

User's Guide



Version 1.4

Information in this document is subject to change without notice and does not represent a commitment on the part of Information Security Corporation. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use without the prior written permission of Information Security Corporation.

SpyProof! software is commercial computer software and, together with any related documentation, is subject to the restrictions on U.S. Government use as set forth below.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 52.227-7013. "Contractor/manufacturer" is Information Security Corporation, 1141 Lake Cook Road Suite D, Deerfield, IL 60015-9461.

The U.S. International Traffic in Arms Regulations (ITARs) (22 CFR 125.03) prohibits the dissemination of certain types of technical data to foreign nationals.

Protected by U.S. Patents No. 5,274,707 and 5,373,560.

All trademarks and/or registered trademarks are the properties of their respective owners.

SpyProof! and SecretAgent are registered trademarks of Information Security Corporation.

Copyright © 1991-2007 Information Security Corporation. All rights reserved.
Printed in U.S.A., SpyProof!, sixth edition (February 2007)

Information Security Corporation

1141 Lake Cook Road, Suite D
Deerfield, IL 60015-9461

Product Information: 800-203-5563
Technical Support: 708-445-9415
Internet Support: tech@infoseccorp.com

R E G I S T R A T I O N

Register *SpyProof!* now through our website, by fax or by mail. All we need is your name, address, phone number, serial number and date of purchase. You will be added to the list of registered *SpyProof!* licensees and be eligible to receive free technical support and product update notifications for one year (maintenance fees are required for product support after year one).

To Register On-line:

- ◆ Visit the Information Security Corporation website at <http://www.infosecorp.com/support/register.htm>.

To Register By Fax:

- ◆ Fill out the registration form below and fax it to us at: (847) 405-0506.

To Register By Mail:

- ◆ Fill out the form below and mail it to us at:
Information Security Corporation
1141 Lake Cook Road, Suite D
Deerfield, IL 60015-9461

Please add my name to your list of *SpyProof!* registered licensees.

Company/Organization Name

Name

Address

City

State

Zip

Daytime Phone

Purchase Date

Serial # _____

TECHNICAL SUPPORT

Information Security Corporation provides technical support for SpyProof! as follows:

For Technical Support

Hours: 8:30 a.m. to 5:00 p.m. Central Time

Voice: (708) 445-9415

Fax: (847) 405-0506

Web: <http://www.infosecorp.com/support/contents.htm>

E-mail: tech@infosecorp.com

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	6
USING THIS GUIDE.....	6
CONVENTIONS USED IN THIS GUIDE.....	6
<i>Print Conventions</i>	6
<i>Command Terminology</i>	6
<i>Mouse Conventions</i>	7
IMPORTANT INFORMATION	7
CHAPTER 2: INSTALLATION.....	8
SYSTEM REQUIREMENTS	8
<i>System Software</i>	8
<i>Hardware Requirements</i>	8
INSTALLING SPYPROOF!.....	9
CHAPTER 3: QUICK START	13
SPYPROOF! AND SECRETAGENT	14
GETTING A CERTIFICATE.....	14
STARTING SPYPROOF! FOR THE FIRST TIME	22
CREATING A SPYPROOF! DISK	24
MOUNTING A SPYPROOF! DISK	26
UNMOUNTING SPYPROOF! DISKS	26
REMOVING A SPYPROOF! DISK	28
EXPANDING A SPYPROOF! DISK	29
TRANSFERRING A SPYPROOF! DISK	30
EXITING SPYPROOF!	31
SHARING SPYPROOF! DISKS	32
<i>Viewing and changing recipients for a SpyProof! disk</i>	32
<i>Importing a SpyProof! disk</i>	35
<i>Exporting a SpyProof! disk</i>	36
THE DISK MANAGER	37
<i>Making disks mount automatically</i>	37
<i>Assigning drive letters to disks</i>	37
<i>Change the profile used to mount a disk</i>	37
ADDITIONAL TOOLS.....	38
<i>Configuring the Unmount All HotKey</i>	38
<i>Recovering Incompletely Rekeyed Disks</i>	38
COMMAND LINE FUNCTIONALITY	39
GLOSSARY	41

Chapter 1: Introduction

Overview

SpyProof! creates encrypted virtual partitions that allow users to secure files on their systems in an easy to use and transparent manner. Applying the latest Federal and industry standards in cryptographic technology, SpyProof! ensures the confidentiality of your data. SpyProof! is intuitive and user-friendly, providing transparent disk encryption through an easy to use system tray application.

Using this Guide

This guide is designed to assist you in effectively using SpyProof!. The User's Guide for SpyProof! is organized as follows:

Chapter 1, Introduction

The first chapter provides an overview of the organization and contents of this guide and presents the style conventions used throughout the guide.

Chapter 2, Installation

The second chapter provides the system software and hardware requirements, and instructions for installing SpyProof!.

Chapter 3, Quick Start

The third chapter presents the key steps needed to begin working with SpyProof!.

Glossary

The glossary provides a list of terms that are common in the world of cryptography and public key infrastructure but which may be unfamiliar to people new to the field.

Conventions Used in this Guide

This User's Guide consistently employs certain formatting and language conventions to assist you in learning how to use SpyProof!.

Print Conventions

The following conventions are used throughout this guide for screen displays, command entries, and keyboard characters:

- ◆ Window titles, menu names, and dialog names are printed in **bold type** and match those in the application. For example: Click the **Create** button.
- ◆ Actions requiring key combinations are joined with a plus sign, *e.g.*, **<Ctrl + P>**. To execute this type of action, press and hold the first key, then press the second key and release both keys.

Command Terminology

The following terminology is used consistently in describing individual or multi-step actions.

- ◆ *Select* refers to making a choice from a menu or list of options in a dialog box. For example, "select the **Drive Letter** to use from the drop down list" means that you must select this option by clicking on it with the mouse.

- ◆ Steps that involve making two or more successive selections are often presented in combination. For example, when you read “Select **Mount | Disk name** from the system tray menu” click the system tray icon, then select **Mount** and the **disk name** to mount from the menu.

Mouse Conventions

The assumption throughout this User’s Guide is that your left mouse button is configured as the Windows primary mouse button and that the right button is the secondary button. (You may, of course, choose to reverse the roles of these buttons using Windows’ Mouse Control Panel.) The following terminology regarding mouse usage is employed throughout this manual:

- ◆ *Click* means to position the mouse cursor over an object and then to press and immediately release the primary button without moving the mouse.
- ◆ *Double-click* means to position the mouse cursor over an object and then to press and immediately release the primary button twice in quick succession.
- ◆ *Drag* means to position the mouse cursor over an object (the source of the drag operation) and then to press and hold the primary button while moving the cursor to a new location. Once the cursor has reached its destination, release the mouse button to “drop” the object onto the target.

Important Information

Before installing or using SpyProof! for the first time, please review the README.TXT file that may be included on the distribution media you received. This file may contain information that supersedes the information printed in this manual.

For current product information, visit Information Security Corporation’s website at:
<http://www.infosecorp.com>.

Chapter 2: Installation

Overview

This chapter provides the basic information you'll need to install SpyProof! on your computer.

This chapter covers:

- ◆ System Requirements
- ◆ Installing SpyProof!

System Requirements

System Software

SpyProof! for Windows requires Microsoft Windows NT 4.0, 2000, or XP. To use some of the user interface elements described below, you will also need to have Microsoft Internet Explorer 4.0 or higher installed on your system, though SpyProof! will run without it.

Hardware Requirements

SpyProof! operates on any PC-compatible computer with an Intel Pentium II-class processor or equivalent. The minimum hardware requirements are:

- ◆ 20MB of free hard disk space
- ◆ 64MB RAM
- ◆ Super VGA or better monitor (800 x 600 resolution or higher is recommended)
- ◆ Mouse and keyboard
- ◆ CD-ROM drive (unless you're performing a network install)

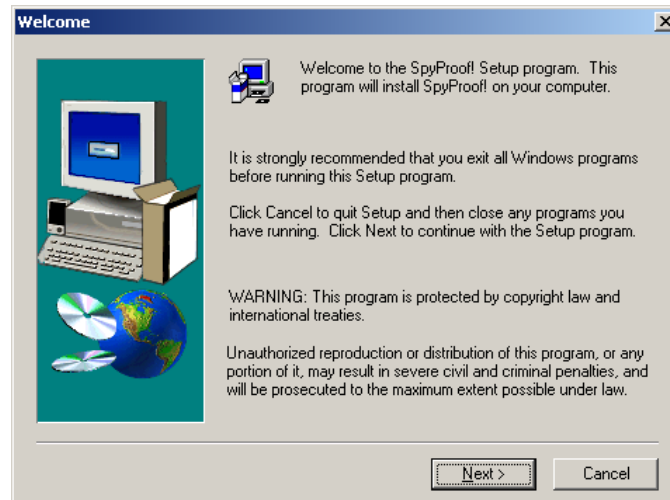
Installing SpyProof!

This section explains how to use the SpyProof! Setup Program to install SpyProof! on a stand-alone computer from the CD-ROM distribution media. (If you are installing from a network server, the SpyProof! CD-ROM may not be required; consult your system administrator for instructions.)

⇒ To install SpyProof!:

1. Insert the SpyProof! disc into your CD-ROM drive.

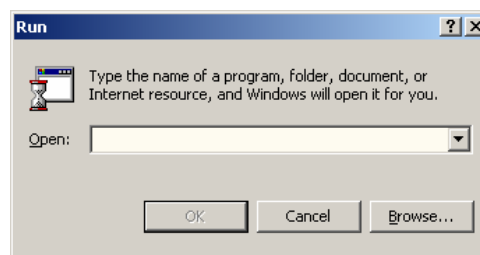
If the SpyProof! **Welcome** window appears automatically continue to step 4.



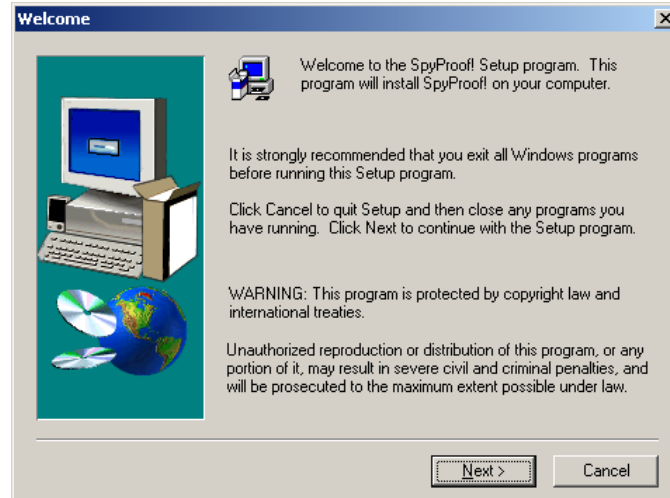
If the SpyProof! **Welcome** window does not start automatically proceed to step 2.

