HP ProtectTools Security Software, Version 6.0

User Guide

© Copyright 2009, 2010 Hewlett-Packard
Development Company, L.P. The
information contained herein is subject to
change without notice.

Microsoft, Windows and Windows Vista are
either trademarks or registered trademarks
of Microsoft Corporation in the United
States and/or other countries.

The only warranties for HP products and
services are set forth in the express
warranty statements accompanying such
products and services. Nothing herein
should be construed as constituting an
additional warranty. HP shall not be liable
for technical or editorial errors or omissions
contained herein.

This document contains proprietary
information that is protected by copyright.
No part of this document may be
photocopied, reproduced, or translated to
another language without the prior written
consent of Hewlett-Packard Company.

**HP ProtectTools Security Software User
Guide**

Third Edition: November 2010

Document Part Number: 581746-003

About This Book

This guide provides basic information for upgrading this computer model.

⚠ **WARNING!**   Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

△ **CAUTION:**   Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

📝 **NOTE:**   Text set off in this manner provides important supplemental information.

Table of contents

1 Introduction to security

HP ProtectTools security software provides security features that help protect against unauthorized access to the computer, networks, and critical data. Enhanced security functionality is provided by several HP ProtectTools software modules.

HP ProtectTools provides two versions that can be utilized: HP ProtectTools Security Manager Administrative Console and HP ProtectTools Security Manager (for general users). Both Administrator and user versions are available in the **Start** > **All Programs** > **HP** menu.

Function	Features
HP ProtectTools Security Manager Administrative Console	● Requires Microsoft Windows system administrator rights to access ● Access to modules to be configured by an administrator and not available to the general user ● Allows initial security setup and configures options or requirements for all users
HP ProtectTools Security Manager (for general users)	● Allows users to configure options provided by an administrator ● Can restrict access and only allow a user limited controls of some HP ProtectTools modules

NOTE: Password Manager, Smart Card Security, Face Recognition (some models) and Drive Encryption are configured using the Security Manager setup wizard. HP Professional Desktop systems do not currently support fingerprint devices.

HP ProtectTools software modules may be preinstalled, preloaded, or available as a configurable option or as an after market option. Visit http://www.hp.com for more information.

NOTE: The instructions in this guide are written with the assumption that you have already installed the applicable HP ProtectTools software modules.

HP ProtectTools features

The following table details the key features of HP ProtectTools modules:

Module	Key features
HP ProtectTools Security Manager Administrative Console	- The Security Manager setup wizard is used by administrators to set up and configure levels of security and security logon methods. - Configure options hidden from basic users. - Activate Drive Encryption and configure user access. - Configure Device Access Manager configurations and user access. - Administrator tools are used to add and remove HP ProtectTools users and view user status.
HP ProtectTools Security Manager (for general users)	- Configure and change File Sanitizer Shred, Bleaching, and Settings. - View settings for Encryption Status and Device Access Manager. - Use Privacy Manager to increase security of e-mails and documents. - Activate Computrace for HP ProtectTools - Configure Preferences and Backup and Restore options.
Credential Manager for HP ProtectTools (part of Security Manager)	- Organize, set up and change user names and passwords. - Configure and change user credentials such as Windows password and Smart Card. - Acts as a personal password vault, streamlining the logon process with the Single Sign On feature, which automatically remembers and applies user credentials. - Create and Organize single sign on user names and passwords.
Drive Encryption for HP ProtectTools	- Provides complete, full-volume hard drive encryption. - Forces pre-boot authentication in order to decrypt and access the data on the hard drive. - Offers the option to activate SED drives (Self Encrypting Drives), if equipped.
Privacy Manager for HP ProtectTools	Used to obtain Certificates of Authority, which verify the source, integrity, and security of communication when using Microsoft e-mail and Microsoft Office documents.
File Sanitizer for HP ProtectTools	Allows you to securely shred digital assets (securely delete sensitive information including application files, historical or Web-related content, or other confidential data) on your computer and periodically bleach the hard drive (write over data that has been previously deleted but is still present on the hard drive in order to make recovery of the data more difficult).

