

Laplink PCdefense™ Quick Start Guide

011106

laplink
connect your world®

Contact Laplink Software



For technical support issues or questions, please visit: www.laplink.com/support.

Email: CustomerService@laplink.com

Tel (USA): +1 (425) 952-6000

Fax (USA): +1 (425) 952-6002

Tel (UK): +44 (0) 870 2410 983

Fax (UK): +44 (0) 870 2410 984

Laplink Software, Inc.

14335 NE 24th Street
Bellevue, WA 98007
USA

Copyright/Trademark Notice

© Copyright 2006 Laplink Software, Inc. All rights reserved. Laplink, the Laplink logo, and PCdefense are registered trademarks or trademarks of Laplink Software, Inc. in the United States and/or other countries. Other brands and products are trademarks of their respective holder(s).

Thank you for using the best defense your computer can have, PCdefense. Below are instructions for installing the software, and step-by-step suggestions for using PCdefense for the first time.

Installation and Setup

Before installing, make sure to close all programs running on the computer.

Follow the instructions below that are appropriate for the way you will install PCdefense.

Installing from CD: Insert the PCdefense CD in a CD-ROM/DVD drive. On the PCdefense Welcome screen, click **Install PCdefense**. If the Welcome screen does not appear, open Windows Explorer and double-click PCdefense_en.exe on the PCdefense CD-ROM.

Installing from downloaded file: If you downloaded PCdefense, double-click on the downloaded file called PCdefense_en.exe.



Welcome Screen: Click Next to proceed with the installation of PCdefense. On any screen, click Cancel to exit the installation.

License Agreement: Click Yes to accept the PCdefense License Agreement, or No to exit the software installation.

Customer Information: Type your name, company name, and serial number. Click Next.

If you installed from CD: Your serial number is located on the PCdefense CD sleeve.

If you purchased PCdefense online: When you purchased, you were sent a confirmation email. Your serial number and a link to the My Downloads section of My Support are located in that email. At the My Downloads section, you can get a copy of your PCdefense software, obtain your serial number, and more.

To access your My Support account, go to: <http://www.laplink.com/mysupport/> and enter your user name and password.

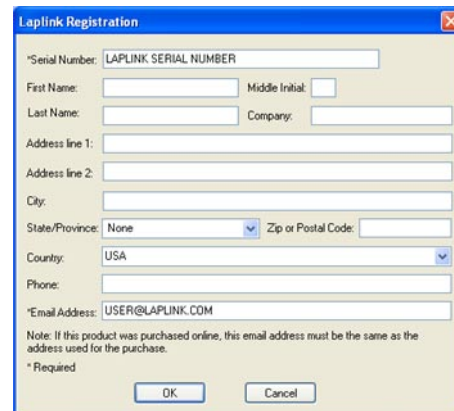
Choose Destination Location: Choose the drive and directory into which you would like to install PCdefense, or accept the default. Click Next when ready.

Start Copying Files: PCdefense has all the information it needs to install. Review your current settings, and click Back to make changes, or Next to continue.

Setup will install PCdefense on your PC. Click **Finish** when installation is complete.

Getting Started- Registration

When you first open PCdefense, a pop-up screen lets you know that you have 30 days to register PCdefense. Click Yes to register now, and No to register later.



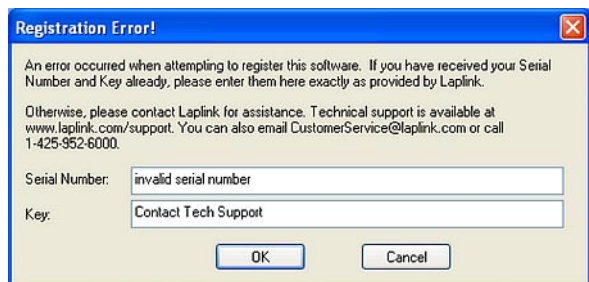
The screen above will appear. Note that the serial number is automatically written to the proper field. Please fill out the information as listed, and make sure to provide a valid email address. Once you register PCdefense, this screen will not appear.

You can choose to cancel at this screen. This screen will appear at startup until you register PCdefense. **You must register PCdefense within 30 days of installation to continue to use the software.**

Note: You must register PCdefense prior to creating Disaster Recovery images.

If registration fails...