Note: Please read all of the information in each dialog before advancing to the next step.

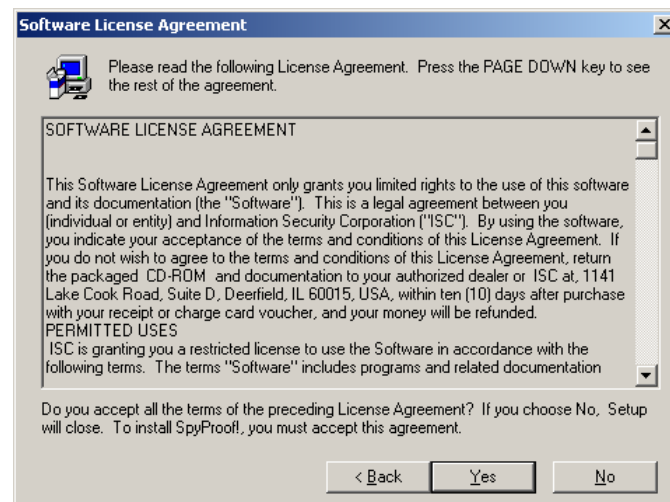
2. Since the SpyProof! Setup Program did not start automatically; from the **Start** menu, select **Run** to display the **Run** dialog.



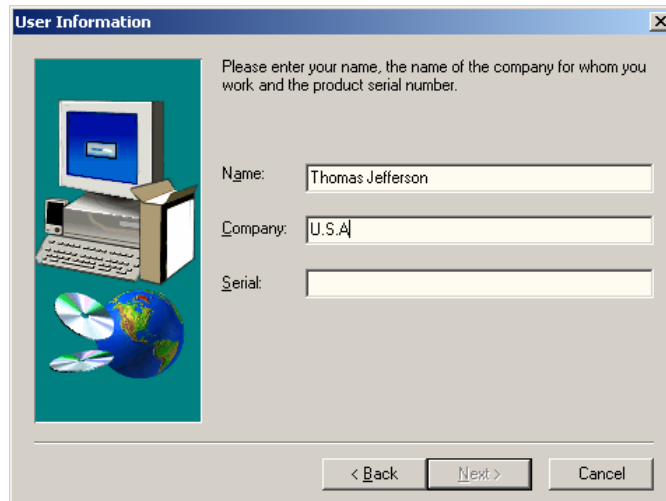
3. Type **D:\setup.exe** in the **Run** dialog's Open field and click **OK** to start the Setup Program. Be sure to substitute an appropriate drive letter if your CD-ROM drive is not D. The **SpyProof!** window appears.
4. Follow the onscreen prompts provided by the installation wizard clicking **Next**, **Yes**, or **Finish** as required. Click **Next** on the **Welcome** dialog to display the **SpyProof! Software License Agreement** dialog.



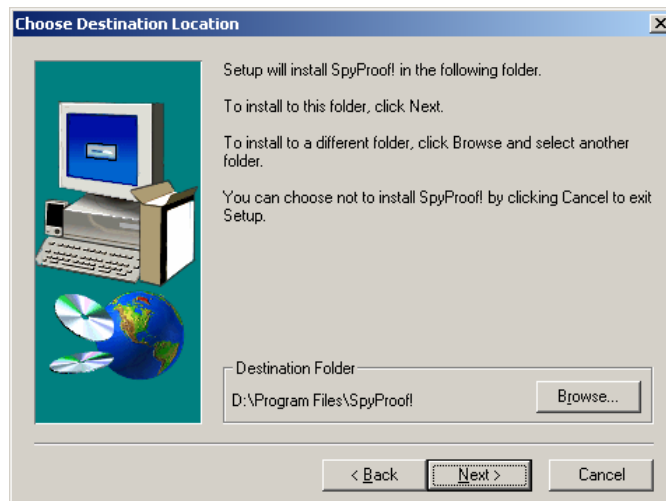
5. Carefully read the software license agreement and, if you agree to the license agreement, press **Yes** to continue the installation and display the **User Information** dialog.



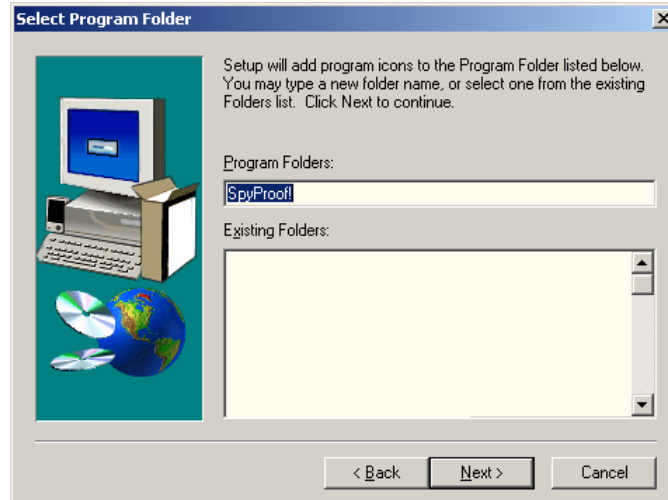
6. Enter your name, your company's name, the serial number located on the CD sleeve, and press **Next** to display the **Choose Destination** dialog.



7. Decide where you want SpyProof! to install. You can leave the destination folder as is or use the **Browse** button to choose a different location. Once you have selected a destination folder press the **Next** button to display the **Select Program Folder** dialog.



8. The **Select Program Folder** dialog enables you to determine where the SpyProof! icons are placed on your **Start** menu. Pressing the **Next** button starts the file transfer process.



9. After the SpyProof! files are transferred to your computer you may be prompted to let SpyProof! configure Windows to clear the pagefile during system shutdown. Enabling this feature will ensure that no secure data placed in the pagefile during system use is left in the clear. Choosing this option may significantly increase the time required to shut your machine down but provides a greater level of security.
10. You will be prompted to choose if you want SpyProof! to start automatically when Windows starts. This option affects all user profiles on the machine. When a user logs in SpyProof! will automatically start and mount any drives marked as automount disks.
11. The **Setup Complete** dialog may inform you that the setup program needs to restart your machine in order to complete the installation process. If this is the case you should choose **Yes, I want to restart my computer now** in order to complete the installation. SpyProof! will not function properly unless you restart the machine as requested. If you select **No, I will restart my computer later** you will have to manually restart your computer before using SpyProof!.



12. SpyProof! is now installed. Proceed to Chapter 3: *Quick Start*.

Chapter 3: Quick Start

Overview

This chapter provides the basic information you need to configure and begin working with SpyProof!. It is intended for first-time users of the product and provides a quick overview of SpyProof!'s functions. This chapter assumes you have completed the installation of SpyProof! (see Chapter 2: *Installation*). We explain how to start SpyProof!, how to configure SpyProof, how to create and use SpyProof! disks, and how to exit SpyProof!.

This chapter covers:

- ◆ SpyProof! and SecretAgent
- ◆ Getting a Certificate
- ◆ Starting SpyProof!
- ◆ Creating a SpyProof! disk
- ◆ Mounting a SpyProof! disk
- ◆ Unmounting a SpyProof! disk
- ◆ Removing a SpyProof! disk
- ◆ Expanding a SpyProof! disk
- ◆ Transferring a SpyProof! disk
- ◆ Exiting SpyProof!
- ◆ Sharing SpyProof! disks
 - ◆ Viewing/Changing SpyProof! disk recipients
 - ◆ Importing a SpyProof! disk
 - ◆ Exporting a SpyProof! disk
- ◆ The Disk Manager
- ◆ Additional Tools
 - ◆ HotKey Unmount All
 - ◆ Disk Recovery
- ◆ Command Line Functionality

SpyProof! and SecretAgent

SpyProof! operates differently if SecretAgent is installed. If SecretAgent is installed SpyProof! makes use of SecretAgent's profiles and certificate stores. For this reason SecretAgent should be configured before SpyProof! is used (this also applies if you install SecretAgent after using SpyProof! in standalone mode). Please refer to the SecretAgent documentation for information on Getting a Certificate and creating a profile. This document assumes you are using SpyProof! in its standalone mode, and will note any differences as it goes along.

Getting a Certificate

SpyProof! requires that you have a key pair (a certificate and a private key) in your local CAPI store that is capable of encryption or key exchange. Purchasing SpyProof! entitles you to receive one renewable X.509v3 certificate issued by ISC. You can enroll for your certificate by going to the following webpage using Internet Explorer:

<http://www.infosecorp.com/ca/silver/contents.htm>

Once there do the following:

1. After reading the Relying Party Agreement, choose the link to enroll using a new key pair generated by your browser.

The screenshot shows a web browser window titled "CertAgent™ Certificate Request Form - Microsoft Internet Explorer". The address bar shows the URL "http://ca1.infosecorp.com/certagent/public/crq.jsp?issuer=iscsilver". The page content includes a navigation menu with links for "Main Menu", "CA Information", "Issued Certificates", "Enrollment", "Pick Up", and "Help". The main heading is "Request a browser certificate from: ISC Silver Subscriber CA". Below this is a brief instruction: "Complete the following certificate enrollment form and click Submit. A certificate request will be created in your CAPI store and submitted to the specified CA. Provide your e-mail address if you want it included in your certificate or if you wish to be notified when your request has been processed." The form is divided into two sections: "User Information" and "Key Generation Options".

User Information:

Name: * Thomas Jefferson
Title: President
Organizational Unit: www.infosecorp.com/ca/silver
Country: US
E-Mail Address: * n@whitehouse.gov Include in certificate.

Key Generation Options:

CSP: * Microsoft Enhanced Cryptographic Provider v1.0
Key Usage: * Encrypt Sign Both
Key Size: * 2048
 Enable strong private key protection
If you check this box, you will be prompted to set a CAPI security level for your private key.
 Mark keys as exportable
Check this box if you might want to extract your private key from CAPI.
 Use local machine store
Check this box if you are requesting an IPsec local computer certificate. You must have administrative rights on your system to successfully generate a key in the local machine store.

