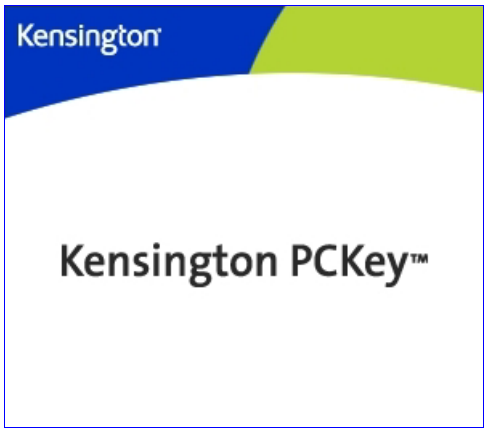



Kensington®

# PCKey™ User Guide

**For Windows XP**

**Version 2.0**

**NOTE**: This guide contains important information and procedures to help safeguard your data during and after installation.

# Kensington PCKey™

Document Version 2.0.0.1.33 – 12/02/03

Copyright © 2002-2003 Authenex, Inc. All rights reserved.

# Contents

# 1. Your User Guide

This user guide provides instructions for installing, using, and uninstalling your Kensington PCKey. It is divided into the following sections:

- **About Kensington PCKey**

  A description of the Kensington PCKey USB device and software features, and how to use your Kensington PCKey.

- **Prepare Your Computer for Installation**

  A “best practices” checklist to guide you in preparing your computer for a trouble-free installation.

- **Install Kensington PCKey**

  Procedures to install Kensington PCKey on your computer. Installation includes the following:

  - Install Kensington PCKey software
  - Install Kensington PCKey USB device drivers
  - Program your password in the Kensington PCKey
  - Encrypt your hard drive
  - Register your Kensington PCKey and Password

- **Using Kensington PCKey Tools**

  Kensington PCKey provides several easy-to-use tools that give you versatile control over using your PCKey. Most importantly, the PCKey and Password Recovery Process provides the **only** “backup” solution for you if you lose your PCKey or password.

- **Uninstall Kensington PCKey**

  Procedures to uninstall the Kensington PCKey, including decryption of your hard drive and restoration of your files.

- **FAQs**

  Frequently Asked Questions and technical support information.

# 2. About Kensington PCKey

Kensington PCKey protects a PC or notebook using *two-factor authentication* and 128-Bit AES Encryption. The combination of these technologies makes PCKey one of the strongest computer security tools you can own. Unless of course, you own Fort Knox.

- **What is Two-Factor Authentication?**

  Two-factor authentication is security technology that allows access to a computer only when you insert your Kensington PCKey in the USB port, and you use your password. This is similar to the two-tier security required when you use your ATM bank card along with your PIN. Neither your ATM card or your PIN will work without the other. Two-factor authentication is considered very safe because it requires two specific identifiers – something you have (your PCKey), and something you know (your password).

- **What is 128-Bit AES Encryption?**

  Encryption is the method of translating normal data on your computer's hard drive into an unbreakable code that is impossible for anyone else to use. When the content of your hard drive is encrypted, it is virtually impossible for anyone to decrypt the content – except if they have both your PCKey and password.

  Kensington PCKey uses 128-Bit AES encryption because it is one of the strongest encryption technologies available. The encryption "cipher" code used by Kensington PCKey would take hundreds of thousands of years to break – even if a hacker used today's most powerful computers.

- **What does my Kensington PCKey do?**

  The Kensington PCKey contains a chip that allows PCKey software to encrypt and decrypt the content of your hard drive instantly and invisibly while you use your computer. After you encrypt the content of your hard drive using PCKey, you must insert your PCKey in your computer to "unlock" it. Your data cannot be decrypted without your PCKey, and your PCKey will not work without your password. The password you select is programmed into your PCKey, and nothing and no one can get it out.

  When you shut down your computer, the information on your hard drive is completely secure. Even if your computer is stolen or your hard drive is installed in another computer, all information on it remains encrypted.

- **How do I use Kensington PCKey?**

  You use your Kensington PCKey and password every time you start your computer and log in, and every time your computer re-starts after sleep or hibernation mode.

  To log in, simply insert your Kensington PCKey before or after you turn on your computer. When the PCKey login screen appears, enter your password and log in.

After you log in, encryption and decryption is automatic and transparent. PCKey software decrypts the data you need, when you need it. (Data on the drive remains encrypted; it is decrypted only when transferred to temporary memory.) Your computer will work exactly as before, except of course, you will be locked out of your computer if you lose either your PCKey or password. (Note: Registration with Kensington for the *PCKey and Password Recovery Process* is your only recovery option!)

Even if you accidentally leave your PCKey in your computer, your hard drive is inaccessible without your password.

- **Can the Kensington PCKey key be compromised?**

  No. The Kensington PCKey will be destroyed if someone attempts to open it. However, the PCKey stands up to virtually any punishment, working after being immersed in water or put through the washing machine.

- **What type of USB adapter do I need? Can I use a PS/2 adapter?**

  Kensington PCKey will work with any A-type USB 1.1 or USB 2.0 port, USB hub, or USB extension cable connected directly to your computer. You cannot use the PCKey with a USB-to-PS/2 conversion adapter.

- **Is PCKey easy to install? What do I need to do?**

  Kensington PCKey is easy to install. The *Installation Wizard* fully automates the installation process. Before you click "*setup,*" please read *Prepare Your Computer for Installation*, and Kensington PCKey *FAQs***.**

- **Does PCKey encrypt all drives on my computer? What about network, external, or removable hard drives?**

  Please read the *FAQs* section for an explanation.

- **What is "Registration" and why should I register my Kensington PCKey and Password?**

   *Registration is the only safeguard you have to access your computer if you lose either your Kensington PCKey or password*. If you do not register and you lose your Kensington PCKey or password, you will lose all data on your hard drive.

  When you register, your Kensington PCKey serial number and your password are stored securely by Kensington. If you have registered and you lose your Kensington PCKey or password, the online *PCKey and Password Recovery Process* enables you to access your computer.

  If you lose your Kensington PCKey or password, and you have not registered first, we are sorry. There is nothing we can do to decrypt your hard drive. It is impossible.

# 3. Prepare Your Computer for Installation

The installation procedure for both the Kensington PCKey USB device driver and Kensington PCKey application software is automatic. An *InstallShield Wizard* guides you through the process, prompts you with messages and instructions, and provides status information.

 **Do not insert your Kensington PCKey in the USB port until you are instructed.**

**Time Needed**

Depending on the speed of your computer and size of your hard drive, the Kensington PCKey program installation and encryption of your hard drive(s) requires approximately 15-30 minutes. Allow yourself an additional 45 minutes to read this guide and to follow preparation procedures.

## 3.1. Installation Preparation Requirements and Recommendations

**Important!** Follow these "required," "recommended," and "optional" steps to help ensure a trouble-free installation.

- ❑ **Read *System Requirements*** (Section 3.2) to be sure your computer meets the minimum requirements, including free hard drive space.
- ❑ **Read *Installation Requirements*** (Section 3.3) and ***FAQs*** (Section 7.) Additional installation requirements or considerations are explained.
- ❑ **Back up your data** for installation safety, and for data recovery if you lose an unregistered PCKey or password (recommended.)
- ❑ **Run Check Disk, and Defrag**. See Windows documentation (recommended.)
- ❑ **Uncompress and decrypt** all data on your hard drive, see Section 3.5 (required.)
- ❑ **Restore items in the Recycle Bin**. Kensington PCKey installation deletes all content in the Recycle Bin. Restore any files that you want to keep, before installation (optional.)
- ❑ **Remove or disconnect ALL drives or storage media that should not be encrypted – including:** Internal IDE drives; ZIP, Jaz, Iomega, Syquest or other removable drive cartridges; External drives connected by USB, Firewire, PCMCIA, or parallel port; and USB or other "Flash" memory drives and storage media. You can reinstall or re-attach drives after installation/encryption (required.)
- ❑ **Record the hard drive configuration.** Uninstallation requires the original drive configuration. See Section 6 for more information (required.)
- ❑ **Create a Restore Point.** See Windows documentation (recommended.)

- ❑ **Disconnect any wired or wireless network connections** to help ensure that there will be no disk reads or writes during encryption. You do not need to uninstall networking software (recommended.)
- ❑ **Restart your computer** after completing the preliminary steps above, and just before you begin the installation (required.)
- ❑ **Close as many applications as you can** after you restart your computer. Many applications start automatically. The System Tray (on the lower right of the Task Bar) often shows applications that are loaded at startup. Close or disable utility applications such as firewalls and virus checkers. It is not necessary to close standard Windows utilities such as the clock or task scheduler (recommended.)

## 3.2. System Requirements

- Processor: Pentium-compatible CPU
- RAM: 64MB minimum, 128MB recommended
- One available USB port – either USB version 1.1 or 2.0
- Windows XP - Home Edition or Professional (English version only)


Windows 2000 is supported. See the *PCKey User Guide* for Windows 2000. PCKey is not supported on Windows 98, or Windows ME.

## 3.3. Installation Requirements

- Kensington PCKey must be installed on the local system. Network or remote administrative installation is not supported.
- Kensington PCKey must be installed by a user that has full *local* "administrative" privileges in the operating system. (Any user with an existing user account can use Kensington PCKey after installation.)
- A minimum of 200 MB free hard drive space per partition (each drive letter) is required. Kensington PCKey installation checks free space: if any drive has less than 200 MB free space, installation will not occur.
- Kensington PCKey is not supported on a multi-operating system computer (a computer that has multiple boot partitions or a partition manager that is actively managing the boot of the system.)
- Kensington PCKey will not encrypt any file that is bigger than the free space on the drive the file is on. For example, if a media clip is 450 MB and there is only 300 MB free space on your drive, the media file will not be encrypted.

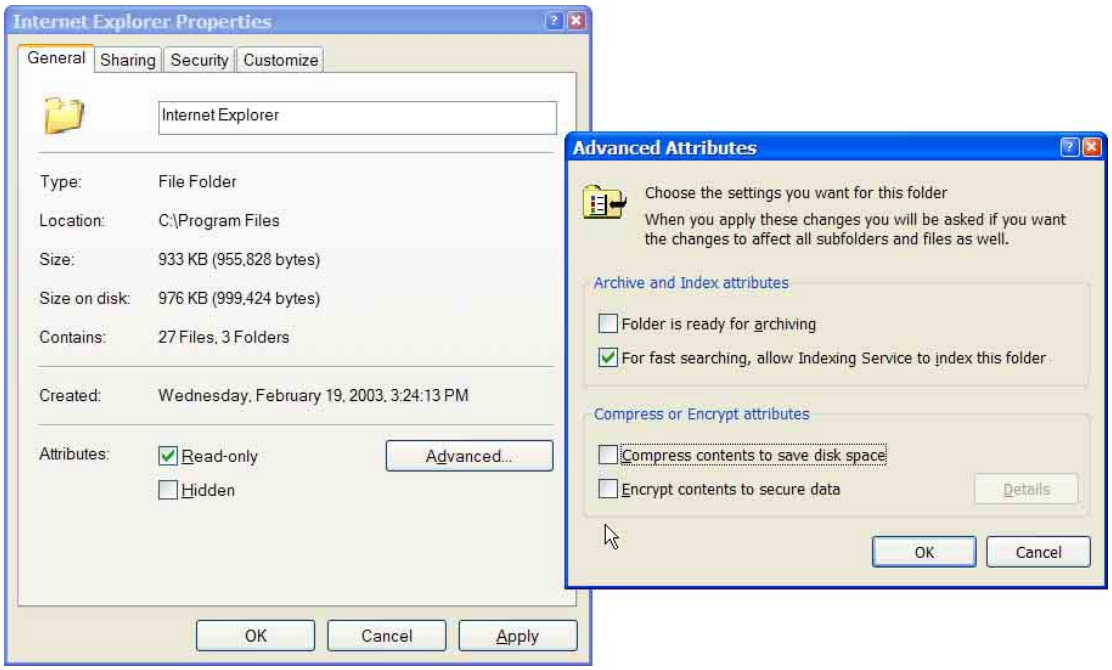
## 3.4. Uncompress and Decrypt All Data

Windows XP offers a method of saving space on your hard drive, called *compression*. Today's fast computers allow data to be compressed and uncompressed on-the-fly without affecting the operation and speed of the computer. Likewise, Windows XP offers an encryption feature that allows you to encrypt the folders and data that you choose. (Windows encryption is protected only by a password, whereas Kensington PCKey encryption protects your computer with two-factor authentication.)