If registration fails for any reason (invalid serial number, serial number entered improperly, Internet connection failure, etc) the screen below will appear.



At this screen, it is necessary to contact Laplink Technical Support via email or by phone.

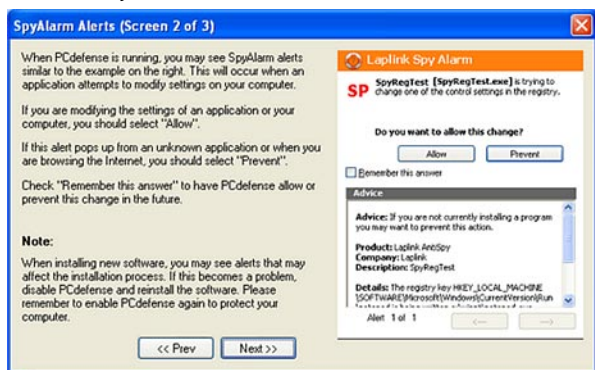
- Email- CustomerService@laplink.com
- Telephone- + 1 (425) 952-6000

Laplink customer service will validate your purchase, and provide you your serial number and key to allow you to successfully register PCdefense.

Getting Started Tutorial

After the registration screen, you will see three pop-up tutorial pages. These pages are essential to understanding how PCdefense works, and what to expect when first using PCdefense.

The first page welcomes you to using PCdefense, and mentions many of its important features. Click **Next** when ready.



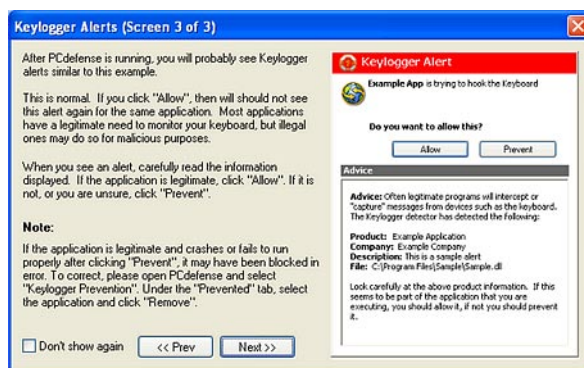
The next screen, shown above, explains SpyAlarm Monitoring. SpyAlarm Alerts occur when an application attempts to modify certain settings on your PC. If you are in the process of manually changing settings on your PC, and you get SpyAlarm Alerts, these alerts are probably perfectly normal, and you can check the **Allow**

button. If you are browsing the Internet and get an Alert when not making program modifications, click the **Prevent** button.

Check the **Remember this answer** checkbox to have PCdefense remember your choice and handle this program the same way every time.

Click **Next** when ready.

The next screen offers you tips on interpreting Keylogger Alerts.



Keylogger alerts will pop up when programs attempt to hook the keyboard. This is normal behavior when opening and installing programs, and you can usually click Allow.

If you get Keylogger Alerts when browsing the Internet, or at times other than when you are installing or opening programs, click Prevent.

For detailed information regarding SpyAlarm Monitoring, Keylogger Prevention and all the powerful features available in PCdefense, see the PCdefense User Guide.

Running PCdefense for the First Time

Unless you are installing PCdefense on a brand new, just out-of-the-box PC, it is a good idea to immediately perform scans to clean your computer and adjust settings to prevent new infections.

PCdefense is set up to allow you to simply accept the defaults on each screen to successfully clean and safeguard your PC. For detailed instruction on how to define scans and manage Disaster Recovery image creation, see the PCdefense User Guide.

To use PCdefense to clean your PC, follow the steps listed in this Quickstart Guide, accepting all defaults.

Step One: Run Spyware Scan

While there are many different definitions, spyware is generally defined as any software that employs a user's Internet connection without their knowledge or explicit permission. Spyware Scan allows you to scan your PC for spyware currently installed on your system. It also allows you to decide what to do with anything it finds.

To run Spyware Scan:

In PCdefense, click on Spyware Scan under the Defend options.

- 1 Click the Run Spyware Scan button.
- 2 When the Spyware Scan page launches, click the Start button to begin scanning your PC.
- 3 When the scan is completed, you will see a list of files detected as spyware, and the risk to your PC. All files will be selected by default. Look through the list of files and deselect any that you don't want PCdefense to take action on. When ready, click Remove to delete all marked files.