Submit

Terms of Use

Information Security CORPORATION

2. Fill out the form with your information and click **Submit**. You will be provided with online instructions detailing how to pick up and install your certificate into your local CAPI store. Once you have your certificate installed you are ready to begin using SpyProof!. Skip the rest of this section and proceed to the section **Starting SpyProof! for the First Time**.

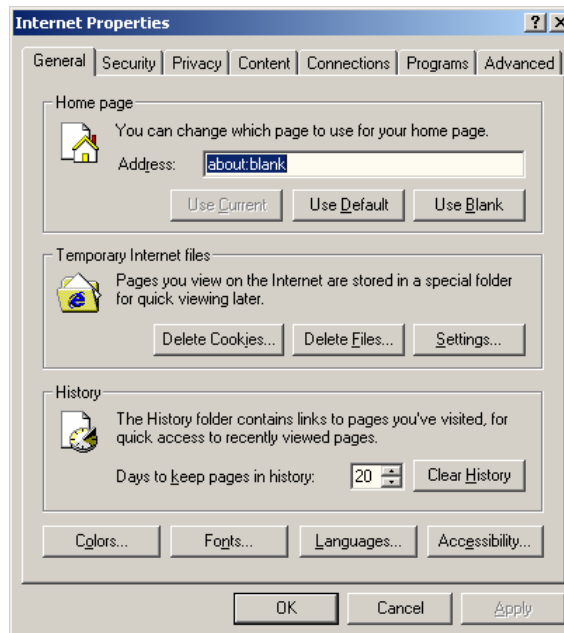
Alternatively, you may either import an existing key pair from a PKCS #12 format file or request a new key pair using Internet Explorer and your CA. If you are using a smart card please see your smart card documentation for getting a key pair onto your smart card.

Note: If you are using SpyProof! in conjunction with SecretAgent please see SecretAgent's documentation for instructions on getting a certificate.

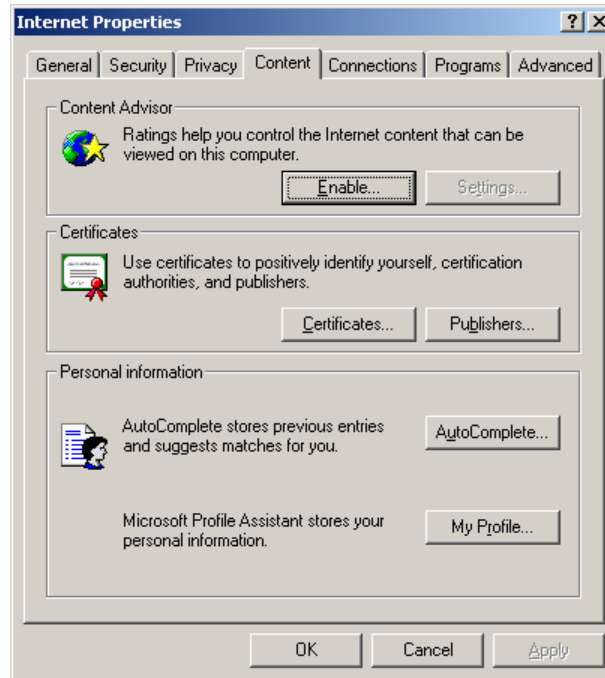
Note: If you do not use strong private key protection with a security level of high or use a smart card your data will not be secure as CAPI will only use the fact that you are logged on to allow access to your private key. Since your logon username and password can be determined using various programs freely available on the Internet it is highly recommended that you enable strong private key protection with a security level of high. This does not apply when using SpyProof! with SecretAgent installed.

⇒ **To Import a PKCS #12 file:**

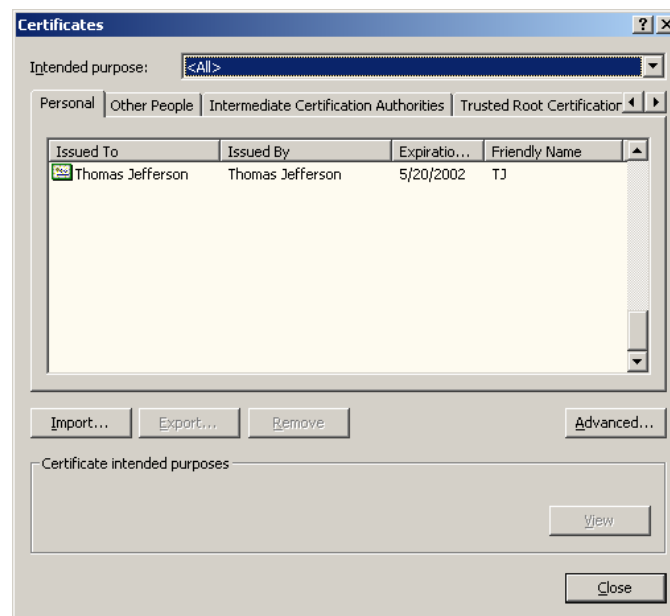
1. Use the secondary mouse button to click the Internet Explorer icon on the Windows desktop to display the **Internet Properties** dialog.



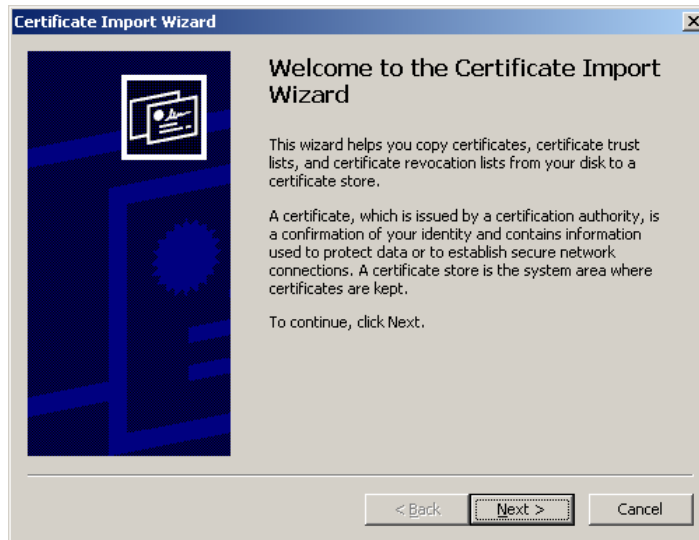
2. Select the **Content** tab.



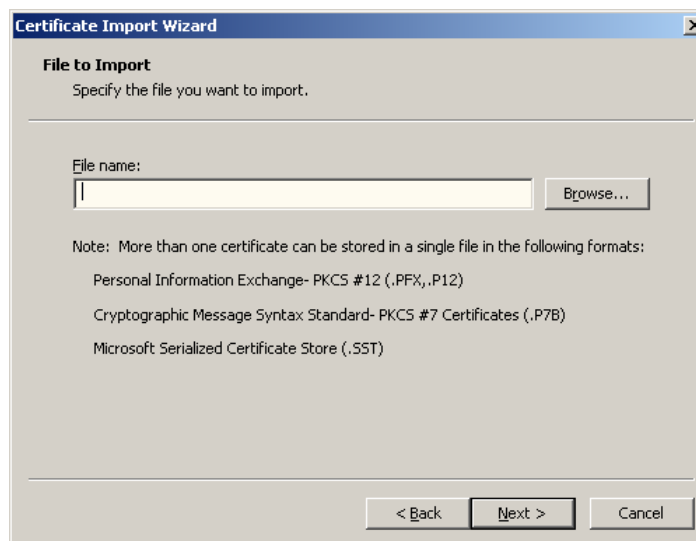
3. Click the **Certificates** button to display **Certificates** dialog.



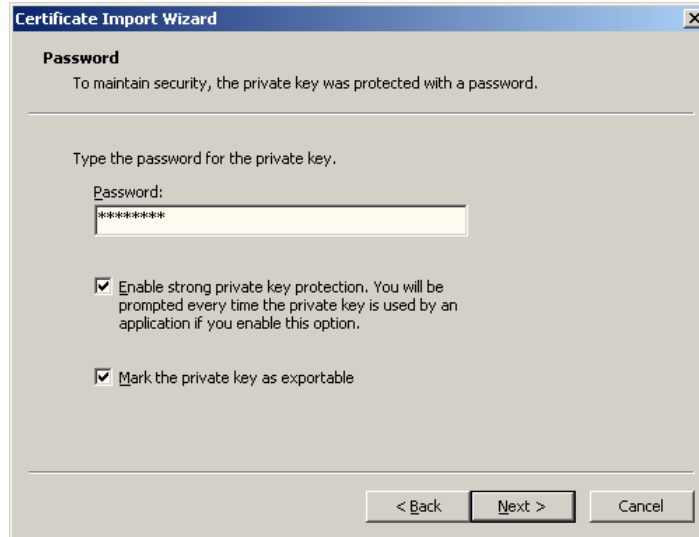
4. Click the **Import** button to display the **Certificate Import Wizard**.



5. Click **Next** to display the **File to Import** wizard page.

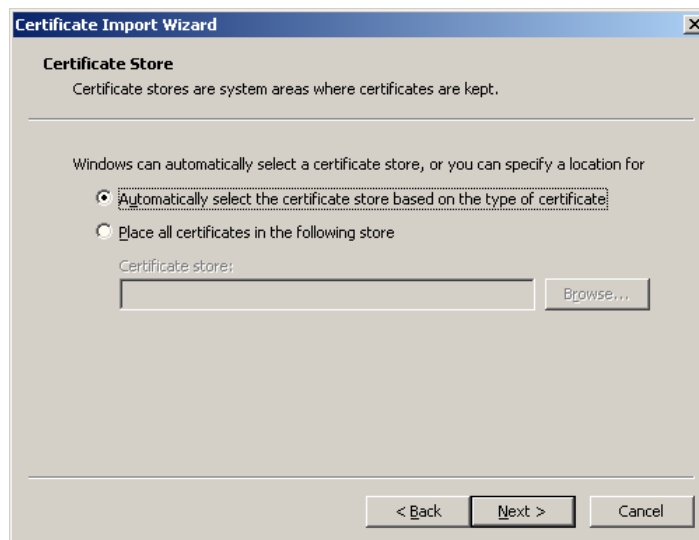


6. Use the **Browse** button to select the file to import. Then click **Next** to display the **Password** dialog.

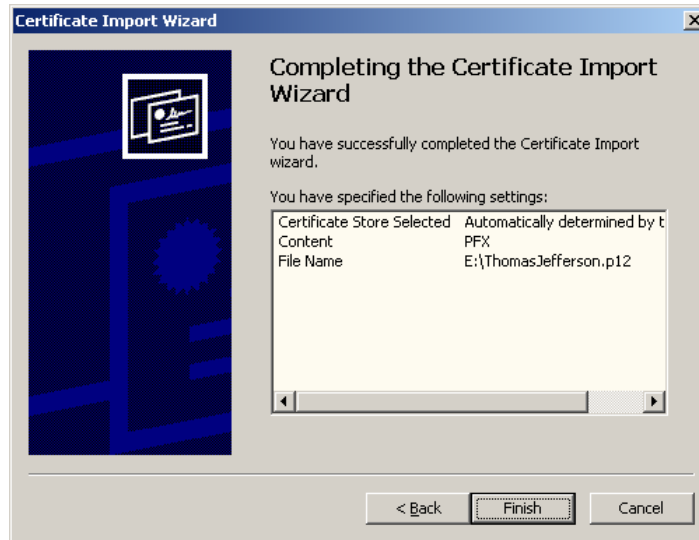


7. Make sure to check both the **Enable strong private key protection** and the **Mark the private key as exportable** check boxes. Click **Next** to display the **Certificate Store** dialog.