Module	Key features
Smart Card Security (part of Security Manager)	• Provides a management software interface for Smart Card. HP ProtectTools Smart Card is a personal security device that protects authentication data requiring both the card and a PIN number to grant access. The Smart Card can be used to access Password Manager, Drive Encryption, or any number of third party access points. • Change PIN number.
Embedded Security for HP ProtectTools	• Uses a Trusted Platform Module (TPM) embedded security chip (if equipped) to help protect against unauthorized access to sensitive user data or credentials stored locally on a PC. • Allows creation of a personal secure drive (PSD), which is useful in protecting user file and folder information. • Supports third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations.
Device Access Manager for HP ProtectTools	• Allows IT managers or administrators to control access to devices such as USB ports, optical drives, personal music players, etc. based on user profiles. • Prevents unauthorized users from removing data using external storage media and from introducing viruses into the system from external media. • The administrator can disable access to writeable devices for specific individuals or groups of users. • Allows the administrator to schedule when access is provided to hardware.
Computrace for HP ProtectTools	• Provides secure asset tracking. • Can monitor user activity along with hardware and software changes. • Remains active even if the hard drive is reformatted or replaced. • Requires separate purchase of tracking and tracing subscription to activate.

HP ProtectTools security products description and common use examples

Most of the HP ProtectTools security products have both a user authentication (usually a password) and an administrative backup to gain access if passwords are lost, not available, forgotten, or any time corporate security requires access.

NOTE: Some of the HP ProtectTools security products are designed to restrict access to data. Data should be encrypted when it is so important that the user would rather lose the information then have it compromised. It is recommended that all data be backed up in a secure location.

Credential Manager (Password Manager) for HP ProtectTools

Credential Manager (part of Security Manager) is a repository for user names and passwords. It is most often used to save login names and passwords for Internet access or web mail. Credential Manager can automatically log the user into a web site or mail.

Example 1: A Purchasing Agent for a large manufacturer makes most of her corporate transactions over the Internet. She also frequently visits several popular web sites that require login information. She is keenly aware of security so does not use the same password on every account. The Purchasing Agent has decided to use Credential Manager to match web links with different user names and passwords. When she goes to a web site to log in, Credential Manager presents the credentials automatically. If she wants to view the user names and password, Credential Manager can be configured to reveal them.

Credential Manager can also be used to manage and organize the authentications. This tool will allow a user to select what web or network asset they choose and directly access the link. The user can also view the user names and passwords when necessary.

Example 2: A hard working CPA has been promoted and will now manage the entire accounting department. The team must log into a large number of client web accounts with each account using different login information. This login information needs to be shared with other workers so confidentiality is an issue. The CPA decides to organize all the web links, company user names, and passwords within Credential Manager for HP ProtectTools. Once complete, the CPA deploys Credential Manager to the employees so they can work on the web accounts and never know the login credentials that they are using.

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools provides the ability to create a Personal Secure Drive. This capability allows the user to create a virtual drive partition on the PC that is completely hidden until accessed. Embedded Security could be used anywhere data needs to be secretly protected while the rest of the data is not encrypted.

Example 1: A Warehouse Manager has a computer that multiple workers access intermittently throughout the day. The Manager wants to encrypt and hide confidential warehouse data on the computer. He wants the data to be so secure that even if someone steals the hard drive, they cannot decrypt the data or read it. The Warehouse Manager decides to activate Embedded Security and moves the confidential data to the Personal Secure Drive. The Warehouse Manager can enter a password and access the confidential data just like another hard drive. When he logs off or reboots the Personal Secure Drive, it cannot be seen or opened without the proper password. The workers never see the confidential data when they access the computer.

Embedded Security protects encryption keys within a hardware TPM (Trusted Computing Module) chip located on the motherboard. It is the only encryption tool that meets the minimum requirements to resist password attacks where someone would attempt to guess the decryption password. Embedded Security can also encrypt the entire drive and e-mail.