The detected spyware will be quarantined on your PC. If you want, you can choose to permanently delete it later.

Note: Depending on the scan options you choose and the size and speed of your PC, spyware scans can take anywhere from a few minutes to an hour or more.

Step Two: Run Virus Scan

The ability to browse the Internet to obtain information, software tools, credit card and banking information has made the PC an invaluable information, entertainment and communication resource. However, these activities can result in malware and viruses being installed on your PC without your knowledge. Laplink Online Virus Scan is a fully-functional antivirus product, featuring all required elements for antivirus scanning and cleaning: it scans system's memory, all files, folders and drives' boot sector, providing the user with the option to automatically clean the infected files.

Note: You can also choose to further define your Virus Scan options and settings. Select the **click here** links on the scan page to see your options. You can learn more about your scanning options in the PCdefense User Guide.

To run Virus Scan:

In PCdefense, click on Virus Scan under the Defend options.

- 1 Click the **Run Virus Scan** button.
- 2 When the Virus Scan page launches, click the **Click Here to Scan** button to begin scanning your PC.

Virus Scan will detect and immediately act upon viruses on your PC, deleting and disinfecting any viruses found.

Note: You will need to install an Active X control to use Virus Scan.

Note: Depending on the scan options you choose and the size and speed of your PC, virus scans can take anywhere from a few minutes to an hour or more.

Step Three: Rootkit Scan

Rootkits are the newest and most serious threats to PCs. Rootkits might perform the same types of functions as a keylogger, a virus, or any malware or spyware, and still go undetected by spyware or virus checkers, because they mask themselves on the PC.

What is a rootkit?

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a hacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that monitor traffic and keystrokes. Rootkits sometimes create a "backdoor" into the system for the hacker's use, alter log files, attack other machines on the network, and alter existing system tools to escape detection. Rootkits have become more common and their sources more surprising. Experts worry that the practice may be more widespread than the public suspects.

Rootkits are hidden from conventional detection; they can't be detected by looking in file listings or in the registry. Standard antivirus and antispayware softwares usually can't detect much less remove rootkits.

Using PCdefense Rootkit Scan

If a rootkit is detected on a system, we strongly recommend removing it, as rootkits have the capability to act as spyware or keyloggers, and can capture and send your personal data to the source.

For information regarding removing rootkits from your PC, see the PCdefense User Guide

Run Rootkit Scan

In PCdefense, click on Rootkit Scan under the Defend options.

- 1 Click the **Run Rootkit Scan** button on your PC to detect any existing rootkits.



If an anomaly, which is possibly a rootkit, is detected on your PC, you will see the screen above. Click on the link on this screen to go to the **Laplink Security Center**, where you will find information about common anomalies, and advice on what your next steps should be.

The Laplink PCdefense Rootkit Scan detects rootkits using a variety of methods. These proprietary methods include:

- Hidden Process Detection
- Hidden Inline Module Hooking
- Hidden Kernel Driver Detection
- Hidden Kernel Driver Hooking

Step Four: Create a Disaster Recovery image

PCdefense Disaster Recovery (DR) allows you to create a safe backup image of your PC, assists you in writing the backup to other drives or media, and allows you to restore your backup copy to your system.

Prepare for Disasters

Maybe using tools like PCdefense will keep your PC safe, and you won't have problems. But what if something just breaks, or is stolen? What if your computer just dies? Do you have a complete backup, not just of a few files but of everything, all the programs you use, all of your email, all of your files and settings?

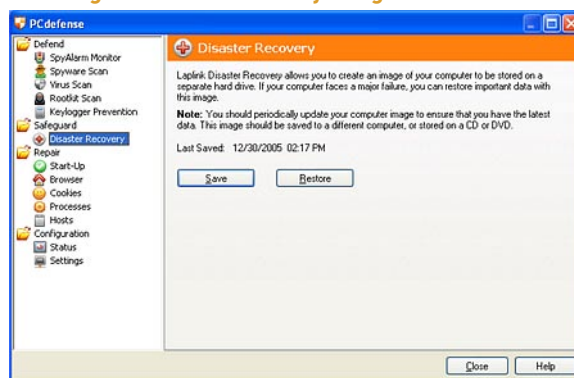
Regardless of how it happens- through a virus, a hacker, or whether you spill coffee on your PC, computers can get damaged, and valuable data can be lost.