You **must** uncompress and decrypt all data on your hard drive before installing Kensington PCKey.

You can check or change the compression and encryption status of a folder or files in Windows XP by selecting a folder in Windows Explorer, and "right-clicking." Click the *Advanced* button. In the *Advanced Attributes* dialog box (below, right) you have a choice to:

- *Compress contents to save disk space*, or
- *Encrypt contents to secure data*




Note that Windows does not allow you to select both the encryption and compression options at the same time. This is because compression and encryption are not compatible. You risk permanent loss of your data if you try to use compression and encryption technologies simultaneously.

Likewise, Kensington PCKey encryption cannot be safely used with folders that are compressed by Windows.

### Windows Uncompression and Decryption Procedure

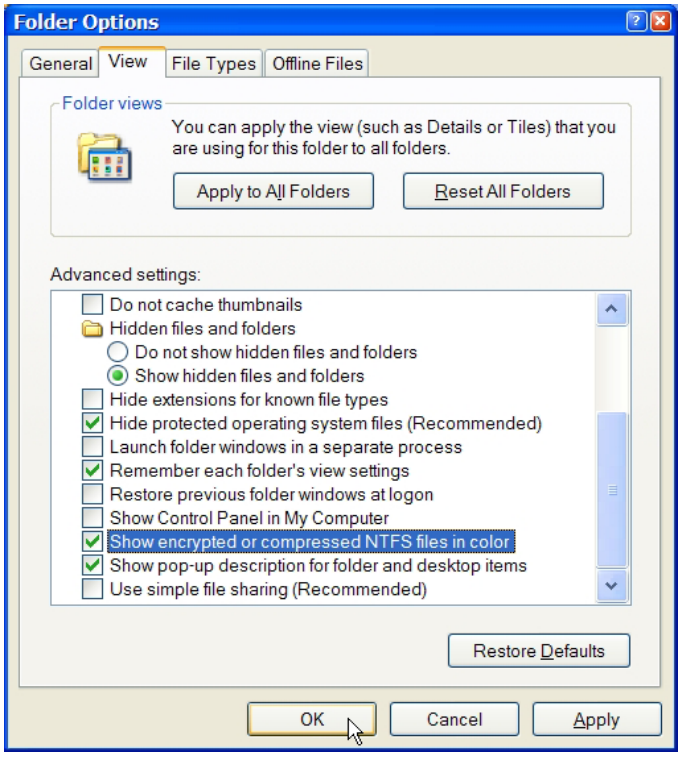
Follow this procedure to uncompress and decrypt all compressed or encrypted folders and files on your hard drive before installing Kensington PCKey.

#### I.) See which folders and files are compressed.

You can change settings in Windows to automatically highlight compressed or encrypted folders and files in light blue.

You may not see any compressed or encrypted folders after changing settings to see them. You may not have any compressed or encrypted folders on your computer.

- In Windows Explorer, click *Tools*, *Folder Options*, and the *View* tab.
- In the *Folder Options* window (below), select the following three options:
  - *Show encrypted or compressed NTFS files in color*
  - *Show hidden files and folders*
  - *Display the contents of system folders*
- Click *Apply*, then *OK* to close the *Folder Options* window.




#### II.) Uncompress and decrypt folders.

- In Windows Explorer, *right-click* on each folder displayed with an alternate color.
- In the context menu, click *Properties*.
- Click *Advanced*.

- Unselect *Compress contents to save disk space,* or *Encrypt Contents to secure data.*
- Click *OK*.
- Click *Apply*.
- Select *Apply changes to this folder, subfolder, and files*.
- Click *OK*, twice to close the dialog windows.

# 4. Install Kensington PCKey

 **Do not insert your Kensington PCKey in the USB port until you are instructed.**

**Let's Start!**

In just a few minutes, you will install the Kensington PCKey software, you will program your password into your Kensington PCKey, you will log in using your password, and Kensington PCKey will encrypt your hard drive. After installation, you will have a highly secure computer that even the most sophisticated hackers will be unable to access!

When you launch the Kensington PCKey installation application (setup.exe), an *InstallShield Wizard* guides you through Phase I of the installation process. The *InstallShield Wizard* makes the installation of application files automatic and easy for advanced and novice users alike.

**Time Needed**

You must follow directions in *Prepare Your Computer for Installation* before installing Kensington PCKey. In addition to time required for preparation, you will need approximately 15 to 30 minutes (or more for very large drives) to install Kensington PCKey, including encryption.

**Installation Overview**

During installation, your computer will automatically shut down and restart two times (for Phase I and Phase II of installation.) This is normal. Do not turn off the power switch, do not press the reset switch, and do not unplug your computer until the entire installation process is complete. If there appears to be a delay or "hang," be patient!

**Installation Phase I – PCKey USB Device Driver and Software Installation**

- Prepare your drive (empty Recycle Bin files, optional)
- Install Windows USB device drivers for the Kensington PCKey USB device
- Install Kensington PCKey software
- Restart Computer #1

**Installation Phase II – Password Setup, Hard Drive Preparation and Encryption**

- Set up your password (program your password in the Kensington PCKey)
- Prepare your drive (remove Windows' temporary files, etc.)
- Encrypt your hard drive
- Restart Computer #2

**Installation Phase III – Log In, Account Set-up, and Registration**

- Log in, and register your PCKey and Password

## 4.1. Installation Phase I – PCKey USB Device Driver and Software Installation

Installation Phase I includes:

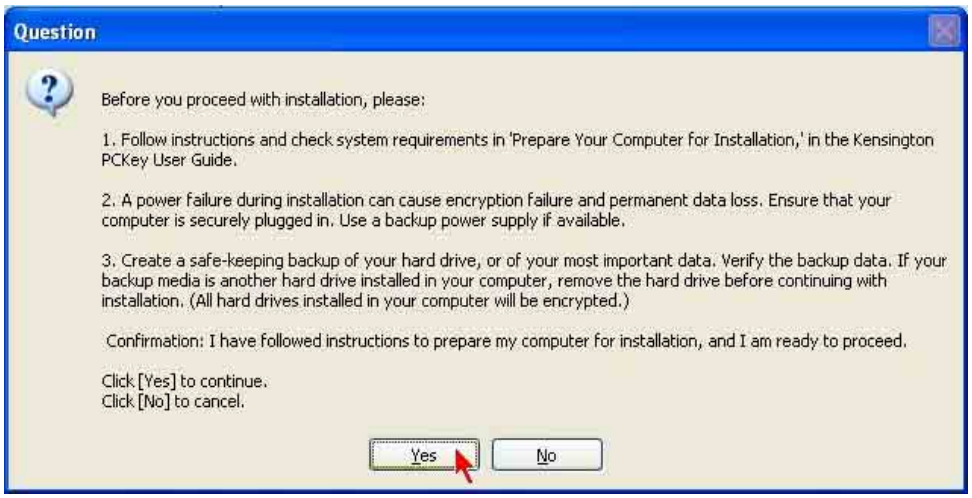
- Install Windows device drivers for the Kensington PCKey USB device
- Install Kensington PCKey application software

Read the *FAQs* section before you start the installation process! The FAQs section provides installation tips and other important information – such as which drives are encrypted, and which Windows operating system folders are excluded from encryption.

**Procedures**

**4.1.1.** Insert the **Kensington PCKey Installation CD**. The *InstallShield Wizard* should begin automatically. If not, click **Setup.exe** in the root folder on the CD. The InstallShield Wizard briefly displays a welcome screen (not shown.)

An advice message suggests important steps to take before you install Kensington PCKey.



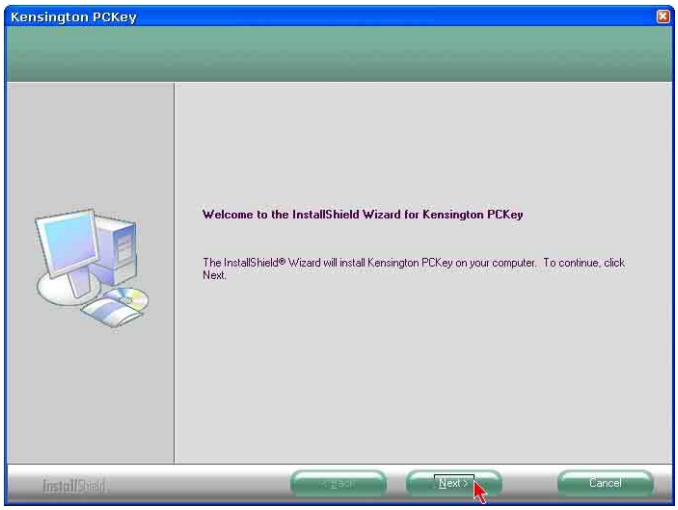

Click **Yes**.

**4.1.2.** The *InstallShield Wizard* prompts you to allow Kensington PCKey to empty the Recycle Bin on all local drives before continuing.

- Click **Yes** to continue if your Recycle Bin is empty or if you want to allow PCKey installation to empty the Recycle Bin.
- Click **No** to first restore files from the Recycle Bin. Clicking No cancels installation.

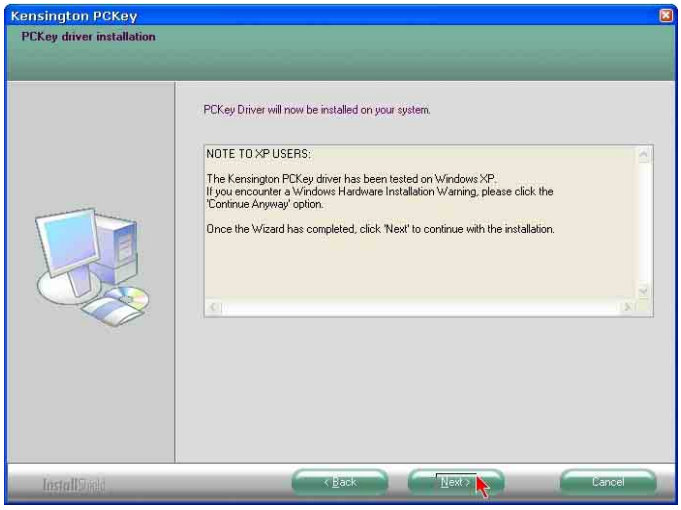

Click **Yes**.