Note: this only applies to users who are not using smart cards.



8. Click **Next** to display the **Completing the Certificate Import Wizard** dialog.



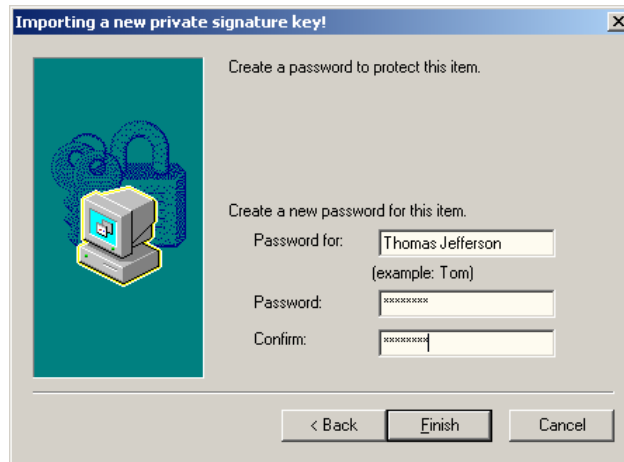
9. Click **Finish** to display the **creating a Protected item** dialog.



10. Click the **Set Security Level** button to display the **Security Level Selection** dialog.



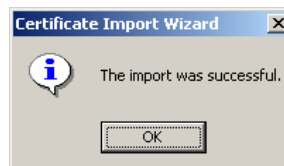
11. Select **High** to password protect your private key and then click **Next** to display the **Create Password** dialog.



12. Enter an identifier in the **Password for:** box and then enter a new password in both the **Password:** and the **Confirm:** boxes. Then click the **Finish** button to return to the **creating a Protected item** dialog.



13. Click **OK** to finish importing your key pair and display the **The import was successful** dialog.



14. Click **OK**.
15. You have now imported a PKCS #12 key pair into Microsoft's CAPI please proceed to the **Starting SpyProof!** section.

⇒ **To request a new certificate from a CA using Internet Explorer:**

1. Double-click the Internet Explorer icon on the Windows desktop to launch Internet Explorer.
2. Enter the web address of your Certificate Authority and press **Enter**. Please contact your Certificate Authority for this information.
3. Follow the instructions supplied by your Certificate Authority for getting a key pair making sure to check any box labeled **Enable strong private key protection** and following steps 9-12 of the Importing PKCS #12 section to password protect the private key you are creating.

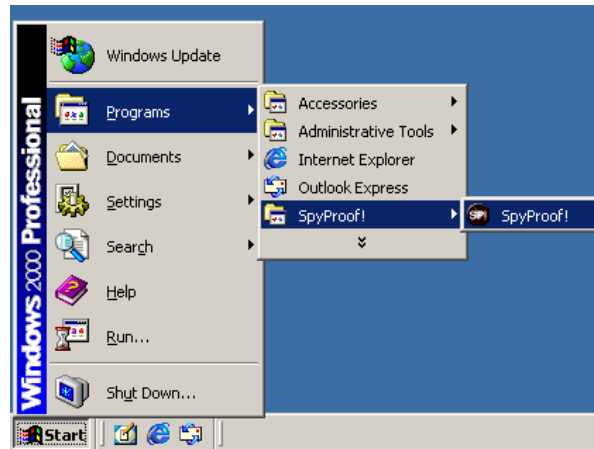
Note: this only applies to users who are not using smart cards.

Starting SpyProof! for the First Time

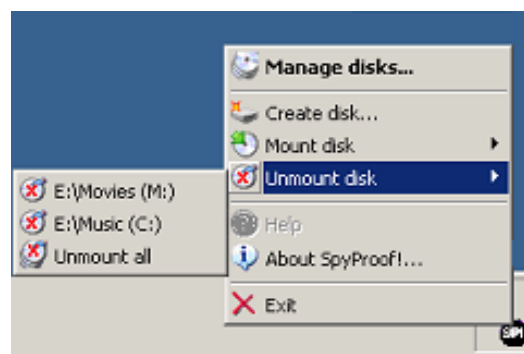
Once you have a certificate and private key you can start SpyProof! as follows.

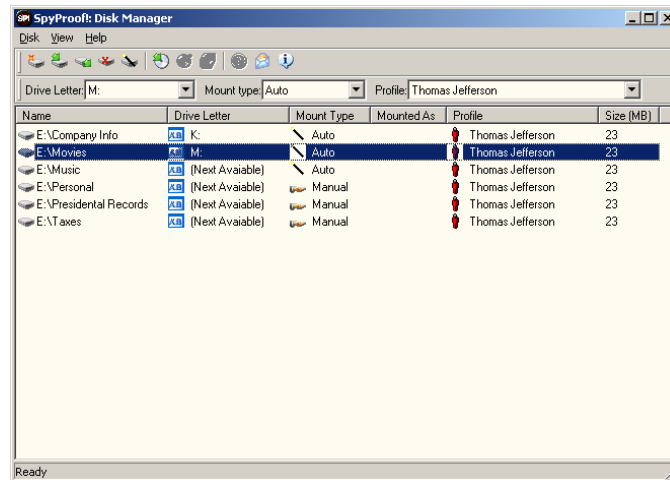
⇒ **To start SpyProof!:**

1. Click the Windows **Start** button to display the Start menu:
2. Select **Programs | SpyProof! | SpyProof!** to start the program.



3. The SpyProof! splash screen will display and the SpyProof! system tray icon will appear in your Windows system tray (the location of the clock and volume control icons usually in the lower right hand corner of your screen).
4. To access SpyProof!'s functionality click on the icon with the secondary mouse button to display the SpyProof! menu or double-click the icon with the primary button to display the **Disk Manager** dialog.





5. From either the menu or the **Disk Manager** you can create, mount, or unmount disks. The **Disk Manager** also lets you mark disks as auto mountable, import disks, export disks, remove disks, change recipients, assign a different profile to a disk, assign specific drive letters to disks, and more.

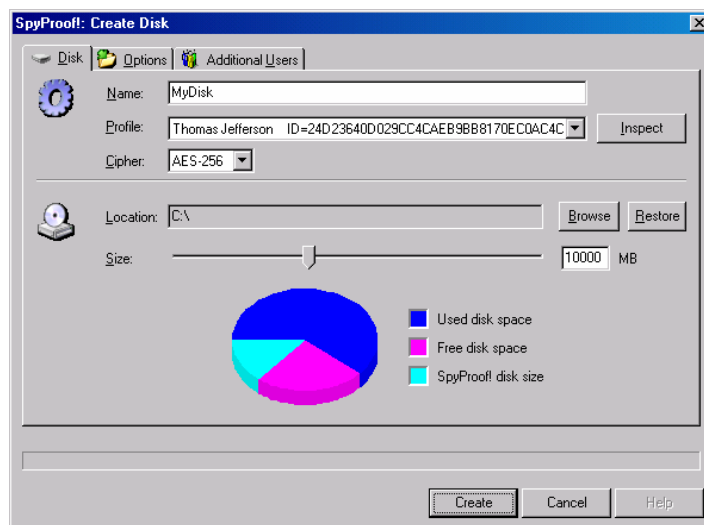
Creating a SpyProof! disk

SpyProof! lets you create disks usable by the selected profile and any additional users you choose to add. Additional users are other people who may mount and use the disk. This is a useful feature when sharing the disk among a small group or when distributing disks to many people (possibly using only a single key pair that they all have) securely on CD or other media.

Follow these steps to create a SpyProof! disk.

⇒ To create a SpyProof! disk:

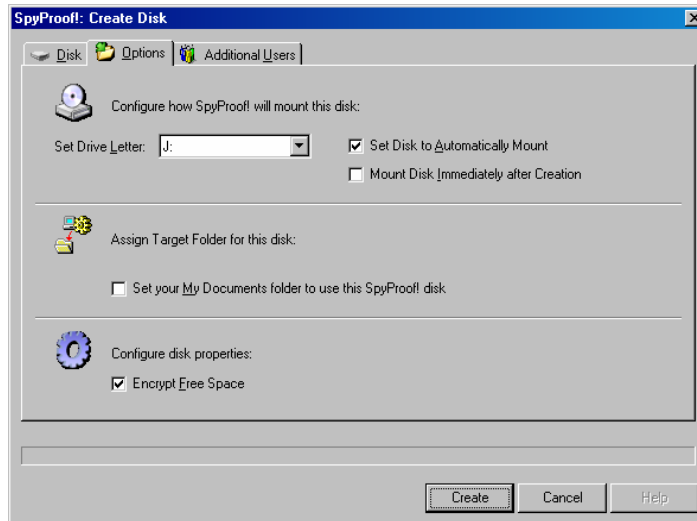
1. To access SpyProof!'s create disk functionality, click on the system tray icon with the secondary mouse button to display the SpyProof! menu and select **Create disk...** or if you are in the **Disk Manager** either select **Create...** from the **Disk** menu or use the keyboard combination <Alt + D, C> to display the **Create Disk** dialog.



2. On the Disk tab of the **Create Disk** dialog enter the **Name** of the disk, select the **Profile** that uses the disk, select the **Cipher** (bigger equals greater security) to use to secure the disk, select a **Location** to store the file that contains your encrypted disk using the **Browse** button, and select the size of your disk by moving the slider.