PCdefense includes Disaster Recovery, which allows you to create a complete backup image of your system. This way, no matter what happens to your PC, you have a safe

backup of your data.

Disaster Recovery (DR) is a tool to be used to safeguard against system crashes, lost laptops and other data disasters, not a daily backup tool. PCdefense creates an image of everything on your PC to restore when disasters occur. The more frequently you update your image, the less chance you will lose data.

Creating a Disaster Recovery Image



Note: You must have Administrator privileges on your PC to use Disaster Recovery.

- 1 **Define your DR Image**

In PCdefense, under the Safeguard option, click Disaster Recovery. Click **Save** to start.

Disaster Recovery restores every file and registry setting that does not already exist when you restore. It does not overwrite anything. Hardware settings and temporary folders are not restored, which means that, even if you need to restore to a new PC, it will work. These are the most common settings and options a person would want to include in an image.

On the main page of the Create Image Wizard you can choose to accept the defaults by clicking the **Next** button.

IMPORTANT! Save Image to another location!

If your PC has a catastrophic failure, you may permanently lose all data stored on these drives. This would include any Disaster Recovery images saved on you local drives. It is strongly suggested that you save images to a network drive, CD or another PC. Make absolutely certain to have at least a copy of your Disaster Recovery images stored in a safe location off your PC.

- 2 **Build Image Components**

At the next screen, click **Next** to begin building the components necessary to create your Disaster Recovery image.

Map Users

The first component is Map Users. The screen allows you to include or exclude users on your PC.

To accept All Users (system default), and continue with Disaster Recovery image creation, click **Done**.

To Include or Exclude a User: From your DR image, highlight the user, and click the Exclude or Include button. Regular users are displayed by default.

Map Drives

Disaster Recovery allows you to choose which drives to include or exclude in your Disaster Recovery image.

If you want to Include or Exclude one of the drives listed, click on the drive to highlight it, and click the Include or Exclude button.

When you have selected the drives you want to include in your Disaster Recovery image, click **Done**.

Next, a progress screen will show your image snapshot being created.

3 Name Your DR Image

The next screen requires you to name your DR image.

Your Disaster Recovery image is a backup of files and data on your entire system, and the files can be quite large. **We strongly recommend that users:**

Write your DR image to a network drive or external device (Disaster Recovery allows you to write to CD/DVD), so that in the event of a system crash, your backup will be in a safe location.

When you have chosen a drive that is in a safe location and has sufficient drive space, click Next.

4 Data Storage Options

PCdefense and Disaster Recovery allows you to break the backup into pieces. This is primarily used when you are writing to CD. By default, it breaks the image into 600 megabyte pieces, as that is how much data the standard writable CD will hold.

Choose the file size that best serves your Disaster Recovery image needs, and click Next.

5 Create the Disaster Recovery Image

PCdefense now has all the information it needs to create your DR image. Click Next to begin creating your image.

The Disaster Recovery image creation process can take minutes to hours, depending on how much data is being generated and other factors.

Congratulations! Your Disaster Recovery image is now being created. When it is complete, **make sure you have**

a copy of the image stored to another location.

Step Five: Make sure SpyAlarm Monitoring and Keylogger Prevention are Enabled

Both **SpyAlarm Monitoring** and **Keylogger Prevention** are enabled by default, but it is important to understand these features.

SpyAlarm Monitoring prevents applications from installing on your system without your knowledge and permission. Some spyware installs behind the scenes, without user knowledge. SpyAlarm Monitor provides a pop-up message when an application attempts to write to sensitive areas of Windows. Through these alerts, you can control whether an application is allowed to perform the modification.

Keylogger Prevention stops keyloggers on your PC from collecting data. A keylogger is a computer program or a hardware device designed to record keystrokes. It can either be a hardware device (installed on a keyboard) or software that causes keystrokes to be recorded. The Keylogger Prevention feature blocks keyloggers from being able to see the keys you are typing.

Note: When a keylogger is detected by PCdefense, and you choose Prevent on the pop-up alert, you must restart your PC to permanently disable and prevent this keylogger on your PC.