**4.1.3.** The *InstallShield Wizard* welcome screen appears after the Recycle Bin is emptied.



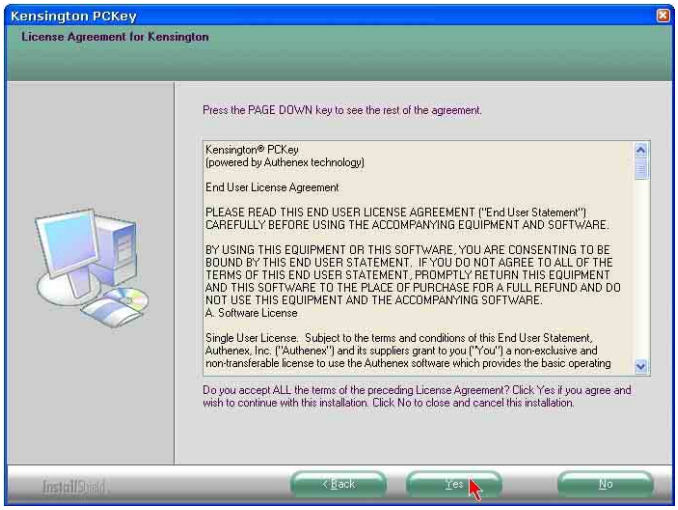

Click **Next.**

**4.1.4.** The *PCKey Driver Installation* window provides an informational message.

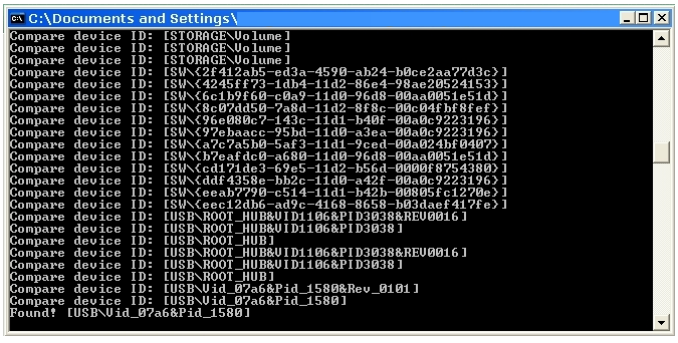



Read the message, and click **Next**.

**4.1.5.** The Kensington PCKey *End User License Agreement* appears.




Click **Yes** to agree with the license agreement and continue the installation of Kensington PCKey application files. The following screen briefly appears.



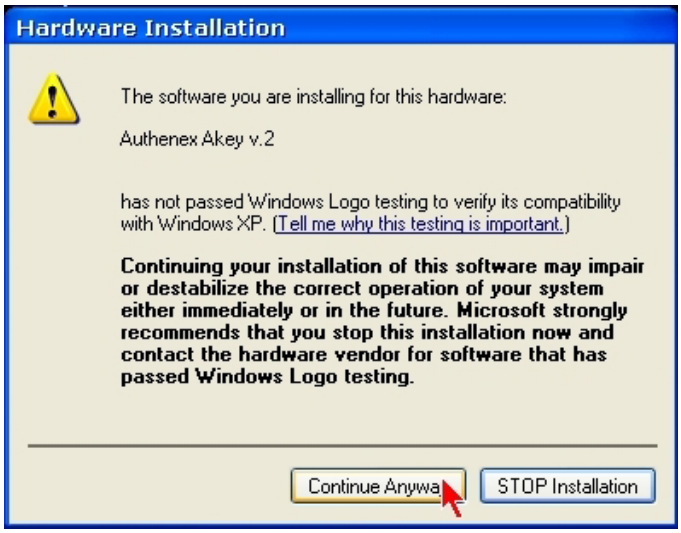
**4.1.6** A request message asks you to insert your Kensington PCKey in the USB Port.


**4.1.7.** Moments after you insert your PC-Key, Windows starts the ***Found New Hardware Wizard***. The *Hardware Wizard* installs Windows device drivers that are included on the Kensington PCKey installation CD. This is not the same as installing the Kensington PCKey application.

**NOTE!** The *Found New Hardware Wizard* will not start if a Kensington PCKey USB device has been inserted previously in your computer and device drivers are already installed (for example, if this is a reinstallation of Kensington PCKey.) If the Hardware Wizard does not start, click **OK** (in the message in Step 4.1.6.) and proceed now to Step 4.1.8.


Select **Install the software automatically**. Click **Next**.

Windows XP displays the following message. It is OK to continue. The drivers have been fully tested.




Click **Continue Anyway**.

The Hardware Wizard notifies you when it finishes installing Kensington PCKey USB device drivers.


Click **Finish**.

**Possible Error Message**: If you have Windows XP installed with the Service Pack 1 update [on the Start menu; go to *Settings / Control Panel / System* to check] you may receive a Found New Hardware Wizard error message informing you that the “Driver Cannot be Installed.” If you see this message, just unplug and reinsert your Kensington PCKey in the USB port. This will clear the error message and the driver installation will complete successfully.

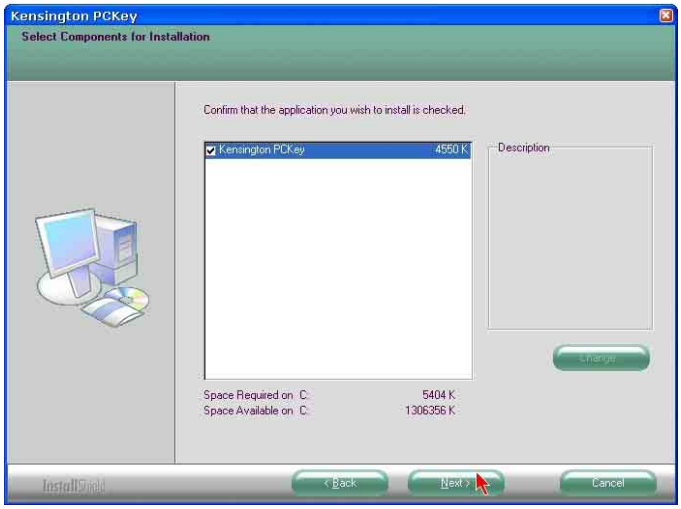
In addition, if you see the following message, reinsert your PCKey and click **OK**.


**4.1.8.** After the Found New Hardware Wizard (step 4.1.7), continue with the message box presented in step 4.1.6.

Click **OK.**

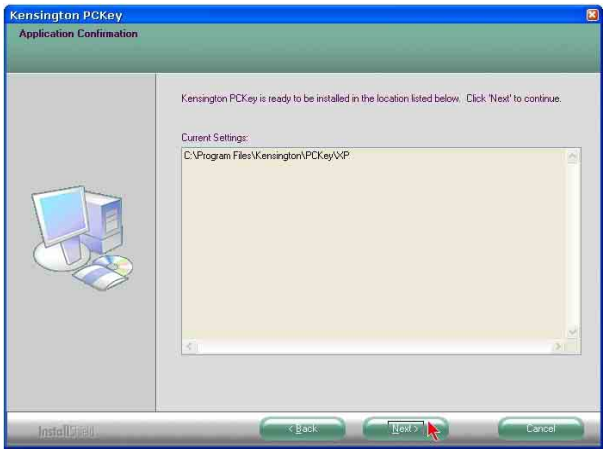
**4.1.9.** Select the component for installation. Verify that Kensington PCKey is selected. Kensington PCKey files are installed in C:\Program Files\Kensington\PCKey\XP.

(You do not have an option to install into a different folder.)

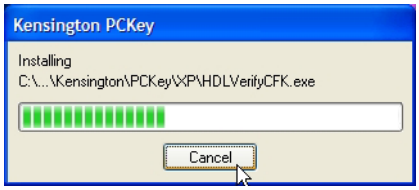



Click **Next**.

**4.1.10.** The *InstallShield Wizard* is ready to install Kensington PCKey application files, and asks for confirmation.

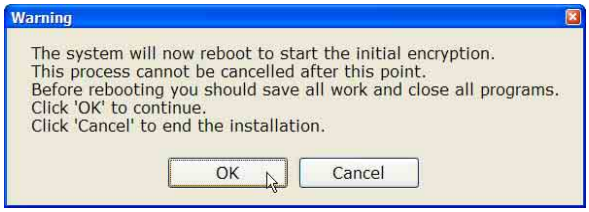



Click **Next**. A progress bar shows the installation status of the application files.




**4.1.11.** When the application files are installed, save all work and close all applications, and verify that you have followed instructions in *Preparing Your Computer for Installation*.

**IMPORTANT** – Before you click **OK,** this is the last opportunity you have to stop the encryption process. If you select OK, you will not have a “cancel” option in the remaining steps, and you must continue with the encryption of your hard drive.




Click **OK**. Kensington PCKey will automatically restart your computer.

**End of Installation Phase I**

The *InstallShield Wizard* part of the installation process is complete. The Kensington PCKey application files, and the new Windows PCKey USB device drivers are installed. The remainder of the installation process is performed by the Kensington PCKey application.

Do not remove your Kensington PCKey from the USB port.

## 4.2. Installation Phase II – Password Setup, Hard Drive Preparation and Encryption

Installation Phase II includes:

- Programming your password in your PCKey
- Preparation and encryption of your hard drive

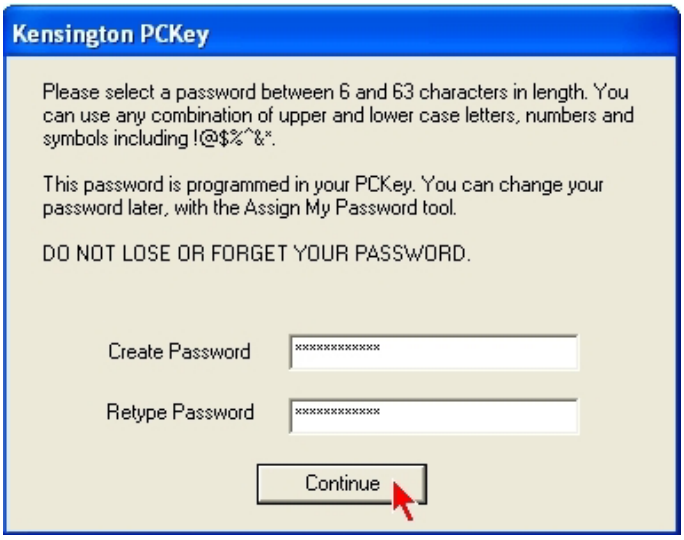
**Procedure**

**4.2.1.** The following message automatically appears when your computer restarts:


Click **Continue**.

**4.2.2.** You need to select and confirm a password to program into your PCKey. Type a password, and type the password again on the next line to ensure that you have not mistyped it the first time.

**NOTE**: If you are re-installing PCKey, or if you have used your PCKey with another computer, your PCKey will already have a password programmed into it. (You can use the *Assign My Password Tool* to change your password.) Skip this step and go to **4.2.3.**




Click **Continue**. Your password is now programmed in the PCKey.

**4.2.3.** Verify your password to start encryption. Type your password.


Click **Continue**.

**Tip:** If you want to quit now, enter the wrong password three times.

The next step begins hard drive preparation.

**4.2.4.** Empty temporary files (optional). Temporary files can slow down the encryption process. Temporary files are Windows-generated and considered safe to delete.