Note: If using SecretAgent, you will see a check box on this first tab that, when checked, will cause SpyProof! to display the names of encrypt-capable SecretAgent Profiles in the **Profile** drop-down. When unchecked, SpyProof! will instead display the names of your personal CAPI certificates.

3. (Optional) On the Options tab, you can specify mounting options such as specifying a drive letter, setting the disk to automount, mounting the disk after creation, assigning the target of your My Documents folder to this disk, and encrypting free space.



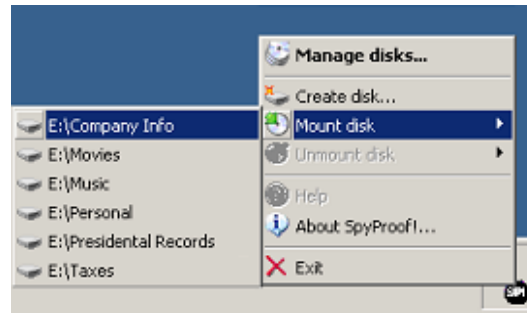
4. (Optional) On the Additional Users tab, you can specify additional recipients if you want to share this disk with others.
5. After you have configured the necessary options, click the **Create** button.
6. The progress meter will move from left to right indicating the progress of disk creation. Depending on the size of your disk, your processor speed and your hard disk performance this may take between 1 second and 1 or more hours of time to complete.
7. Once the disk is created the **Create Disk** dialog will disappear. If it is not already mounted, you may mount your disk by following the instructions in the **Mounting a SpyProof! disk** section.

Mounting a SpyProof! disk

Follow these steps to mount a SpyProof! disk.

⇒ **To mount a SpyProof! disk:**

1. To mount a SpyProof! disk click on the system tray icon with the secondary mouse button to display the SpyProof! menu and select **Mount disk** to display the list of disks you may mount. If you are in the **Disk Manager** select the disk to mount and then either select **Mount** from the **Disk** menu or use the keyboard combination <Alt + D, M> to mount a disk.



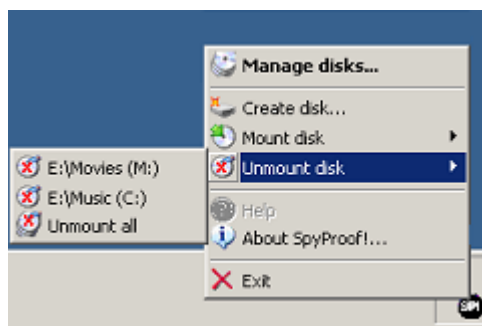
2. You may be prompted to enter your password and then the disk will mount at either the drive letter specified in the **Disk Manager** or at the first available drive letter that is unused.

Unmounting SpyProof! disks

Follow these steps to unmount a SpyProof! disk.

⇒ **To unmount a SpyProof! disk:**

1. To unmount a SpyProof! disk click on the system tray icon with the secondary mouse button to display the SpyProof! menu and select **Unmount disk** to display the list of disks you may unmount. If you are in the **Disk Manager** select the disk to unmount then either select **Unmount** from the **Disk** menu or use the keyboard combination <Alt + D, U> to unmount the disk.



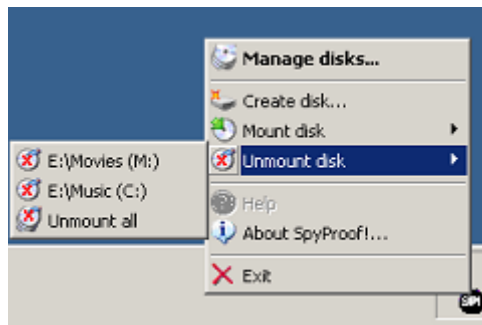
2. You may be warned that the disk is in use. In this case you can elect to leave the disk mounted and attempt to exit any programs using the disk (this would include Windows Explorer) and then unmount the disk again or you may force SpyProof! to unmount the disk risking possible data loss or poor behavior in some programs.

Follow these steps to unmount all SpyProof! disks.

⇒ **To unmount all SpyProof! disks:**

1. To unmount all mounted SpyProof! disks click on the system tray icon with the secondary mouse button to display the SpyProof! menu, select **Unmount disk | Unmount All**. If you are in the **Disk Manager** either select **Unmount all** from the **Disk** menu or use the keyboard combination <Alt + D, N>.

Note: You can also specify a hotkey to silently dismount all SpyProof! disks using the **Configure HotKeys** dialog as described later in this manual.



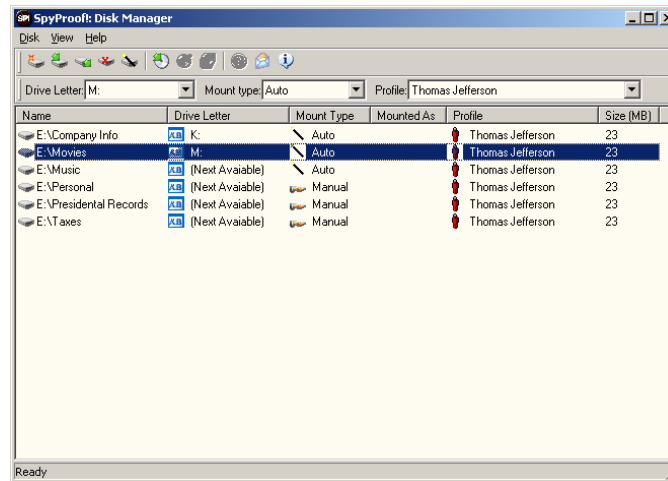
2. You will be warned that unmounting all disks may cause data loss. Click **Yes** to unmount all disks.

Removing a SpyProof! disk

Follow these steps to remove a SpyProof! disk.

⇒ **To remove a SpyProof! disk:**

1. To remove a SpyProof! disk double click on the system tray icon to display the **SpyProof! Disk Manager**. Select the disk to remove then either select **Remove** from the **Disk** menu or use the keyboard combination **<Alt + D, R>** to remove the disk.



2. When prompted to remove the disk select **Yes**.
3. When prompted to remove the files making up the disk select **Yes** if you really want to delete the encrypted disk. If you may want to import the disk at a later time or have another reason for keeping the disk's actual data around select **No**.

Expanding a SpyProof! disk

Follow these steps to expand a SpyProof! disk.

⇒ To expand a SpyProof! disk:

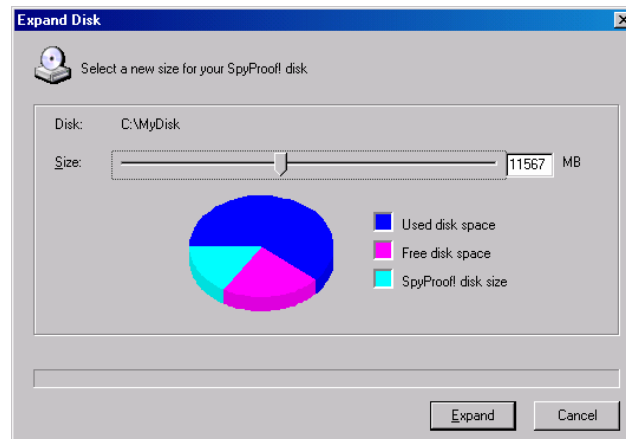
1. To expand a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**. Select the disk to expand then either select **Expand** from the **Disk** menu or use the keyboard combination **<Alt + D, X>** to expand the disk.

Note: Disks created using SpyProof! 1.2 or later are formatted using NTFS. Disks created using versions prior to release 1.2 formatted using FAT12, FAT16, or FAT32. These legacy disks cannot be expanded unless they are first converted to NTFS. To convert a FAT formatted disk to NTFS do the following:

1. Mount the SpyProof! disk you want to expand.
2. Open a command prompt window and enter:

```
convert drive_letter: /fs:ntfs
```

where *drive_letter* is the letter the drive is mounted as.



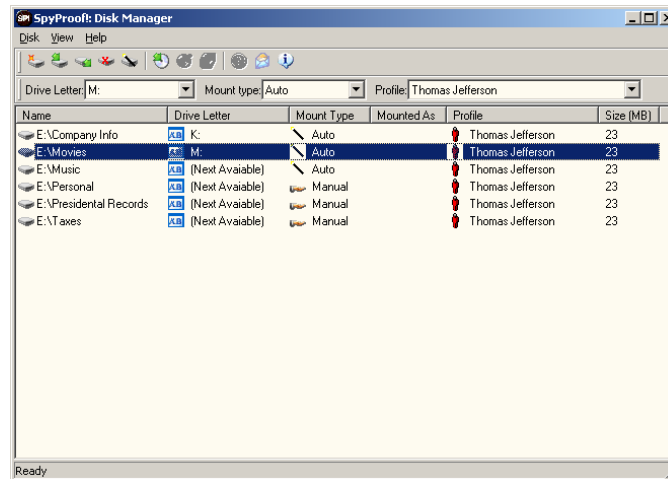
2. In the **Expand Disk** dialog, select a new size for your disk by moving the slider. Then click **Expand**.
3. You may be prompted to enter your password and then the disk will begin expanding. Depending on how much larger you are making the disk, this may take some time. After it has completed you will be returned to the **Disk Manager**.

Transferring a SpyProof! disk

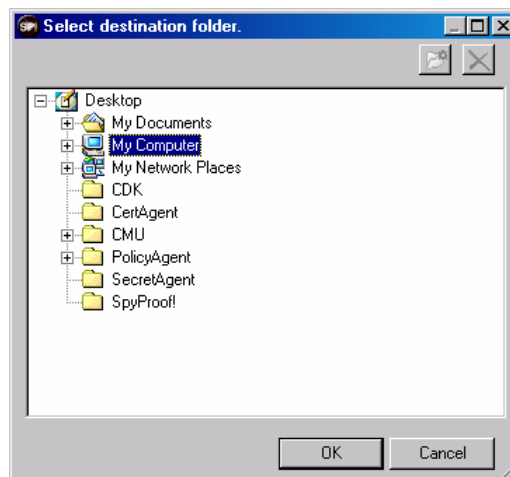
Follow these steps to change where SpyProof! stores the underlying files for a particular SpyProof! disk. This may help you if you are running out of disk space on the drive where the files are currently stored or otherwise help you manage your disks.

⇒ To transfer a SpyProof! disk:

1. To transfer a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**, then either select **Transfer** from the **Disk** menu or use the keyboard combination <Alt + D, T> to start the transfer process.