Example 2: A Stock Broker wants to transport extremely sensitive data to another computer using a portable drive. She wants to make sure that only these two computers can open the drive, even if the password is compromised. The Stock Broker uses Embedded Security TPM migration to allow a second computer to have the necessary encryption keys to decrypt the data. During the transport process, even with the password, only the two physical computers can decrypt the data.

Drive Encryption for HP ProtectTools

Drive Encryption is most often used to restrict access to the data on the entire computer hard drive or a secondary hard drive. Drive Encryption can also manage SED (Self Encrypting Drive) drives.

Example 1: A Doctor wants to make sure only he can access any data on his computer hard drive. The Doctor activates Drive Encryption which enables preboot or requiring authentication before Windows login. Once set up, the hard drive cannot be opened without a password before it even boots to the operating system. The Doctor could further enhance drive security by choosing to encrypt the data with the SED (Self Encrypting Drive) option.

Both Embedded Security and Drive Encryption for HP ProtectTools will not allow access to the encrypted data even when the drive is removed because they are both bound to the original motherboard.

Example 2: A Hospital Administrator wants to ensure only doctors and authorized personnel can access any data on their local computer without sharing their personal passwords. The IT department adds the Administrator, doctors, and all authorized personnel as Drive Encryption users. Now only authorized personnel can boot to the computer or Domain using their personal username and password.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools is used to permanently delete data, including Internet browser activity, temporary files, previously deleted data, or any other information. File Sanitizer can be configured to run either manually or automatically on a user-defined schedule.

Example 1: An Attorney often deals with sensitive client information and wants to ensure data on deleted files cannot be recovered. The Attorney uses File Sanitizer to "Shred" deleted files so it is almost impossible to recover.

Normally when Windows deletes data, it actually does not erase the data from the hard drive. Instead, it marks the hard drive sectors as available for future use. Until the data is written over, it can be easily recovered using common tools available on the Internet. File Sanitizer overwrites the sectors with random data (multiple times when necessary) thereby making the deleted data unreadable and unrecoverable.

Example 2: A Researcher wants to shred deleted data, temporary files, browser activity, etc. automatically when she logs off. She uses File Sanitizer to schedule "Shredding" so she can select the common files or any custom files to be permanently removed automatically.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools can be used to block unauthorized access to USB flash drives where data could be copied. It can also restrict access to CD/DVD drives, control of USB devices, network connections, etc. An administrator can also schedule when or how long drives can be accessed. An example would be a situation where outside vendors need access to company computers but should not be able to copy the data to a USB drive. Device Access Manager for HP ProtectTools allows an administrator to restrict and manage access to hardware.

Example 1: A Manager of a medical supply company often works with personal medical records along with his company information. The employees need access to this data, however, it is extremely important that the data is not removed from the computer by a USB drive or any other external storage media. The network is secure, but the computers have CD burners and USB ports that could allow the data to be copied or stolen. The Manager uses Device Access Manager to disable the USB ports and CD burners so they cannot be used. Even though the USB ports are blocked, mouse and keyboards will continue to function.

Example 2: An Insurance company does not want its employees to install or load personal software or data from home. Some employees need access to the USB port on all computers. The IT Manager uses Device Access Manager to enable access for some employees while blocking external access to others.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools is used when Internet e-mail communications need to be secured. The user can create and send e-mail that can only be opened by an authenticated recipient. With Privacy Manger, the information cannot be compromised or intercepted by an imposter.

Example 1: A Stock Broker wants to make sure his e-mails only go to specific clients and ensure no one can fake the e-mail account and intercept it. The Stock Broker signs himself and his clients up with Privacy Manager. Privacy Manager issues them a Certificate of Authentication (CA) to each user. Using this tool, the Stock Broker and his clients must authenticate before the e-mail is exchanged.