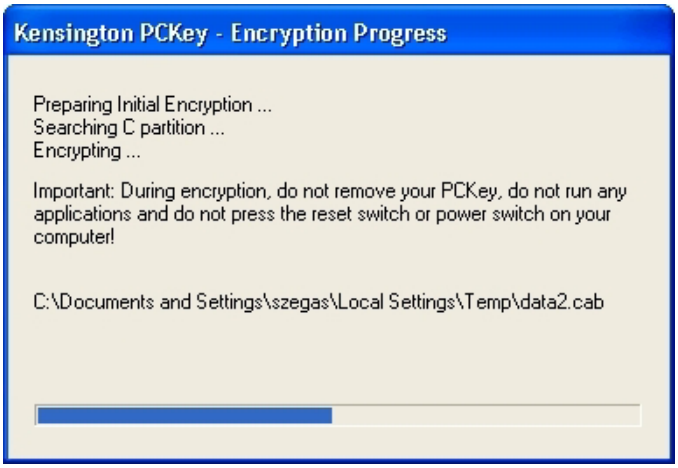
- Click **Yes** to empty the Windows temp folder (recommended). If you click *Yes*, Kensington PCKey deletes temporary files.
- Click **No** to continue without deleting temporary files.


Click **Yes,** or **No**.

**4.2.5.** Your hard drive is now ready to be encrypted. Kensington PCKey closes any open applications, and encrypts the hard drive.


Click **OK**.

During the encryption process, you see the following progress report:




After the hard drive is encrypted, Kensington PCKey automatically restarts your computer.

### End of Installation Phase II

Your password is programmed in your PCKey and your hard drive is encrypted. Your computer will now restart. In Installation Phase III, you logon with your PCKey and password, you create a new user account, and you register with Kensington.

Be sure to reconnect:

- Network connections (cable or DSL phone line Internet connection, Ethernet, or other connection) that you disconnected during preparation.
- Internal or external drives that you removed before encryption.

 If you need to reconnect or reinstall drives or connections, you can turn off power to your computer as soon as PCKey shuts down your Windows session. When you power up again, PCKey installation will continue.

## 4.3. Installation Phase III – Log In, Account Setup, and Registration

The Kensington PCKey password setup, and the hard drive encryption process is complete. Keep your PCKey in the USB port and re-enter your PCKey password to log in.

Installation Phase III includes:

- Logging in to Windows using the password you programmed in your PCKey
- Setting up one or more user accounts
- Registering your PCKey and password with Kensington

**Preparation**

- Read Section 4.4, *Set Up and Manage Kensington PCKey User Accounts*.

**Procedure**

**4.3.1.** When your computer restarts, you will see a new, Kensington PCKey **Logon Windows** screen. (This logon screen replaces the standard Windows Logon screen.)

- Verify that your Kensington PCKey is inserted into the USB port of your computer.
- Type your password.


Click **Log On**.

If the password is incorrect, Kensington PCKey denies access and displays the following:


Click **OK** to try again.

**4.3.2.** In User Account List, select **New Account.**

 See **Section 4.4** for information about creating and managing user accounts.


Click **OK.**

**4.3.3**. The *Add New User Account to Your PCKey* window appears.


The first time that you select New_Account, the *user account* and *domain/computer name* fields are filled in with your information (the user who installed PCKey.) Provide your Windows account password, and click **Log On**.

**4.3.4.** Finally, the following message appears when you log on for the first time.


Click **OK**.

After you set up the first PCKey user account, PCKey automatically starts the Registration process. Registration is the **only** protection you have to gain access to your computer if you lose your PCKey or password.

Go now to **Section 5.1**, Registration.

## 4.4. Set Up and Manage Kensington PCKey User Accounts

### Overview of Windows and Kensington PCKey User Accounts

Windows provides the option of having multiple Windows users (i.e., Windows logon usernames). This feature allows more than one person to use a computer, yet for each person to keep their individualized Windows configuration options such as email accounts, menu and desktop preferences, and access to certain folders and applications (called, resources).

Kensington PCKey supports multiple Windows users. For example, you may have two Windows users on your home computer, yourself and your spouse. Each user has a specific set of Windows resources – and a different Windows username and *password*.

With Kensington PCKey, you can set up multiple PCKey user accounts, one for each Windows user. This allows more than one person to use a single PCKey – without losing individualized Windows account resources.

 However, when multiple Windows users share a computer and PCKey, they will also share ONE PCKey password. PCKey currently does not support multiple passwords.

### Using One PCKey and Password with Multiple Users

The PCKey password (programmed in the PCKey) remains the same for all users. Thus, any user with a PCKey user account can log in as any other PCKey user on the computer.

For example, the users *joesmith* and *marysmith* have Windows user accounts with different passwords. After they install Kensington PCKey and they each set up a PCKey user account, they will no longer use their Windows password to logon to Windows. With PCKey, they will use the same PCKey password. Thus *joesmith* can log in as *marysmith* — using *marysmith* as the username, and the one PCKey password.

Note that Windows still requires the user's password when logging in. When users set up a new PCKey account, they provide their Windows password and logon name. PCKey stores this information and uses it ("quietly") to log in the Windows user.

### Understand Local and Domain Computers

**Local and Domain User Accounts** – There are two types of Windows user accounts, local and domain. As a rule, you can create a new PCKey user account only for users who already have an *existing* Windows local and/or network domain account.

**Local** – A Windows local user account is for a user on a non-networked computer, or for a user on a networked computer who does not have network access (only access to the local computer.) In either case, the PCKey "User Account" name is the same as the Windows user's logon name.

**Domain** – A Windows domain user account is for a user on a networked computer who does have network access. If you want to create a PCKey user account for a domain

user, that user must be set up with an account in the network domain before you create their PCKey user account.

 Do not confuse “networked” with Internet access. You can have a non-networked (“local”) computer that has Internet access.

### Create a New Windows and PCKey User Account

To create a new *Windows* user account, a user with administrative privileges must logon and set up a new user in Windows Control Panel. Next, the administrator must log off, or the computer must be restarted.

Subsequently, the new user can log in (with the PCKey and password) to create a new PCKey user account. (See steps 4.3.2 and 4.3.3.)

At the PCKey Logon Windows screen, (Step 4.3.1) the new user should provide the PCKey password. Next, PCKey asks you to select the user to log in. Select **New_Account** and click OK. Enter the new Windows user’s User Account name, the Domain/Computer name, and (Windows) Account Password – and click Log On. The new PCKey account is stored in the PCKey (i.e., the user’s Windows credentials are stored in the PCKey) and the new user is logged on.

### Fields in the Create New User Dialog Screen

**User Account** – The user account is the same name as the Windows logon account name.

**Domain/Computer Name** – When you create a new PCKey user account, PCKey automatically enters the name of your computer or domain (it does have an identity) in the Domain/Computer Name field. If your computer is networked, change the domain name to the Domain Name of your LAN. If your computer is not networked, leave the (local) name of your computer.

**Account Password** – This is the password the user normally uses when logging on to Windows, not the password programmed in the PCKey. The Windows password is used only when creating a new PCKey user account, not for routine logon using PCKey. After a new PCKey user account is created, the new PCKey user will use their PCKey password to logon.

# 5. Using Kensington PCKey Tools

Kensington PCKey provides several tools to assist you in using your PCKey. Most importantly, the Registration Tool provides a backup solution for you if you lose your password or your PCKey.

The tools are:

- Registration Tool
- PCKey and Password Recovery Process
- Assign My Password Tool
- File Recovery Tool
- Configuration Tool

### Tool Descriptions

- The **Registration Tool** allows you to register your PCKey and your password safely and securely online, with Kensington. Registration is a prerequisite in the event that you ever need to use the *PCKey and Password Recovery Process.*
- The **PCKey and Password Recovery Process** is an online service that allows you to obtain access to your computer is you lose either your PCKey or password.
  - **Password Recovery** allows you to retrieve your password securely online (using another computer.)
  - **PCKey Recovery** allows you to access your computer (using a special "pass-key" code that you obtain securely online, from another computer) in the event that you lose your PCKey.
- The **Assign My Password Tool** allows you to change the password programmed in your PCKey.
- The **File Recovery Tool** is used in the event of a decryption error during the uninstallation of Kensington PCKey. If any files fail to decrypt during uninstallation, Kensington PCKey generates a special message that allows this utility to work. It works only when this error message is generated.
- The **Configuration Tool** is reserved for use by instruction of Kensington PCKey customer support. It sets the internet address used for Kensington PCKey online services.

### Kensington PCKey Tool Locations

The *Assign My Password Tool*, *Configuration Tool, Registration Tool,* and *File Recovery Tool* are available on the Start menu. Go to ***Programs / Kensington / PCKey / (tool name)***.

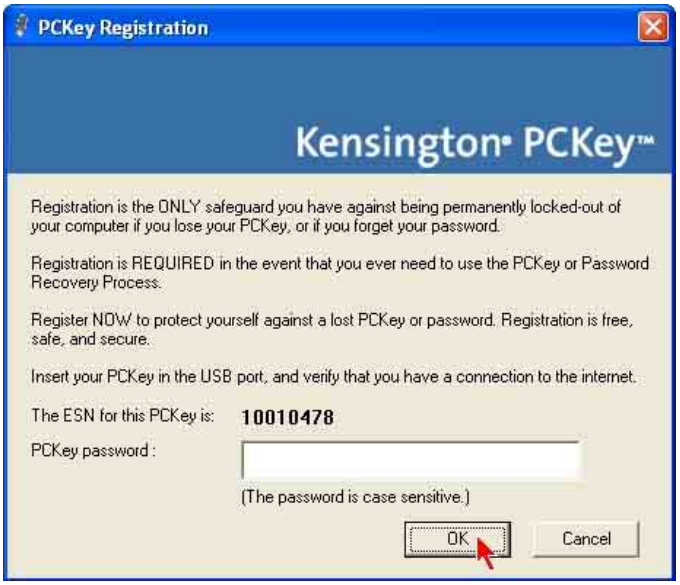

The *PCKey and Password Recovery Process* is available online at www.pckey.kensington.com.

## 5.1. The Registration Tool

The **Registration Tool** allows you to register your Kensington PCKey and your password safely and securely online, with Kensington. Registration safeguards you against loss of your data due to a lost password or lost PCKey. Registration is a prerequisite in the event that you ever need to use the *PCKey and Password Recovery Process.*

#### Procedure

**5.1.1.** On the Start menu, go to *Programs* / *Kensington* / *PCKey* / *Registration Tools*. Type your **PCKey password**.

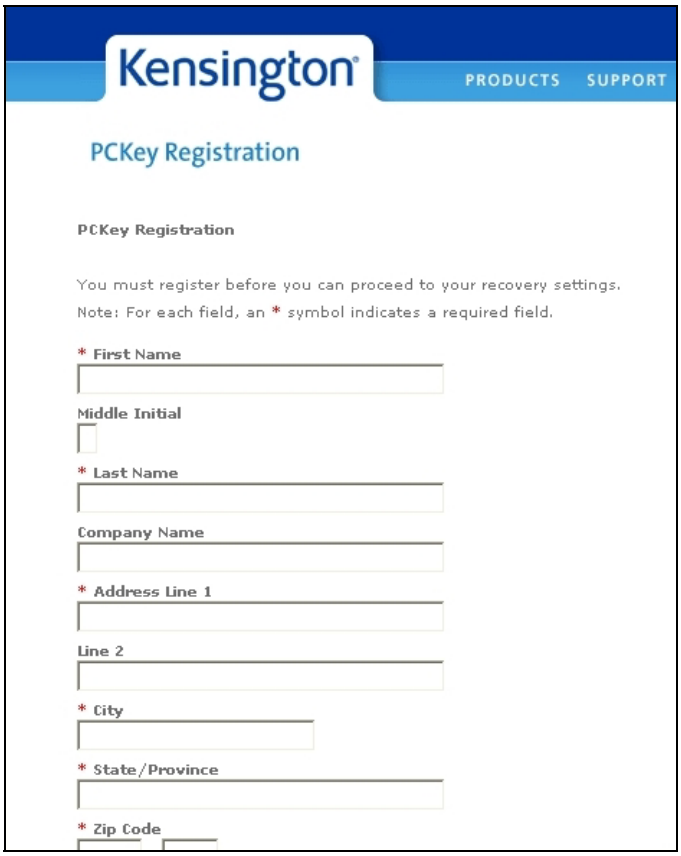



Click **OK**.