2. Select the new location for the disk's files in the **Select destination folder** dialog and click **OK**.



3. SpyProof! will move the disk's .spd and .spk files to the location you specified and update the Disk Manager screen to display the new location. This may take some time depending on the size of your disk.

Exiting SpyProof!

When you exit SpyProof! all mounted disks will automatically unmount which may affect running applications using SpyProof! disks.

Follow these steps to exit SpyProof!

⇒ **To exit from SpyProof!:**

1. To exit SpyProof! click on the system tray icon with the secondary mouse button to display the SpyProof! menu and select **Exit**.
2. If you have disks mounted you will be asked if you really want to exit. Select **Yes** to exit SpyProof! or **No** to leave your disks mounted and continue using SpyProof!.

Sharing SpyProof! disks

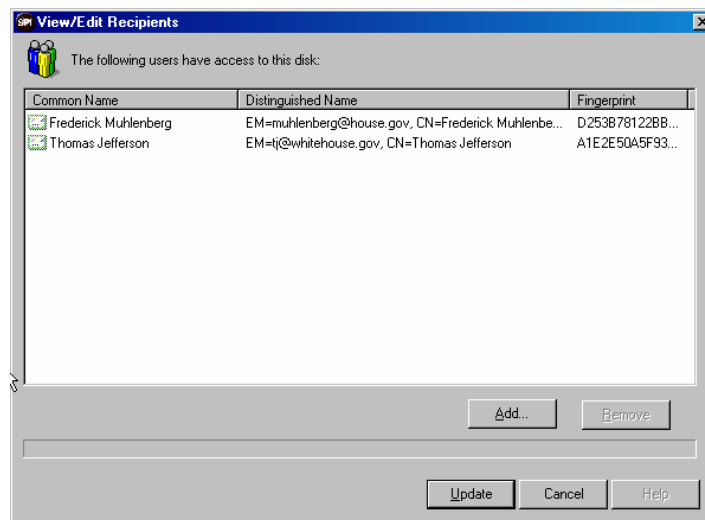
SpyProof! lets you share disks by including additional users when you create the disk, changing additional users after the disk is created, letting you mount disks stored on network drives, and letting you import and export disks. SpyProof!'s export disk process also allows you to easily backup critical data. Once you have created a disk and placed data in it you can export it to a floppy, removable hard drive, compact flash, CDR, and many other portable devices for secure distribution.

Viewing and changing recipients for a SpyProof! disk

Follow these steps to view and change the additional recipients for a SpyProof! disk.

⇒ To view the recipients for a SpyProof! disk:

1. To view a SpyProof! disk's recipients double click on the system tray icon to display the SpyProof! **Disk Manager**, then select the disk you want to view or modify, then either select **View/Edit Recipients** from the **Disk** menu or use the keyboard combination <Alt + D, V> to view the current recipients.

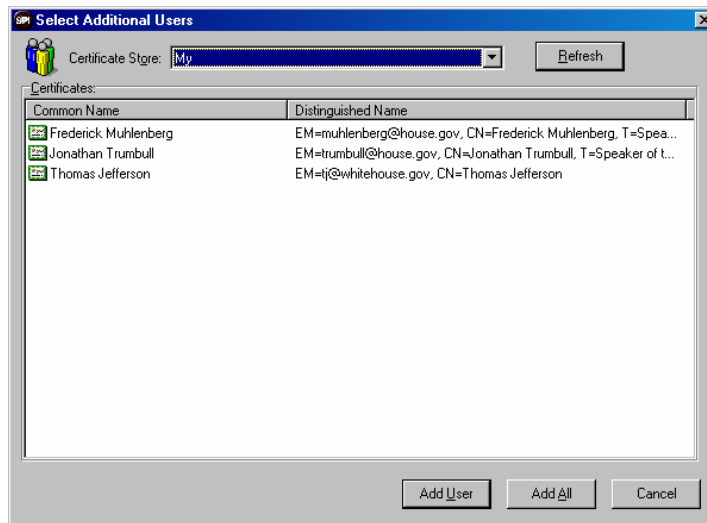


2. The icon to the left of each recipient provides information about the status of the certificate. A faded certificate icon indicates the user is currently a recipient and the certificate is valid. A red 'x' icon indicates the user is currently a recipient but the certificate is not valid (you will not be able to update the recipients to the disk unless you remove such certificates from the list.) An icon showing two people with a key indicates that your administrator has configured the certificate to be used for key recovery (you will not be able to remove such certificates from the list.)
3. If you are done viewing the recipients and do not want to modify the list you can click **Cancel** to return to the **Disk Manager**. If you want to add recipients, follow the instructions in the next section, **Adding Recipients to a SpyProof! disk**. If you want to remove recipients, follow the instructions in the next section, **Removing Recipients from a SpyProof! disk**.

⇒ Adding recipients to a SpyProof! disk:

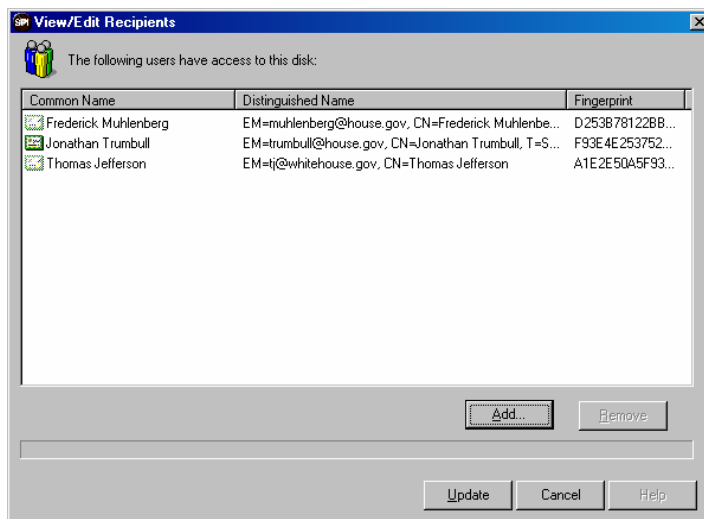
1. To add recipients to a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**, then select the disk you want to view or modify, then either select **View/Edit Recipients** from the **Disk** menu or use the keyboard combination <Alt + D, V> to view the current recipients.

- From the **View/Edit Recipients** dialog, you can both add and remove recipients to the disk. To add recipients click the **Add** button. This will display the **Select Additional Users** dialog.



- You can select recipients by first choosing a Certificate Store. Then select the new intended recipient from the list and click **Add User**. You will return to the **View/Edit Recipients** dialog. A clear certificate icon is used to indicate the new recipient.

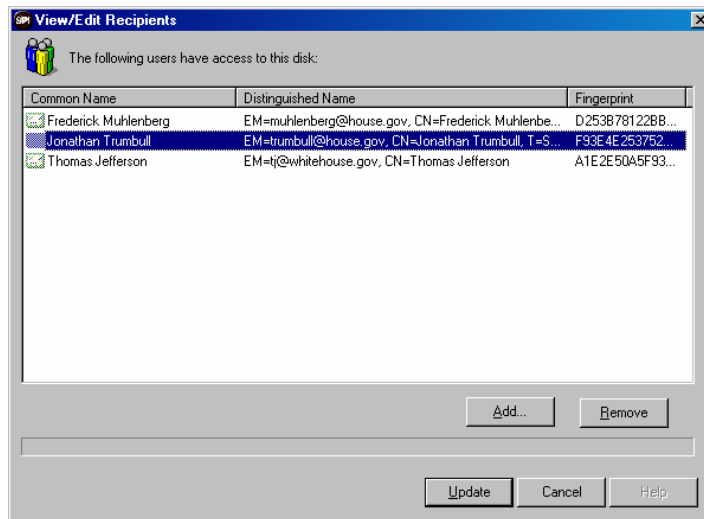
Note: If using SecretAgent, the available certificate stores are those configured in SecretAgent's Certificate Explorer (including any LDAP queries and CAPI connections.) Also, any certificates selected will be verified before being added (a dialog will be displayed indicating the problems with any invalid certificates if applicable.) If not using SecretAgent, the available certificate stores will instead be your personal CAPI store, your Address Book CAPI store, and your Root CAPI store and these certificates will be verified before being displayed.



- To process these changes click the **Update** button. You may be prompted to enter your password. After SpyProof! has updated the recipients list you will be returned to the **Disk Manager**.

⇒ **Removing recipients from a SpyProof! disk:**

1. To remove recipients from a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**, then select the disk you want to view or modify, then either select **View/Edit Recipients** from the **Disk** menu or use the keyboard combination **<Alt + D, V>** to view the current recipients.
2. From the **View/Edit Recipients** dialog, you can both add and remove recipients to the disk. To remove recipients first select the certificate you want to remove then click the **Remove** button.



3. The recipient will be removed from the list. To process your changes, click the **Update** button.
4. You will then be asked if you want to rekey the disk. Rekeying is a process where the session key that is used to encrypt the disk is changed. This process helps ensure that removed users will no longer be able to access any of the encrypted data. If you want to rekey the disk, click **Yes**.

Note: Rekeying a disk changes the session key that is used to encrypt the data on your SpyProof! disk. This session key is individually encrypted for each of the recipients you specify and is stored in the .spk file for this disk. If you do not rekey, the .spk file is updated so that the session key is encrypted only for the current recipients; however, if the removed user has an old copy of the .spk file that included them as a recipient, they could still access the encrypted data since the session key has not changed. For this reason, rekeying is recommended if you want to ensure removed recipients can no longer access the disk.

5. If you choose to rekey, you will be asked if you want to backup your SpyProof! disk. If you want to backup your disk, click **Yes**.

Note: Rekeying the contents of the disk temporarily leaves the contents of your SpyProof! disk in an inaccessible state. To make sure no important data is lost, it is strongly suggested you backup your SpyProof! disk. This backup process is similar to exporting the disk (described below) so all data will still remain in an encrypted format. Backing up will help guarantee no information is lost if the rekeying process is not allowed to complete (system crash, loss of network connectivity, etc.) If the rekeying process is aborted, you can continue the process by using the **Disk Recovery** tool described later.