Privacy Manager for HP ProtectTools makes it easy to send and receive e-mail where the recipient has been verified and authenticated. The mail service can also be encrypted. The encryption process is similar to the one used during general credit card purchases on the Internet.

Example 2: A CEO wants to insure that only the members of the board of directors can view the information he sends through e-mail. The CEO uses the option to encrypt the e-mail sent and received from the directors. Privacy Manager Certificate of Authentication allows the CEO and directors to have a copy of the encryption key so only they can decrypt the confidential e-mail.

Computrace for HP ProtectTools (formerly known as LoJack Pro)

Computrace for HP ProtectTools is a service that can track the location of a stolen computer whenever the user accesses the Internet.

Example 1: A school principal instructed the IT department to keep track of all the computers at his school. After the inventory of the PCs was made, the IT Administrator registered all the computers with Computrace so they could be traced in case they were ever stolen. Recently, the school realized several computers were missing, so the IT Administrator alerted authorities and Computrace officials. The computers were located and were returned to the school by the authorities.

Computrace for HP ProtectTools can also help remotely manage and locate computers as well as monitor computer usage and applications.

Example 2: A real estate company needs to manage and update computers all over the world. They use Computrace to monitor and update the computers without having to send an IT person to each computer.

Accessing HP ProtectTools Security

To access HP ProtectTools Security Manager from the Windows Start menu:

▲ In Windows, click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

To access HP ProtectTools Security Manager Administrative Console from the Windows Start menu:

▲ In Windows, click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

NOTE: After you have configured the Password Manager module, you can also open HP ProtectTools by logging on to Password Manager directly from the Windows logon screen.

Achieving key security objectives

The HP ProtectTools modules can work together to provide solutions for a variety of security issues, including the following key security objectives:

● Protecting against targeted theft

● Restricting access to sensitive data

● Preventing unauthorized access from internal or external locations

- Creating strong password policies

- Addressing regulatory security mandates

Protecting against targeted theft

An example of this type of incident would be the targeted theft of a computer or its confidential data and customer information. This can easily occur in open office environments or in unsecured areas. The following features help protect the data if the computer is stolen:

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. See the following chapters:

  - Password Manager for HP ProtectTools on page 25

  - Embedded Security for HP ProtectTools on page 49

  - Drive Encryption for HP ProtectTools on page 29

- DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system.

- The Personal Secure Drive feature, provided by the Embedded Security for HP ProtectTools module, encrypts sensitive data to help ensure it cannot be accessed without authentication. See the following chapter:

  - Embedded Security for HP ProtectTools on page 49

- Computrace can track the computer's location after a theft. See the following chapter:

  - Computrace for HP ProtectTools on page 57

Restricting access to sensitive data

Suppose a contract auditor is working on site and has been given computer access to review sensitive financial data; you do not want the auditor to be able to print the files or save them to a writeable device such as a CD. The following feature helps restrict access to data:

Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be printed or copied from the hard drive onto removable media. See Device class configuration (advanced) on page 54.

Preventing unauthorized access from internal or external locations

Unauthorized access to an unsecured business PC presents a very tangible risk to critical data such as information from financial services, an executive, or R&D team, and to private information such as patient records or personal financial records. The following features help prevent unauthorized access:

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. See the following chapters:

    ○

    ○

    ○

- Embedded Security for HP ProtectTools helps strengthen the protection of sensitive user data or credentials stored locally on a PC. See the following chapter:

    ○

- Password Manager for HP ProtectTools helps ensure that an unauthorized user cannot get passwords or access to password-protected applications. See the following chapter

    ○

- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be copied from the hard drive. See the following chapter:

    ○

- The Personal Secure Drive feature encrypts sensitive data to help ensure it cannot be accessed without authentication. See the following section:

    ○

- File Sanitizer allows you to securely delete data by shredding critical files and folders or bleaching the hard drive (write over data that has been previously deleted but is still present on the hard drive in order to make recovery of the data more difficult). See the following chapter:

    ○

- Privacy Manager allows you to obtain Certificates of Authority when using Microsoft mail, Office documents, and Instant Messenger, making the process of sending and saving important information safe and secure. See the following chapter:

    ○

Creating strong password policies

If a mandate goes into effect that requires the use of strong password policy for dozens of Web-based applications and databases, Password Manager for HP ProtectTools provides a protected repository for passwords and Single Sign On convenience. See the following chapter:

-

Additional security elements

Assigning security roles

In managing computer security, one important practice is to divide responsibilities and rights among various types of administrators and users.