**5.1.2.** The Registration Tool checks and authenticates your password, and connects you to the Registration server.

If you enter the wrong password, a *Password Check Failed* message appears. You are allowed three attempts to enter the right password. After the third failed attempt, the Registration Tool closes.

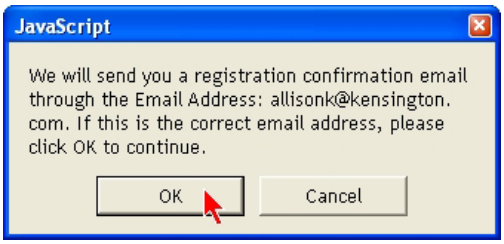
**5.1.3.** The Kensington PCKey Registration screen appears in your web browser.



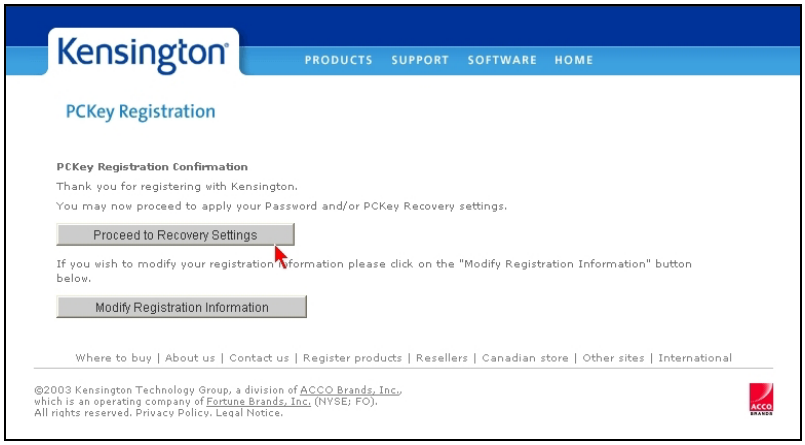

Fill in the form. Click **Submit**.

### 5.1.4. Online Registration Pages

The Registration Tool prompts you to fill in several pages of information. Enter all requested information and complete the registration process. When you complete the registration process, the Registration server sends a verification message to you by email.



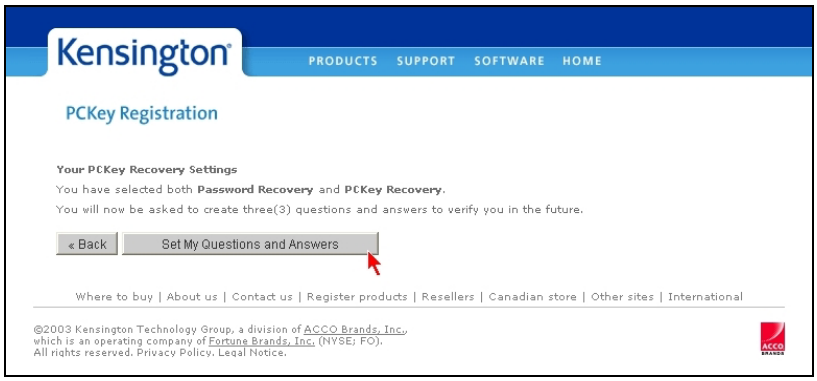

The following graphics show the Kensington PCKey Registration pages you use to register. After the first registration page, proceed to recovery settings, displayed below.



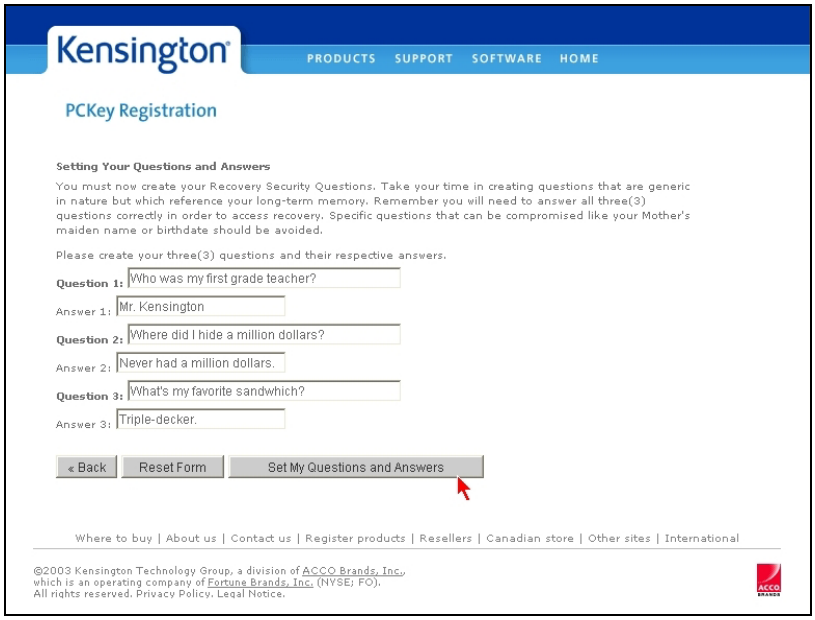

Set your *Questions and Answers*. Kensington PCKey identifies you by requesting the correct answers to your questions. If you do not answer your questions correctly, you cannot use the PCKey and Password Recovery Process.

The “Three Questions and Answers” that you provide are essential to authenticate your identity if you lose your PCKey or password, and you need to use the PCKey and Password Recovery Process.

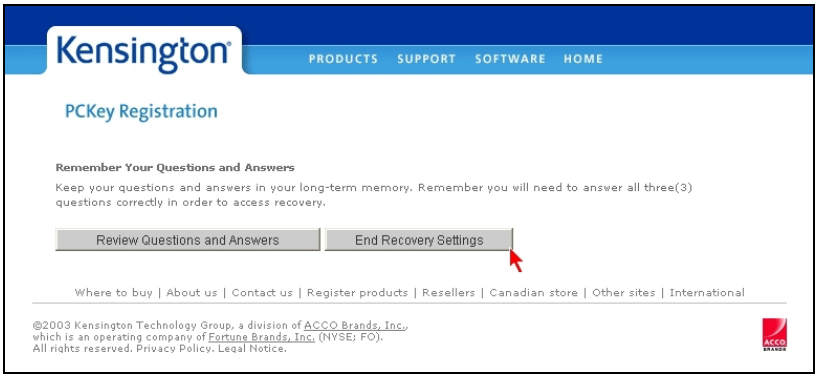
**DO NOT FORGET THE ANSWERS TO YOUR QUESTIONS.**




Be careful! Pick questions and answers that you can easily remember.




Choose either *Review Questions and Answers*, or *End Recovery Settings* to exit.



## 5.2. The PCKey and Password Recovery Process

If you lose your PCKey or your password, your computer is secure, safe, and inaccessible – and has just become a very expensive paperweight. Or has it?

The **PCKey and Password Recovery Process** is an online service that allows you to obtain access to your computer is you lose either your PCKey or password.

- If you lose your Kensington PCKey or password, and you have not registered first, we are sorry. There is nothing we can do to decrypt your hard drive. It is impossible.

**How does the PCKey and Password Recovery Process work?**

- Access the PCKey and Password Recovery Process at http://pckey.kensington.com.
- A browser window opens, bringing you to the **Recovery Process** web page.


- Follow directions provided in the *Recovery Process*.
- When your identity is confirmed, you can follow directions to either recover your password, or if you have lost your PCKey, to log in to your computer using a Key Puzzle—Key Answer.

**How does the Key Puzzle—Key Answer work?**

The Kensington PCKey log in screen provides you with a Key Puzzle, for example: 69dd14aa9b4062bfde0d20c29fb0a49a.

Using another computer, use the PCKey and Password Recovery Process to get your Key Answer. After verification of your identity, you receive a Key Answer, for example bfde0d2069dd14a29fb0a49aa9b4062c. Back on your computer, choose Logon on with Key Answer, and type the Key Answer in the space provided.

 The Key Puzzle–Key Answer replaces the (lost) Kensington PCKey, however, you will need to type in the Key Answer every time you start your computer.


**Procedure**

- In the Kensington PCKey Logon Windows screen, select *Log On with Key Answer*.
- Write down the *Key Puzzle*.
- Access the PCKey and Password Recovery Process from another computer, at http://pckey.kensington.com.
- Answer the questions that verify your identity, and provide the *Key Puzzle* when asked for it.
- Write down the *Key Answer* provided to you.
- Back on your computer, type the *Key Answer* in the Logon Windows screen.
- Click **Log On**.

  You do not need to provide your password when you use the Key Puzzle–Key Answer method to log in.

**Can I use my Kensington PCKey if I find it after using PCKey recovery?**

Yes. You will be able to use your Kensington PCKey if you find it after you use a Key Puzzle–Key Answer. However, after you use your PCKey again, the Key Puzzle–Key Answer will change and you will have to get another Key Answer if you lose your Kensington PCKey again.

**Can I get a replacement Kensington PCKey?**

No. It is not possible to replace a Kensington PCKey.

If you do not find your PCKey and you do not want to continue using the Key Answer to log in, uninstall Kensington PCKey (you can do this with the Key Question–Key Answer) and purchase a new Kensington PCKey.

## 5.3. The Assign My Password Tool

The **Assign My Password Tool** allows you to change the password programmed in your Kensington PCKey.

Important! If you change your password, use the *Registration Tool* to change the password stored for you! Your new password is not sent automatically to the Registration server at Kensington. You must register your new password with Kensington after you change it.

**Procedure**

**5.3.1.** On the Start menu, go to *Programs* / *Kensington* / *PCKey* / *Assign My Password Tool.*


**5.3.2.** The **Assign My Password** message appears.

Verify that your Kensington PCKey is inserted in the USB port.


Click **Continue**.

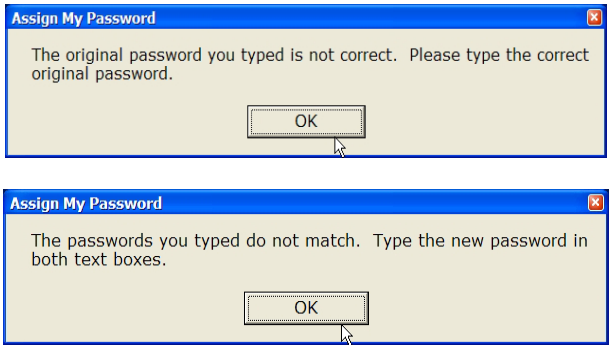
**5.3.3.** The **Assign My Password** dialog box requests old and new passwords:

- Enter your current password on the first line
- Enter a new password in the second line, and enter the password again on the third line, to ensure that you have not mistyped it the first time

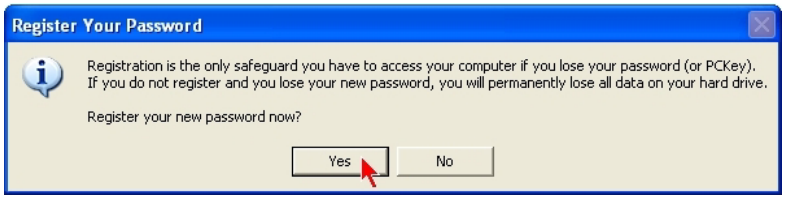
The password must have six to sixty-three characters. You can use any combination of upper and lower case letters, numbers and symbols (!@$%^&*).

