2-12
Operating systems 1-6

Outbreak Warning System 2-11

P

Personal firewall 5-1
Private data protection 3-7
Product information 2-7
Protection 2-2
Proxy settings A-3

R

Real-time scan 3-1
Registration 1-9
Requirements 1-6
Rescue disks A-1

S

Safe computing practices 1-12
Scan tasks 3-4
Scanning a file 3-3
Scanning a folder 3-3
Scanning your computer 3-3
Spam 3-9
Spyware 3-5
Status, antivirus 2-9
Status, Internet security 2-8
System information 2-7
System requirements 1-6

T

Technical support 6-1–6-2
TrendLabs 6-3
Trial version 1-11
Trojans 3-6

U

Uncleanable files 4-2
Updating 1-10
URL Filter 5-5
Using 2-6

V

Vulnerabilities 3-6

W

What's new 1-4
Whitelist 3-9