NOTE: In a small organization or for individual use, these roles may all be held by the same person.

For HP ProtectTools, the security duties and privileges can be divided into the following roles:

- Security officer—Defines the security level for the company or network and determines the security features to deploy, such as Drive Encryption or Embedded Security.

- IT administrator—Applies and manages the security features defined by the security officer. Can also enable and disable some features. For example, if the security officer has decided to deploy Smart Cards, the IT administrator can enable both password and Smart Card mode.

- User—Uses the security features. For example, if the security officer and IT administrator have enabled Smart Cards for the system, the user can use the card for authentication.

Managing HP ProtectTools passwords

Most of the HP ProtectTools Security Manager features are secured by passwords. The following table lists the commonly used passwords, the software module where the password is set, and the password function.

The passwords that are set and used by IT administrators only are indicated in this table as well. All other passwords may be set by regular users or administrators.

HP ProtectTools password	Set in this HP ProtectTools module	Function
Password Manager logon password	Password Manager	This password offers 2 options: • It can be used in a separate logon to access Password Manager after logging on to Windows. • It can be used in place of the Windows logon process, allowing access to Windows and Password Manager simultaneously.
Basic User Key password **NOTE:** Also known as: Embedded Security password	Embedded Security	Used to access Embedded Security features, such as secure e-mail, file, and folder encryption. When used for power-on authentication, also protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
Emergency Recovery Token password **NOTE:** Also known as: Emergency Recovery Token Key password	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the embedded security chip.
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.

HP ProtectTools password	Set in this HP ProtectTools module	Function
Smart Card PIN	Smart Card Security	Can be used as a multifactor authentication option.
		Can be used as a Windows authentication.
		Authenticates users of Drive Encryption, if the Smart Card token is selected.
Computer Setup password **NOTE:** Also known as BIOS administrator, F10 Setup, or Security Setup password	BIOS, by IT administrator	Protects access to the Computer Setup utility.
Power-on password	BIOS	Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
Windows Logon password	Windows Control Panel	Can be used for manual logon.

Creating a secure password

When creating passwords, you must first follow any specifications that are set by the program. In general, however, consider the following guidelines to help you create strong passwords and reduce the chances of your password being compromised:

- Use passwords with more than 6 characters, preferably more than 8.

- Mix the case of letters throughout your password.

- Whenever possible, mix alphanumeric characters and include special characters and punctuation marks.

- Substitute special characters or numbers for letters in a key word. For example, you can use the number 1 for letters I or L.

- Combine words from 2 or more languages.

- Split a word or phrase with numbers or special characters in the middle, for example, "Mary2-2Cat45."

- Do not use a password that would appear in a dictionary.

- Do not use your name for the password, or any other personal information, such as birth date, pet names, or mother's maiden name, even if you spell it backwards.

- Change passwords regularly. You might change only a couple of characters that increment.

- If you write down your password, do not store it in a commonly visible place very close to the computer.

- Do not save the password in a file, such as an e-mail, on the computer.

- Do not share accounts or tell anyone your password.

Backing up credentials and settings

You can back up credentials in the following ways:

- Use Drive Encryption for HP ProtectTools to select and back up HP ProtectTools credentials.

    You can also register for Online Drive Encryption Key Recovery Service to store a backup copy of your encryption key, which will enable you to access your computer if you forget your password and do not have access to your local backup.

- Use Embedded Security for HP ProtectTools to back up HP ProtectTools credentials.