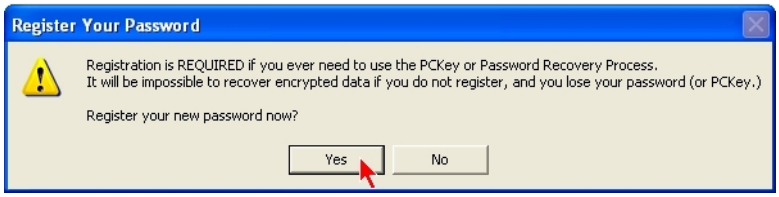

Click **Next**.

**5.3.4.** You will receive an error message either if you mistype the original password, or if you do not type the same new password on the *new* and *confirm password* lines. For example:




**5.3.5.** You are asked to register your new password with Kensington.






Click **Yes** to register your new password with the Kensington Registration process.

**5.3.6.** After you register (or click NO to Register,) the *Password Completed* message indicates that your new password is successfully programmed in your PCKey.


Click **Finish**.

## 5.4. The File Recovery Tool

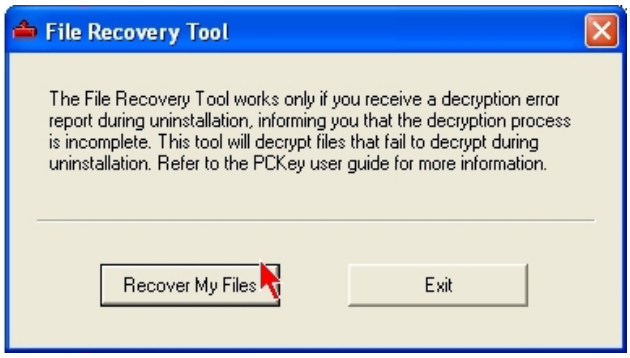
The **File Recovery Tool** is a “backup” utility provided to assist with the decryption of files that fail to decrypt during uninstallation. (This tool does not create a backup copy of your hard drive.)

If any files fail to decrypt during uninstallation, Kensington PCKey generates a decryption error report (see Section 6.2.) In the event of a decryption error report, you can use the File Recovery Tool to decrypt files that did not decrypt during uninstallation. The File Recovery Tool works only when a decryption error report message is generated.

**Procedure**

**5.4.1.** On the Start menu, go to *Programs* / *Kensington* / *PCKey* / *File Recovery Tool.*

The File Recovery Tool opens.



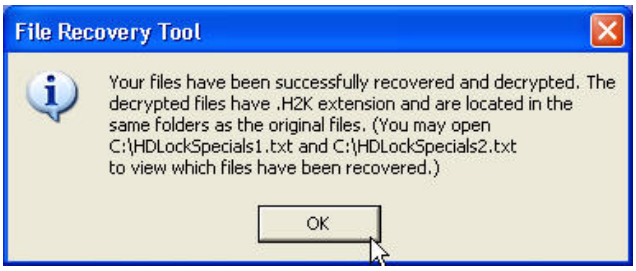

Click **Recover My Files**.

**5.4.2.** If there are no files to recover, the following message appears.


Click **OK**.

**5.4.3.** If you use the File Recovery Tool, recovered files are located in their original folder.

Recovered files are given a .H2K extension to the file name. For example, the file Budget.xls is recovered as a duplicate file in the same folder, named Budget.xls.H2K. The recovery message tells you the name of the report to view to see which files have been recovered.




To use recovered files, rename or delete the original (encrypted) file(s), and rename recovered (decrypted) files by removing the .H2K file extension.

Click **OK**.

## 5.5. The Configuration Tool

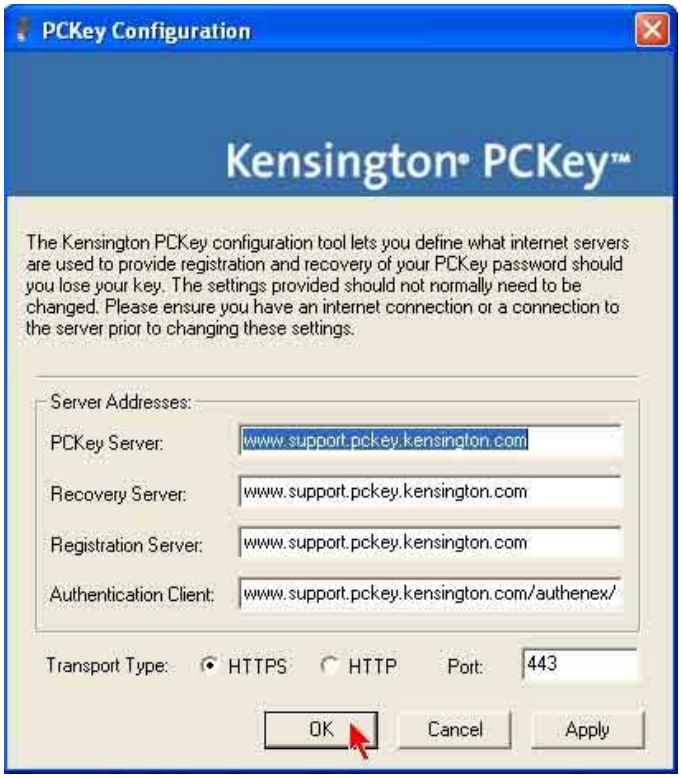
The **Configuration Tool** is reserved for use by instruction of Kensington PCKey customer support. It sets the internet address used for Kensington PCKey online services (Registration, and the PCKey and Password Recovery Process.)

If you are unable to connect to Kensington PCKey online services, contact PCKey customer support for assistance with setting the correct parameters.

### Procedure

On the Start menu, go to *Programs / Kensington / PCKey / Configuration Tools*.

In the Configuration Tool, set the correct *Server Address, Transport Type,* and *Port* parameters as instructed by PCKey customer support.




Click **Apply**.

Click **OK**.

# 6. Uninstall Kensington PCKey

When you uninstall Kensington PCKey, all of the encrypted data on your hard drive is decrypted, and the Kensington PCKey application files are uninstalled by the InstallShield. Kensington PCKey will automatically restart your computer after uninstallation.

Note that if there is a decryption error report, (see Section 6.2) Kensington PCKey application files are not uninstalled automatically by the InstallShield, and your computer does not automatically restart.

 **TIP:** Your Kensington PCKey still has your password programmed into it. Remember to keep your password for when you want to reinstall Kensington PCKey.

**Time Needed**

The uninstall process requires approximately 10 minutes (possibly up to an hour for very large hard drives and/or slower computers.)

**Preparation**

Decryption requires all contents of the Recycle Bin to be emptied. You can allow Kensington PCKey uninstallation to empty the Recycle Bin for you, or you can empty the contents of the Recycle Bin yourself (and optionally restore any items that you want to save) before you start uninstallation.

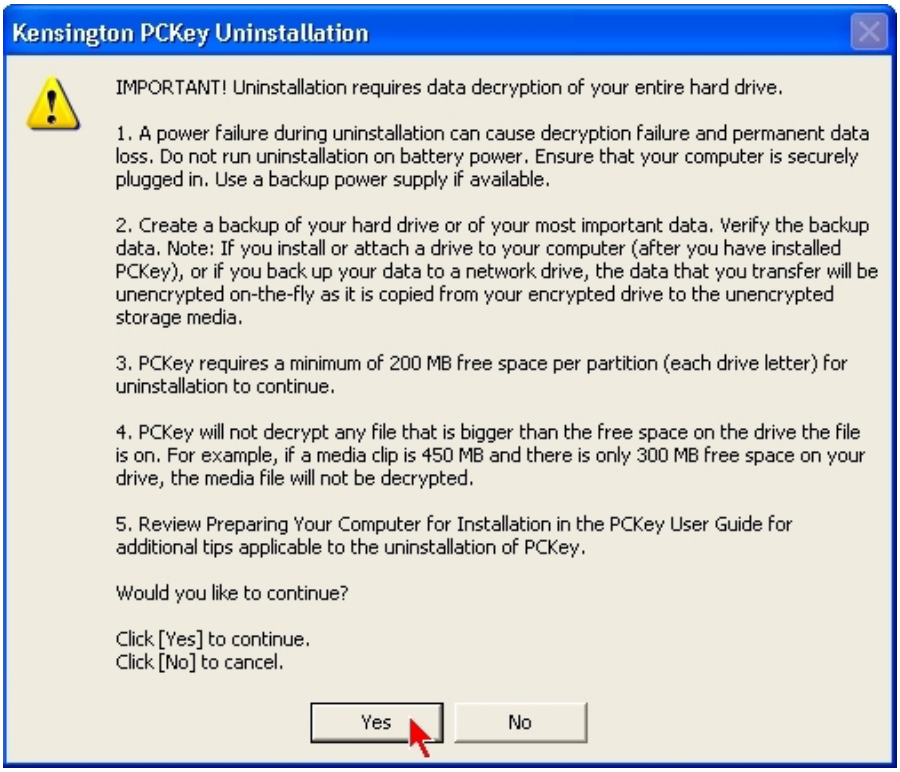
Uninstallation must be performed by the same user who installed PCKey.

## 6.1. Uninstall Procedure

Insert your Kensington PCKey into the USB port of your computer.

**6.1.1.** On the Start menu, go to *Programs* / *Kensington* / *PCKey* / *Uninstall PCKey*. The following instructional message appears.

**Important!** Follow instructions provided in the message.

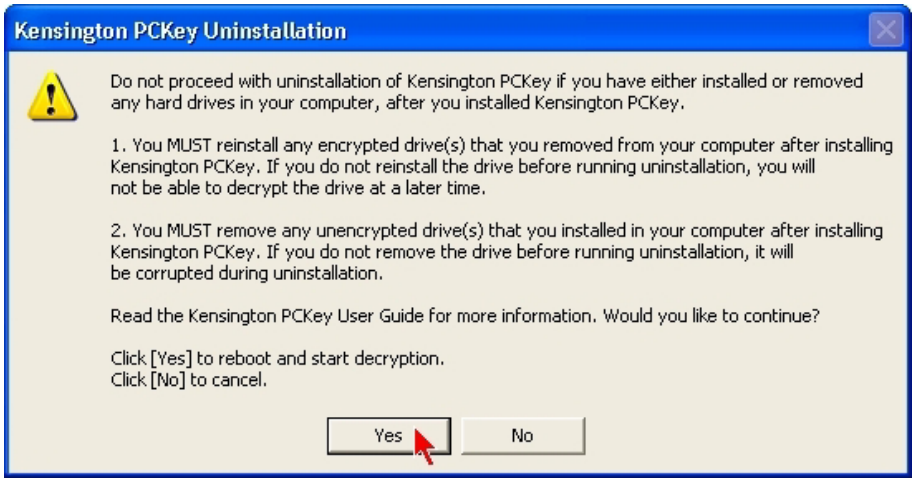



Click **Yes** (only if you have followed pre-uninstallation procedures.)