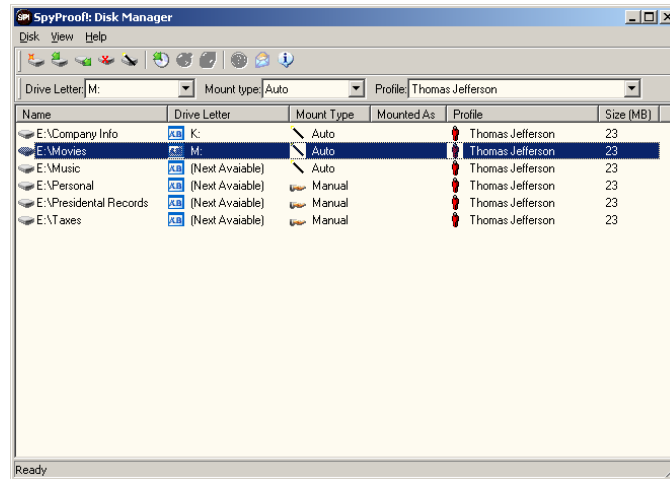
6. You may then be prompted for a password. Enter your password and click **OK** to continue.
7. SpyProof! will begin the removal process. If you are rekeying, this process may take a while depending on the size of your disk. After it has completed, you will be returned to the **Disk Manager**.

Importing a SpyProof! disk

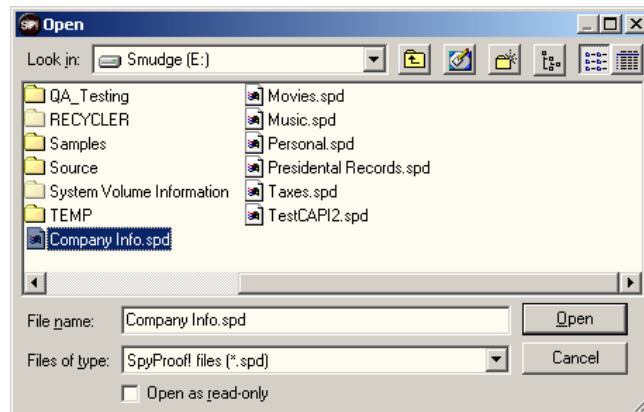
Follow these steps to import a SpyProof! disk.

⇒ To import a SpyProof! disk:

1. To import a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**, then either select **Import** from the **Disk** menu or use the keyboard combination <Alt + D, I> to start the import process.



2. Select the disk you wish to import from the file open dialog and click **Open**.



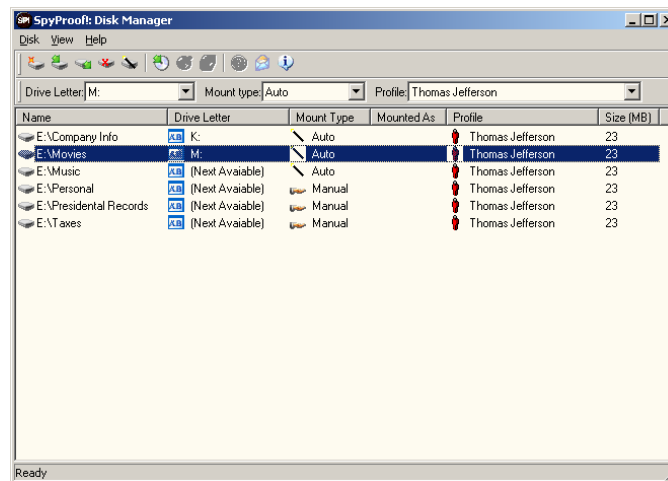
3. SpyProof! will import the disk and automatically attempt to find a profile that can use the disk. If SpyProof! cannot find a profile capable of using the disk you will be asked to assign a profile.

Exporting a SpyProof! disk

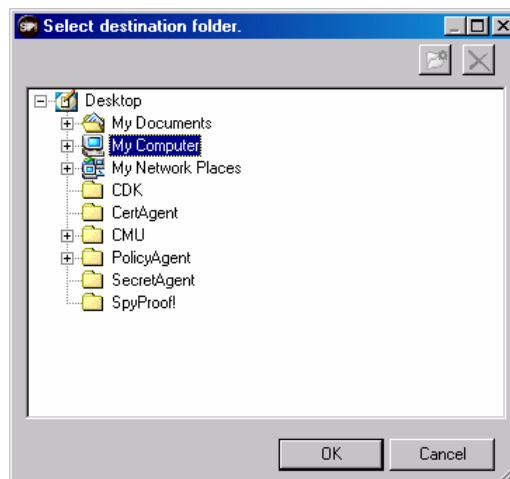
Follow these steps to export a SpyProof! disk.

⇒ **To export a SpyProof! disk:**

4. To export a SpyProof! disk double click on the system tray icon to display the SpyProof! **Disk Manager**, then either select **Export** from the **Disk** menu or use the keyboard combination <Alt + D, E> to start the export process.



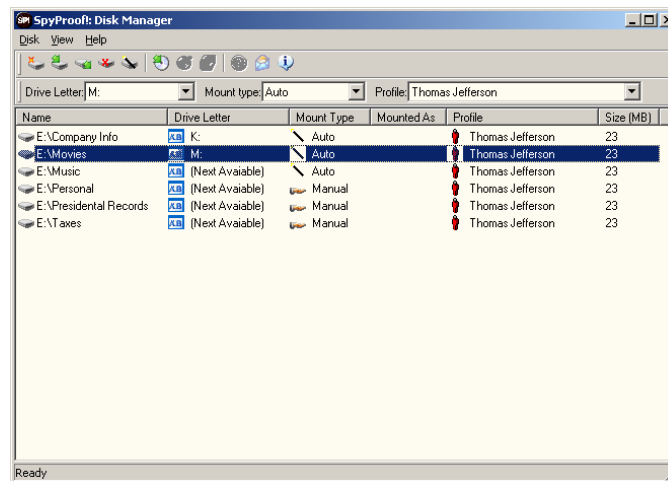
5. Select the path to place the exported disk's files in the **Select destination folder** dialog and click **OK**.



6. SpyProof! will copy the disk's .spd and .spk files to the location you specified. This may take some time depending on the size of your disk.

The Disk Manager

SpyProof!'s **Disk Manager** provides an easy interface for managing your disks. All of SpyProof!'s functionality is available from the **Disk Manager** by using the menu bar, toolbar, or the context menu. The **Disk Manager** lists all disks that you have created or imported, whether they are mounted or not, what drive letter they get mounted on, what profile is used to mount them, and whether they are mounted automatically when SpyProof! starts or are manually mounted.



Making disks mount automatically

⇒ **To make a SpyProof! disk mount automatically when SpyProof! starts:**

1. To make a disk mount automatically when SpyProof! starts, select the disk in the **Disk Manager** and then either select **Automount** from the **Disk** menu or use the keyboard combination <Alt + D, A>.

Assigning drive letters to disks

⇒ **To make a SpyProof! disk always mount at a specific drive letter:**

1. To make a disk always mount at a specific drive letter, select the disk and then choose the drive letter you want to use for that disk from the **Drive Letter** combo box on the toolbar.

Change the profile used to mount a disk

⇒ **To change the profile used to mount a SpyProof! disk:**

1. To change the profile used to mount a disk, select the disk and then choose the profile you want to use for that disk from the **Profile** combo box on the toolbar.

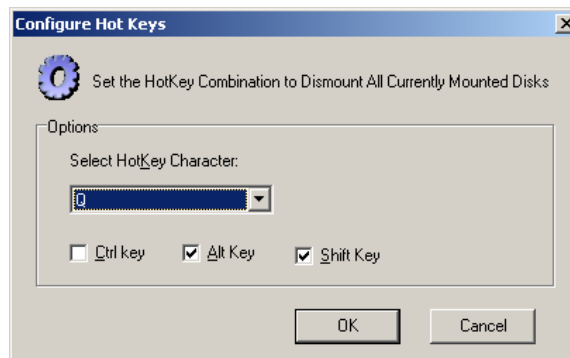
Additional Tools

SpyProof! includes additional tools such as the ability to configure the Unmount All HotKey, recovering disks that were incompletely rekeyed when removing a recipient. This section describes these tools.

Configuring the Unmount All HotKey

⇒ **To configure the Unmount All Hotkey:**

1. From the **Disk Manager**, select **Set HotKey** from the **Options** menu. This will take you to the **Configure HotKeys** dialog.



2. Select the keyboard combination you want to use to have SpyProof! silently dismount all currently mounted disks. Click **OK** when complete. You will return to the **Disk Manager**.

Recovering Incompletely Rekeyed Disks

If you attempted to remove a recipient from a SpyProof! disk but the process was not allowed to complete use the **Disk Recovery** tool to continue the rekeying process.

⇒ **To recover an incompletely rekeyed SpyProof! disk:**

1. From the **Disk Manager**, select **Disk Recovery** from the **Tools** menu. This will take you to the **Disk Recovery Progress** dialog.



2. Click **Start**. SpyProof! will examine the disk. You may be asked for your password twice to begin recovery. Once SpyProof! has the necessary information, the recovery process will begin. Depending on the size of the disk, this can take several minutes. After it has completed, you will return to the **Disk Manager**.

Note: During the rekeying process, SpyProof! creates temporary files in the same directory as the .spd and .spk files SpyProof! usually creates. To recover a disk these files (extensions .spb and .spi) must be in the same directory as the .spd and .spk files.

Command Line Functionality

Many of the SpyProof! functions described above can be invoked from the Windows command prompt. This helps administrators and developers call SpyProof!'s functions from their own scripts, batch files, or applications. SpyProof! disks can be created, mounted, unmounted, imported, and removed via the command line. The format is as follows:

⇒ Format for Creating SpyProof! disks:

```
AESdisk.exe -cfilename.spd -ssize [-pprofname] [-t] [-a] [-bAESSize]
```

Where :

size: the number of MB

profname: the Common Name of the user's certificate stored in their Personal CAPI store or, if installed, the SecretAgent Profile Name

AESSize: one of 128, 192, or 256 to designate the size of the AES cipher. The default is 128.

-t: if designated, SpyProof! will use SecretAgent Profiles, otherwise SpyProof! uses CAPI

-a: if designated, SpyProof! will mark the disk as automount, otherwise the disk will be set to manually mount

Note: If there is a '-' character in the filename or profile name, you will need to put the name in quotes.

Example: The command

```
AESdisk.exe -cc:\disk.spd -s100 -p"Thomas Jefferson" -b192 -a
```

Creates a 100 MB disk named c:\disk.spd and sets the disk to be automatically mounted. The cipher used will be AES-192. It will use the certificate with a CN of Thomas Jefferson (which should be located in the user's Personal CAPI store).