- Use the Backup and Recovery tool in HP ProtectTools Security Manager as a central location from which you can back up and restore security credentials from installed HP ProtectTools modules.

2 HP ProtectTools Security Manager Administrative Console

About HP ProtectTools Administrative Console

Administration of HP ProtectTools Security Manager is provided through the Administrative Console.

Using the console, the local administrator can:

- Enable or disable security features
- Manage users of the computer
- Adjust device-specific parameters
- Configure Security Manager applications
- Add additional Security Manager applications

Using the Administrative Console

The Security Manager Administrative Console is the central location for administering HP ProtectTools Security Manager.

To open the console:

- Select **Start** > **All Programs** > **HP** > **HP ProtectTools Administrative Console**, or
- Click the **Administration** link in the lower-left corner of the Security Manager console.

The Administrative Console consists of two panes: a left pane and a right pane. The left pane contains the administrative tools. The right pane contains the working area for configuring the tools.

The Administrative Console left pane consists of the following:

- **Home** - Provides easy access to commonly used tasks, including enabling security features, specifying security credentials, and managing users.
- **System** - Manages configuration of system-wide security features, users, and authentication devices such as smart card readers.
- **Applications** - Includes tools for configuring the behavior of Security Manager and its applications.
- **Data** - Provides tools for managing drive encryptions and backing up and recovering encryption keys.
- **Computer** - Device Access Manager provides advanced security options to selectively disallow various types of devices that could compromise PC security and set access permissions for various users and groups.
- **Communications** - Privacy Manager allows the user to manage third-party certificates for e-mail authentication. Embedded Security allows the user to exchange TPM encrypted e-mail.

- **Management Tools** - Opens your default browser to a web page where you can discover additional management applications and tools that extend the features of Security Manager as well as a means to stay notified when new applications and updates are available.

- **Links** - Provides the following:

  - **Setup Wizard** - Launches the Setup Wizard, which guides you through the initial configuration of Security Manager.

  - **Help** - Opens the help file, which provides information about Security Manager and its applications.

  - **About** - Displays information about HP ProtectTools Security Manager, including the version number and copyright notice.

Getting Started - Setup Wizard

Administration of HP ProtectTools Security Manager requires administrative privileges.

The HP ProtectTools Security Manager Setup Wizard guides you through setting up the security features of HP ProtectTools. However, there is a wealth of additional functionality available through the HP ProtectTools Security Manager Console. The same settings found in the wizard, as well as additional security features, can be configured through the console, accessed from the Windows Start menu or from a link within the Administrative console. These settings apply to the computer and all users who share the computer.

The first time that you log on to Windows, you will be prompted to set up HP ProtectTools Security Manager. Click **OK** to launch the Security Manager Setup wizard, which will guide you through the basic steps in configuring the program.

📝 **NOTE:** You can also launch the Security Wizard by clicking **Security Wizard** in the bottom section of the left pane on the Administrative Console.

Follow the on-screen instructions in the Setup Wizard until setup is complete.

If you do not complete the wizard, it will launch automatically until you click **Do not show this wizard again**.

To use the HP ProtectTools Security Manager applications, launch HP ProtectTools Security Manager from the **Start** menu or by right-clicking the **Security Manager** icon in the taskbar notification area (system tray). The Security Manager console and its applications are available to all users who share this computer.

Configuring your system

The **System** group of applications is accessed from the **Tools** menu on the left side of the Administrative Console.

By using the applications included in this group, you can configure and manage the policies and settings for this computer, its users and devices.

The following applications are included in the System group.

- **Security** - Manage security features, authentication policies and other settings that govern how users authenticate when logging on to the computer or HP ProtectTools applications.

- **Users** - Set up, manage and enroll users of this computer.

- **Devices** - Manage settings for security devices built-in or connected to the computer.

Enabling security features

The security features enabled here apply to all users of this computer.