**6.1.2.** The following confirmation message appears. You **MUST** restore the hard drive configuration you had when you installed PCKey:

- Encrypted drives that you removed from your computer after installing PCKey must be reinstalled in your computer before you uninstall PCKey.
- Unencrypted drives that you installed in your computer after installing PCKey must be removed from your computer before you uninstall PCKey.

**Important!** Follow instructions provided in the message.

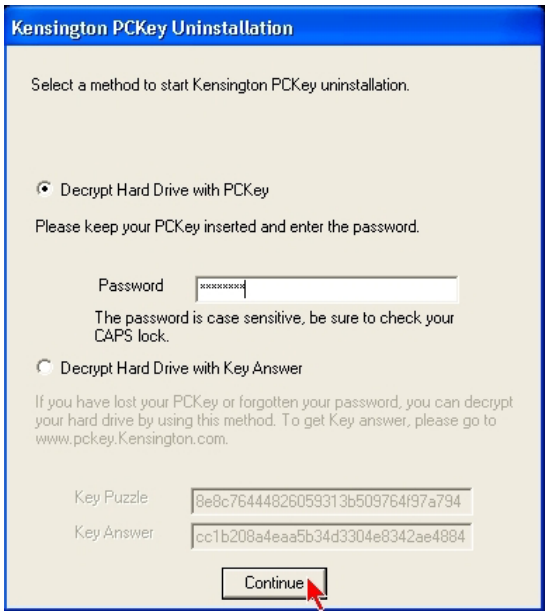


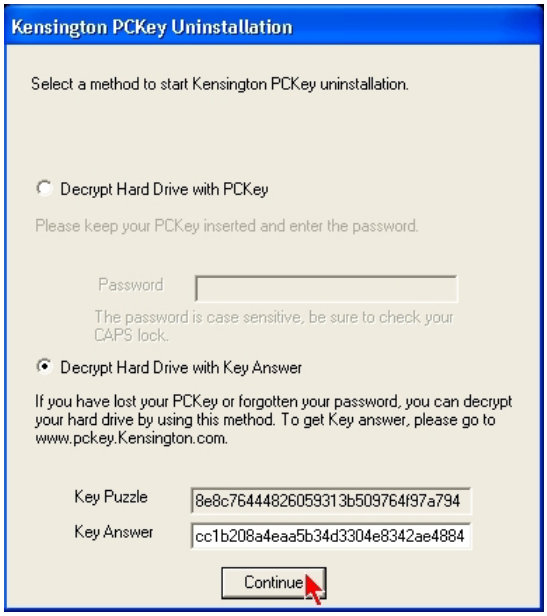

**6.1.3.** The Decrypt Hard Drive password request screen appears.

Select **Decrypt Hard Drive with PCKey**. (Or, if you obtained a Key Answer from using the *PCKey and Password Recovery Process*, select **Decrypt Hard Drive with Key Answer**.)

Select you logon method and type your PCKey **password** (or your **Key Answer**.)

**Tip:** If you want to quit uninstallation now, enter the wrong password three times.




Click **Continue**.

**6.1.4.** Empty the Windows temporary folder (recommended) and continue.

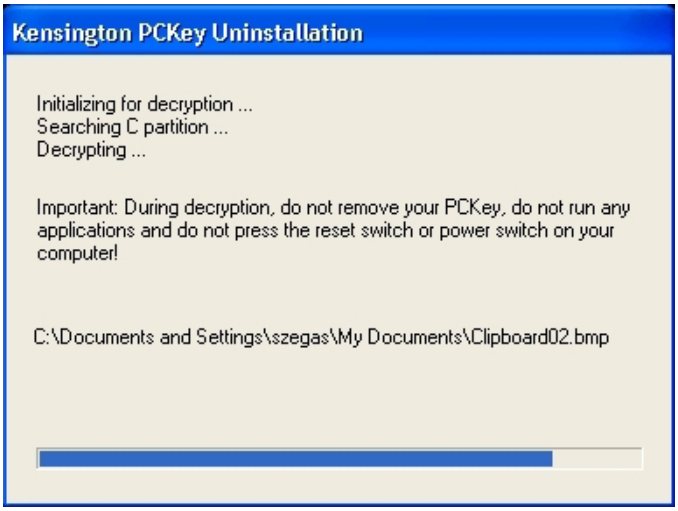

Click **Yes**. Click **No** to continue without emptying the temporary folder.

**6.1.5.** Informational message.


Click **OK**.

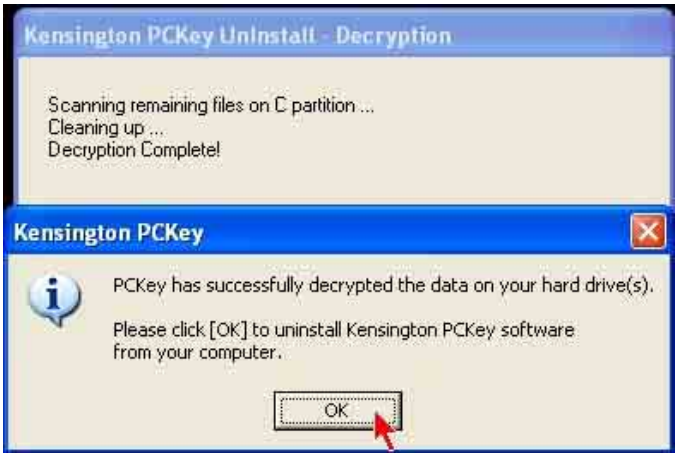
**Caution:** Any interruption in the uninstallation process after this point can result in the permanent inability to decrypt files on your hard drive. **Do not cancel the uninstall process**. If you change your mind, complete the uninstallation, and reinstall PCKey again.

**6.1.6.** Kensington PCKey begins decryption.



Do not turn off the power switch, and do not press the reset switch until the entire uninstallation process is complete. If there appears to be a delay or “hang,” be patient!

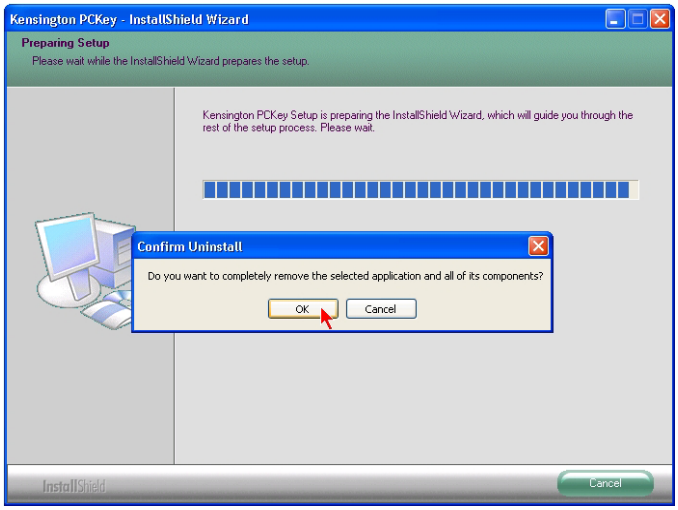
**6.1.7.** Informational message. Decryption is finished.




Click **OK**.

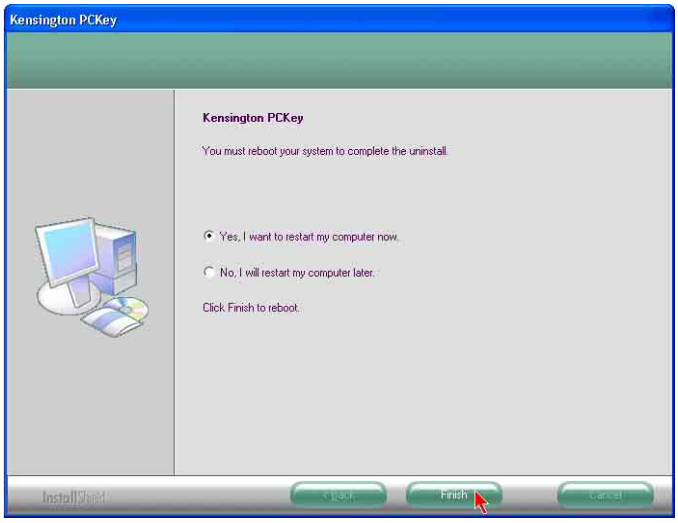
**Note:** If you receive a decryption error report during decryption that says, the “decryption process is incomplete,” go to Section 6.2 now. (The InstallShield Wizard will not start and your computer will not restart automatically if you receive a decryption error report.)

**6.1.8.** Uninstall Kensington PCKey software.




Click **OK**.

**6.1.9.** Restart your computer. Select **Yes, I want to restart my computer now**.

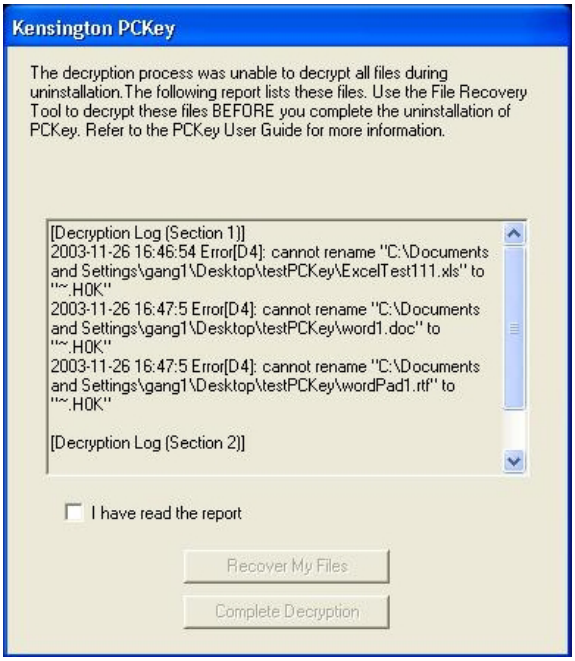



Click **Finish**.

To confirm that the application removed successfully, on the Start menu, go to *Programs* and verify that *Kensington / PCKey* has been removed.

## 6.2. Decryption Error Report

**6.2.1.** If you receive a decryption error report that indicates that some files were not successfully decrypted, you have an option to select either *Recover My Files* or *Complete Decryption*.

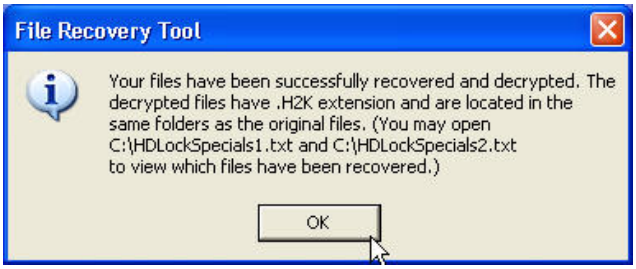


- If you select “Complete Decryption,” you will still have files on your hard drive that did not decrypt during the decryption process. To recover these files, you can use the File Recovery Tool after the decryption process completes, to run the *Recover My Files* process. Alternatively;
- If you select “Recover My Files,” the same file recovery process occurs as provided in the File Recovery Tool.

Select **I have read the report**.