⇒ Format for Mounting SpyProof! disks:

```
AESdisk.exe -mfilename.spd [-h]
```

Where:

-h: SpyProof! will not display a window containing the disk contents after mounting.

Example: The command

```
AESdisk.exe -mc:\disk.spd
```

Mounts the disk named c:\disk.spd. A window showing the newly mounted disk will be displayed. The user may be asked to enter a password depending on how their private key is configured.

⇒ Format for Unmounting SpyProof! disks:

```
AESdisk.exe -ufilename.spd
```

Example: The command

```
AESdisk.exe -uc:\disk.spd
```

Unmounts the disk named c:\disk.spd.

⇒ **Format for Importing SpyProof! disks:**

```
AESdisk.exe -ifilename.spd [-t]
```

Where:

-t: Spyproof! will use SecretAgent Profiles, otherwise SpyProof! uses CAPI

Example: The Command

```
AESdisk.exe -ic:\disk.spd -t
```

Imports the disk named c:\disk.spd. SpyProof! will configure the disk to use an automatically determined SecretAgent profile.

⇒ **Format for Removing SpyProof! disks:**

```
AESdisk.exe -rfilename.spd [-s] [-d|u]
```

Where:

-s: Prompt the user to confirm that the disk should be removed

-d: SpyProof! will delete the associated disk files without asking the user

-u: SpyProof! will not delete the associated disk files without asking the user

Example: The command

```
AESdisk.exe -rc:\disk.spd -s -u
```

Removes the disk named c:\disk.spd. The user will not be asked to confirm the removal of the disk from SpyProof!'s list of known drives. The user will also not be asked whether the associated disk files should be deleted; instead they will automatically not be deleted.

Glossary

Access Control	The process of limiting access to data and other computer system resources to only authorized subjects.
AES	The Advanced Encryption Standard (FIPS 197) is a block cipher based on the Rijndael cryptosystem. SpyProof! provides 128, 192, or 256-bit AES.
Algorithm	A recipe, or sequence of steps, by which a particular result is obtained. A cryptographic algorithm may be conventional (e.g., DES) or public-key (e.g., RSA or ElGamal). With a system of the former type, the encryption and decryption keys are usually identical; with the later type of system they are always different.
Analytical Attack	The attempt to break a particular code and recover plaintext or a secret key by solving a set of mathematical equations obtained from the definition of the cryptographic algorithm. It is believed that the ElGamal cryptosystem is immune to such an attack because the only set of equations presently known, which could be of use, are of sufficient complexity to make all attempts at solution infeasible.
Attack	The attempt to bypass system security controls or break a particular protection mechanism. In general, successful attacks may be active (involving the alteration or destruction of data), or passive (involving the disclosure of sensitive data).
Authentication	A process which provides undeniable proof that someone or something is valid or genuine. In message authentication one is interested in verifying that a received message has not been tampered with, i.e., that there have been no deletions, alterations, or additions of spurious information. This is most easily accomplished using CRCs or encryption. In sender authentication, one is interested in verifying the identity of the originator of a message. Digital signatures may be used for both message and sender authentication.
Block Cipher	A cryptographic system (substitution cipher) in which each plaintext source is broken up into strings of bits or characters of equal length (the block length) and each block is encrypted as a whole. In contrast, a stream cipher is a system in which plaintext units are encrypted one at a time.
Bulk Cipher	A bulk cipher is an encryption algorithm used to encrypt or decrypt large amounts of data with a single secret key. This secret key is then encrypted with each recipient's public key for transport.
CA Certificate	This is a certificate used by a CA to issue end user certificates. CA certificates are not displayed in the Encryption dialog as available recipients.
CBC Mode (Cipher Block Chaining Mode)	Cipher Block Chaining Mode is one mode of operation for block ciphers. The plaintext of the block to be encrypted is XORed with the previous block's ciphertext before encryption. The first block to be encrypted is XORed with an Initialization Vector that is a random value that must be transmitted along with the ciphertext.
Certificate	A certificate is a digital document that affirms the identity of an individual. They allow a receiver to verify that a message has not been altered and that the sender is authenticated. A basic certificate contains a public key and a common name. Certificates can be self-signed or issued by a certificate authority which can vouch for the identity of the sender and the key associated with the sender. Certificates allow receivers of encrypted files to verify that a key belongs to a given individual. Certificates contain the public key for recipients of encrypted archives.
Certificate Authority (CA)	A certificate authority is a combination of software that actually generates certificates and an organization that guarantees the identity of the person requesting the certificate. Since there is an organization guaranteeing that the certificate was issued to the requester it is possible to verify digital signatures and be sure that they are authentic.

Certificate Chain Validation	Certificate chain validation is the process of verifying a certificate. An issuer issues each certificate. The issuer's certificate is used to validate the signature on the end user certificate. The issuer's certificate is then checked in a similar fashion. This continues until the root (a self-signed certificate) is reached. At that point the certificate is considered valid if all of the signatures were valid and the root certificate is trusted (by default all root certificates are trusted, but the SpyProof! PolicyAgent Tool lets a security officer specify which root certificates are trusted). Optionally, each certificate in the chain may also be checked against a CRL and if no certificate in the chain is revoked then the end user certificate is valid. SpyProof! and Certificate Explorer only look for CA Certificates in your Personal Certificate store. In order to properly verify end user certificates you must make sure that the entire certificate chain is in your Personal Certificate Store.
Certificate Revocation List	Certificate Revocation Lists are lists of certificates that have been revoked by a certificate authority for some reason. Certificate Revocation Lists are used as part of the certificate validation process in which each certificate in a certificate chain is checked against the proper CRL and if any certificate in the chain is found in a CRL the end user certificate is not valid.
Certificate Store	A certificate store is a file, folder, server, or other device that stores certificates and provides an interface for retrieval of certificates.
Cleartext	See plaintext.
Ciphertext	Encrypted text or cryptogram. The result of applying an encryption algorithm to plaintext.
Compromise	A violation of a system security policy possibly resulting in the unauthorized disclosure of sensitive information.
Cryptanalysis	The attempt to recover plaintext from ciphertext, thereby defeating the benefits of encryption.
Cryptographic key	A parameter that serves to distinguish different cryptographic transformations in a cryptographic system. This term is also commonly used to refer to that element of a cryptographic system that controls the encryption or decryption algorithms.
Cryptography	The study of secret writing and communication.
Decryption	The process of decipherment, usually under the control of a secret key or password, whereby plaintext is recovered from ciphertext.
DES	An encryption algorithm submitted to the National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards [NBS]) by IBM in 1974 and adopted as a federal standard on July 15, 1977
DES3	Triple-DES is a well-known, federally approved, block cipher that provides slightly less security than AES.
DESX	A modification of the federally approved DES algorithm. Many believe that DESX offers equivalent security to DES3 (112-bit effective session key length) but is 3 times faster.
Decipher	To apply a cryptographic transformation to ciphertext in order to recover the original plaintext.
Diffie-Hellman Cryptosystem	A public key cryptosystem devised by W. Diffie and M. Hellman whose strength lies in the difficulty of computing discrete logs in a large finite field.
Digital Signatures	The means by which a user may sign a message so that the intended recipient of the message can easily establish the sender's authenticity.
Digital Signature Algorithm (DSA)	The digital signature scheme defined in the Digital Signature Standard Federal Information Processing Standard (FIPS 186). The Digital Signature Algorithm (DSA) is intended to be used with the NIST Secure Hash Algorithm (SHA) to provide sender and message authentication in EDI applications.
EIGamal Cryptosystem	A public key cryptosystem devised by T. ElGamal whose strength is based upon the difficulty of computing discrete logarithms in a finite field. One of the two most secure public key cryptosystems currently available. (See also RSA.)

Encipher	To apply a cryptographic transformation to sensitive data (the plaintext) in an effort to protect it from disclosure to an unauthorized subject.
Encryption	The process of encipherment, or “scrambling;” transforming plaintext into ciphertext.
End User Certificate	A certificate issued to an individual by a certificate authority.
Exhaustive attack	An attempt to break a particular code and recover a plaintext message or key by using a direct search method.
Hashing	The transformation of a very large set onto a smaller one. In cryptography, the process of obtaining a relatively short “fingerprint,” or message digest, from a typically large stream of data for use in message authentication or digital signatures.
Hybrid Cipher	A cryptographic system designed to possess the best features of several older systems. Typically a fast conventional cipher is teamed with a public key system for key management and digital signatures.
Key	See secret key or public key.
Key Management	The processes of generation, distribution, and protection of secret keys and or passwords or the maintenance of a public key list. Key management is typically a major problem with a conventional cryptosystem since secret keys must be maintained for users. In a public key system, each user guards their own secret key and there are only public keys to distribute and maintain.
Password	A secret key that allows the owner access to a particular data object or resource.
Personal Certificate Store	The store in SecretAgent’s Certificate Explorer designated as the store in which your private key and matching certificate are stored. It is also the store in which CA certificates are stored.
Physical Security	Physical obstructions and control procedures used as preventative measures or countermeasures against threats to resources and sensitive data.
Plaintext	The original data or message as it appears before encryption.
Public Key	A key that controls the encryption process for a particular code in a public key cryptosystem. Divulging this key should in no way weaken the security of the code.
Public Key Cryptosystem	A cryptographic system in which each code requires the use of two keys: a public key for encryption and a private or secret key for decryption. The existence of separate keys for the two processes allows several users to encipher data using the same public key, while only one specific user may decipher that data.
Private Key	In a public key cryptosystem the private key is that portion of a user’s key pair that is kept secret. The private key is used to decrypt information and to sign information.
RSA Cryptosystem	A public key cryptosystem devised by R. Rivest, A. Shamir, and L. Adleman whose strength is based upon the difficulty of factoring large numbers. The subject of U.S. Patent No. 4,405,829 issued to M.I.T. in 1983, RSA (along with ElGamal) is one the most secure public key cryptosystems available. This patent has expired.
Secret Key	The key that controls the decryption process for a particular code in a public key cryptosystem.
Self-Signed Certificate	A self-signed certificate is an end user certificate that is not issued by a CA. Self-signed certificates are displayed in the Encryption dialog as available recipients if allowed by PolicyAgent settings.
Session Key	The secret key used by a block cipher in a hybrid cipher system. The session key is transmitted securely via a public key encryption algorithm to all recipients.
Stream Cipher	See block cipher.
Token	A device that provides cryptographic operations and/or private key storage.