To access **SpyAlarm Monitoring** control, under the Configuration folder, choose the Settings option. Toggle this option by clicking the Enable SpyAlarm Monitoring button.

To access **Keylogger Prevention** control, under the **Defend** tab on the PCdefense options, click on Keylogger Prevention. Toggle this option by clicking the On/Off button.

Congratulations! Your PC is now cleaned of viruses and spyware, and defenses are set to help prevent them in the future. A clean Disaster Recovery image has been created and saved to a different location.

Other PCdefense Features

Start-up Programs

The programs listed on this PCdefense screen have been added to the Startup group by you or a program installation. These programs run after Windows is displayed. Although disabling programs is usually safe, make sure you understand what your program does

before disabling it, as disabling programs can cause system instability. If you have questions, check with your software vendor.

Current User vs. Machine

- Programs can be placed in different start-up groups.
- Programs under the Machine tabs are set to start up whenever the machine starts up, regardless of who is logged on to the PC.
- Programs under the Current User tabs start up when the current user is logged onto the PC.

Programs can be set to start up in both groups.

Note: Make sure you understand what your Startup program does before disabling it, as disabling resources can cause problems on your PC.

Browser

When you purchase your computer, your browser comes with certain defaults. Certain types of spyware and malware can change these settings, redirecting you to their search engine, asking you if you want to install their software, or make their site your home page. PCdefense Browser repair allows you to revert your browser settings back to the system defaults at the click of a button.

All defaults settings are listed on the Browser Restore screen in PCDefense. If a default setting has been changed for any reason, including manual changes by any user, the setting will appear in Blue under the Current column.

Cookies

Cookies are files placed on your PC by accessing websites so that the site can remember something about you at a later time. Typically, cookies are not malicious, but some sites may use cookies without informing you. This can be dangerous to your data or your system. PCdefense allows you to delete cookies from your system quickly and easily.

Cookie Options

Remove- Select a cookie, then click Remove to delete the cookie from your PC.

Remove All- Removes all cookies from your PC.

View- View the contents of the cookie in a text file.

Details- Shows the details regarding the cookie selected, including: Source URL, the name of the cookie

stored locally, information regarding dates, when the cookie was last accessed, and the expiration date of the cookie.

Properties- (under Details)- Brings up the Windows Properties dialog, allowing you to change attributes, rename the file, and all other features available in the Windows properties dialog screen.

Processes

Although many processes running on your PC are normal and safe, spyware and malware can also run as processes on your PC. You can use the PCdefense Processes tab to shut down any processes on your system.

Terminate- Terminating a process will immediately stop this process on your PC. This can cause undesired results, including loss of data and system instability. The process will not be given a chance to change its state or data before it is terminated.

Properties- Brings up the Windows Properties dialog, allowing you to change attributes, rename the file, and all other features available in the Windows properties dialog screen.

The properties dialog also shows information about the process, such as the software maker, version, security and other information. The information in the properties screen can help you determine if the selected process is one you trust, or one you suspect is spyware or malware.

Details- Clicking the Details button displays the DLL (dynamic link library) files connected to the selected application. This can help you identify malware running on your system.

Sometimes, spyware or viruses attach themselves to a commonly used application, such as Internet Explorer, in the form of a DLL. The Details screen allows you to view all DLLs connected to a particular application. If you see DLLs that you don't recognize or you suspect are not connected to an application you trust, you can search the Internet for information about that file, and disable or delete the process or file if necessary.

Hosts

The Hosts file is like an address book. When you type a web address, such as www.laplink.com, into your browser address bar, the Hosts file is consulted to see if you have the IP address for that site. If you do, then your computer will connect and the site will open. Some spyware/malware will modify your HOSTS table to

redirect a website to a different address, redirecting you to a spyware/malware site without your knowledge.

Settings

The Settings screen in PCdefense provides information regarding the log files created during the use of the software. These log files list when scans were last performed, when software alerts occurred and what action was taken, and other valuable pieces of information. The Settings screen also allows the user to turn some features on or off.

PCdefense Settings

The green checks on the Settings screen indicate when features are enabled.

Log File- Contains a list of all alerts generated in PCdefense.

Alert History- The Alert History file contains full report of all alerts, including time, action and registry key.

Alerts Saved- The Alerts saved file tracks all alerts that have been selected to be “remembered”.