Click either **Recover My Files** or **Complete Decryption.**

If you select *Recover My Files*, recovered files are located in their original folder. Recovered files are given a .H2K extension to the file name. For example, the file Budget.xls is recovered as a duplicate file in the same folder, named Budget.xls.H2K. The recovery message tells you the name of the report to view to see which files have been recovered. To use recovered files, rename or delete the original (encrypted) file(s), and rename recovered (decrypted) files by removing the .H2K file extension.




If you use *Recover My Files*, you do not need to use the File Recovery Tool. If you do *not* use this option *during the file decryption stage of uninstallation*, you should run the File Recovery Tool before you complete the uninstallation of the Kensington PCKey application (in Step 6.2.2.)

**6.2.2.** After you select *Complete Decryption* or *Recover My Files*, you need to (continue to) uninstall Kensington PCKey.

On the Start menu, go to *Programs / Kensington / PCKey / Uninstall PCKey*. The InstallShield opens to continue with uninstallation (as depicted in Step 6.1.8.)

# 7. Kensington PCKey FAQs

This section provides answers to many common questions about Kensington PCKey functions, features, capabilities and limitations.

Encryption technology is widespread and is at work in virtually every area of business, education, government, military, and private use. All software applications, including encryption solutions, have technical limits. Known issues for Kensington PCKey are included in this section.

## Contents

### Recovering Data After Losing My PCKey or Password

**Q 1.** I have not registered my PCKey and password. Can I recover data on my hard drive if I lose either?

**A. No!** You can recover (decrypt) data on your hard drive only if you register your PCKey and password with Kensington PCKey: www.pckey.Kensington.com

### Choosing Internal Drives to Encrypt or Not to Encrypt

**Q 2.** Are all drives encrypted during installation? Can I exclude hard drives or drive letters from encryption during installation?

**A.** By default, all drives and drive letters are encrypted during installation if the drives are installed internally. If you have one physical hard drive ("a primary drive") that is partitioned into several drive letters, all "drives" on that hard drive will be encrypted during installation.

If you have two or more physical drives installed, the secondary hard drive (and all drive letters) will also be encrypted during installation. If you want to exclude any secondary hard drives (and all drive letters on that drive) from encryption, remove the drive(s) from the computer before installing PCKey. You can safely re-install the drive after PCKey installation is complete. The secondary drive(s) will not be encrypted during use.

If you want to install a second drive after installing PCKey and you want to encrypt the second drive, you must follow these steps: uninstall PCKey before installing the new drive; install the new drive; and finally, reinstall PCKey. During PCKey installation, all installed drives are encrypted.

### Using Removable, External and Network Drives, and Flash Memory Devices

**Q 3.** Can I encrypt removable drives, external drives attached to my computer, or network drives?

No. You cannot encrypt or use PCKey protection with external drives or removable drives (such as those attached by USB, Firewire or PCMCIA; or an internal or external ZIP drive.) Also, you cannot encrypt or use PCKey protection on a (remote) network drive. You can use removable, external and network drives normally with PCKey after PCKey installation (removable, external and network drives remain unencrypted and function normally when reconnected after PCKey installation.)

**NOTE!!** Any data transferred from a PCKey-encrypted internal drive to a removable, external or network drive is decrypted when copied to the removable, external or network drive.

**Q 4.** Are external or removable drives, or flash memory cards encrypted during PCKey installation?

**A.** PCKey is not designed to support the encryption of externally connected drives, such as USB and Firewire drives, flash memory cards and flash memory drives, or

ZIP drives. However, in some instances of installation, an external or removable drive or flash storage device may be encrypted. Follow directions to remove or disconnect any drive or storage media that you do not want to encrypt during PCKey installation.

**Moving Drives from the PCKey Computer to Another Computer**

**Q 5.** Can I move an encrypted secondary drive from one computer to another after installing PCKey? (Can I install PCKey on a second computer, and move/install a drive encrypted in the first computer to the second computer?)

**A.** No. You cannot move an encrypted hard drive to another computer that also has PCKey installed. Each installation of PCKey uses a different encryption algorithm. This means that PCKey-encrypted drives cannot be moved to another computer to be used as a secondary drive.

**Restoring Drive Configuration Before Uninstalling PCKey**

**Q 6.** What rules must I follow if I want to uninstall PCKey?

**A.** You must restore the drive configuration you had at the time you installed PCKey, before you uninstall PCKey.

 **NOTE!!** If you installed a second hard drive in your computer after you installed PCKey, it will work normally, as an unencrypted drive. You **MUST** remove the unencrypted drive from your computer before you uninstall PCKey. If you uninstall PCKey without removing the unencrypted drive, the drive will be irrevocably corrupted during uninstallation.

 **NOTE!!** If you plan to uninstall PCKey, you **MUST** (re)install any encrypted secondary drives that were installed at the time of PCKey installation and that you have since removed – *before* you uninstall PCKey. You cannot decrypt a secondary drive after you uninstall PCKey; that is, if you reinstall PCKey software again on the primary drive, then install the previously encrypted secondary drive, and finally uninstall PCKey (to decrypt both drives), the secondary drive will not decrypt. The encryption process is unique to each installation of PCKey. If you fail to reinstall the encrypted secondary drive before you uninstall PCKey, the secondary drive will remain irrevocably encrypted and unrecoverable.

**Identifying Which Drives are Encrypted and Which Are Not**

**Q 7.** I want to uninstall PCKey. I have read the uninstallation information regarding secondary drives that I removed and/or installed in my computer after I installed PCKey. I am not sure which drives are encrypted and which are not – how can I find out?

**A.** First, create a record, or mark the physical configuration of the drives in your computer at the time you install PCKey. Second, if this is unavailable, start your computer in Safe Mode. Open a .txt file (that is in an encrypted folder, see below.) If the file is encrypted, the drive it is on is encrypted. If the file is not encrypted, the drive it is on is not encrypted.

### Installing PCKey USB Device Drivers

**Q 8.** During installation of the USB device drivers, I received an error message that the new hardware was not successfully installed.

**A.** If you see this error message, unplug the PCKey and plug it back in. This will clear the error and will enable the device driver to install.

### Using Windows Update and Other Online "Live Update" Services

**Q 9.** Can I use Microsoft online *Windows Update* and other automatic, online "live update" systems?

**A.** Yes. You can, for example, use *Windows Update* to update Windows XP to Service Pack 1 with PCKey installed. You can update and install operating system files, and applications online – just the same as from a CD. After installation of PCKey, all procedures for installation, upgrade and uninstallation of software on your computer remain the same.

### Installing PCKey on Networked Computers

**Q 10.** Can I install PCKey on a networked computer?

**A.** Yes. PCKey can be installed on a networked computer.

**Q 11.** Can I use PCKey on my networked computer and set up "permissions" for other users to access my drives or folders?

**A.** Yes. Data stored on your drive is encrypted. Once you login using your PCKey and password, you allow the data to be unencrypted on-the-fly when requested. If a remote user has permission to access an folder on your drive, the data will be decrypted for the remote user. "Share" will operate normally after PCKey installation.

**Q 12.** Can I use PCKey on a multi-user system, for example, when two or more users each log in with a different user ID?

**A.** Yes. Kensington PCKey supports more than one user on a computer. However, the PCKey password will be shared for all users. Approximately 10 unique Windows users can set up user accounts with a PCKey (user account information is stored in the PCKey.)

### Installing or Upgrading System Hardware

**Q 13.** What if I add a peripheral component to my system, replace a motherboard, change memory, or install a network card: Do I need to uninstall or reinstall Kensington PCKey when I upgrade my computer?

**A.** No. Kensington PCKey works transparently to encrypt data on a drive – even if the data relates to the changed system configuration.

**IMPORTANT!!** See information above about removing and installing hard drives.

### Creating Backups and Cloning Drives

**Q 14.** Can I make a “Ghost” or cloned image of my drive with PCKey installed? Can I clone my encrypted drive?

**A.** Yes. You can make clones of the drive, or the encrypted C:\ partition. This method of copying content does not “copy folders and files” but copies the data in a way that duplicates the entire drive at once, rather than copying and writing to another drive. The cloned drive or C:\ partition will work with Kensington PCKey the same as the original.

**Q 15.** Can I make backups of my encrypted hard drive? If I make backups of my hard drive, will the backup be encrypted? Will I need my PCKey to access my backups?

**A.** Yes, you can make backups. No, you will not need a PCKey to access the backups if you follow these guidelines.

A backup copy of a PCKey-encrypted hard drive or of selected files and folders will not be encrypted if the backup copy is written to –

- A *removable, external* or *network* hard drive, CD-RW, or tape backup system (except if the backup system you use copies partitions, not files and folders) – because PCKey encrypts only the data that is stored on internal drives that are installed in the computer when PCKey is installed.
- A drive that is installed in the computer after PCKey is installed. Drives installed after PCKey is installed are not encrypted.

**Q 16.** Can I use PCKey in a computer with a RAID controller? Will replicated hard drives be encrypted and can I use a RAID backup drive to replace my primary hard drive?

**A.** Yes. RAID controller systems make exact duplicate copies of a hard drive. A RAID copy of a hard drive that has PCKey installed should operate exactly as the original.

### Zipping Folders and Files

**Q 17.** Can I use WinZip and other “Zip” software?

**A.** Yes, you can use WinZip and other “Zip” software without limitation.

### Compressing Folders and Files

**Q 18.** Can I use Windows compression with PCKey?

**A.** Compression and encryption technologies are generally considered incompatible (see, *Preparing Your Computer for Installation*.) After you install Kensington PCKey and encrypt your disk drive, if you compress any folders using Windows compression or a third-party compression (vs. ZIP) application, you risk the corruption and permanent loss of any data that you compress. If you choose to compress any folders on an encrypted drive, KEEP A BACKUP OF ALL DATA before you compress it.

### Encrypted and un-Encrypted Files on “My Computer”

**Note:** For functionality and compatibility with Windows, certain operating system files and folders cannot be encrypted. Be aware that these folders do not have encryption protection and security.

**Q 19.** Which folders and files are encrypted by PCKey?

**A.** All folders and files on all internal hard drives that are installed when you install Kensington PCKey are encrypted, except for the folders and files:

**Q 20.** Which **files** are not encrypted during installation and normal program operation?

**A.** The following files are not encrypted by PCKey:

- desktop.ini
- index.dat
- usrclass.dat
- usrclass.dat.log
- All files in the C:\ (root) directory
- All files with the extensions of .sys, .bat, .lnk, and .manifest.
- Files listed in the file HDLBADFILES failed to encrypt during installation. (There may be none.)

**Q 21.** Which **folders** are not encrypted during installation and normal program operation?

**A.** The following folders are not encrypted by PCKey:

- C:\ Program Files and all subfolders/files
- C:\ Windows [or, the Windows installation directory] and all subfolders/files
- System Volume Information
- Recycle Bin

### Using Windows XP System Restore

**Q 22**. I have tried to use System Restore and I received an error message.

**A.** PCKey does not support System Restore. To capture a Restore Point, capture it before installing or after uninstalling PCKey. To restore a Restore Point that you made before you installed PCKey, uninstall PCKey, restore the system, and reinstall PCKey.

### Starting Windows in Safe Mode

**Q 23.** What happens if I need to start Windows in Safe Mode?

**A.** When you start Windows in Safe Mode, you need to insert your PCKey and use your PCKey password to logon. You should not use any applications or access any files while in Safe Mode with PCKey installed, however, you can use Safe Mode to install or reinstall any drivers or files, or to make other changes required to allow Windows to work in normal mode.