1. In the left pane of the Administrative Console, expand **Security**, and click on **Features**.

2. To enable a security feature, click the corresponding check box next to **Windows Logon Security** and/or **Protect data** (activates Drive Encryption).

   ● **Windows Logon Security** - protects your Windows account(s) by requiring the use of specific credentials for access.

   ● **Protect data** - protects your data by encrypting your hard drive(s) using Drive Encryption for HP ProtectTools, making the information unreadable by those without proper authorization.

3. Click the **Next** button.

4. Click the **Finish** button.

Defining Security Manager authentication policies

Security Manager authentication policies for this computer are defined on two tabs, Logon and Session, which specify the credentials required to authenticate each class of user when accessing the computer and HP ProtectTools applications during a user session.

Logon tab

To specify the credentials required to access the computer, decrypt the hard drive, and log on to Windows:

1. In the left pane of the Administrative Console, expand **Security** and click on **Authentication**.

2. On the **Logon** tab, select a category of user from the drop-down list.

3. In the **Policy** section, specify the authentication credential(s) required for the selected category of user by clicking the check box or boxes next to the listed credentials. You must specify at least one credential.

4. In the **Policy** section drop-down list, choose whether ANY (only one) of the specified credentials are required, or if ALL of the specified credentials are required in order to authenticate a user.

5. Click the **Apply** button.

NOTE: If the Policy is set to "ALL of the specified credentials are required to authenticate" and the system is configured for both password and Smart Card and the Smart Card is damaged or lost, all administrators could be locked out of Windows and require special tools to regain access.

Session tab

To define policies governing the credentials required to authenticate a user when logging on to HP ProtectTools applications during a Windows session:

1. In the left pane of the Administrative Console, expand **Security** and click on **Authentication**.

2. On the **Session** tab, select a category of user.

3. In the **Policy** section, specify the authentication credential(s) required for the selected category of user by clicking the check box or boxes next to the listed credentials. You must specify at least one credential.

4. In the **Policy** section drop-down list, choose whether ANY (only one) of the specified credentials are required, or if ALL of the specified credentials are required in order to authenticate a user.

5. Click the **Apply** button.

Defining Settings

You can specify which advanced security settings to allow. To edit the settings:

1. In the left pane of the Administrative Console, expand **Security** and click on **Settings**.

2. Click the appropriate check box to enable or disable a specific setting.

3. Click the **Apply** button to save the changes.

NOTE: The **Allow One Step logon** setting allows users of this computer to skip Windows logon if authentication was performed at the BIOS or encrypted disk level.

Managing Users

Within the Users application, Windows administrator can manage this computer's users and the policies that affect them. To access the Users application in the Administrative Console, click on **Users**.

The HP ProtectTools users are listed and verified against the authentication policies set through Security Manager and against the credentials required to meet those policies.

To view the policies in force for a specific user, select the user from the list and click the **View Policies** button.

To supervise a users while they enroll credentials, select the user from the list and click the **Enroll** button.

Adding a user

This process adds users to the Drive Encryption logon list. Before you add a user, that user must already have a Windows user account on the computer and must be present during the following procedure to provide the password.

To add a User to the users list:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the Administrative Console left pane, click **User**.

3. Click the **Add** button. The **Select Users** dialog box opens

4. Click the **Advanced** button and then click the **Find Now** button to search for users to add.

5. Click a user to be added to the list and then click **OK**.

6. Click **OK** in the **Select Users** dialog box.

7. Type the Windows password for the selected account, and then click **Finish**.

NOTE: You must use an existing Windows account and type it exactly. You cannot modify or add a Windows user account using this dialog box.

Removing a user

NOTE: This procedure does not delete the Windows user account. It only removes that account from Security Manager. To completely remove the user, you must remove the user from both Security Manager and Windows.

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the Administrative Console left pane, click **User**.

3. Click the user name for the account you want to remove, and then click **Delete**.

4. In the confirmation dialog box, click **Yes**.

Checking user status

The User section of the Administrative Console shows the current status of each user:

- **Green check mark** - Indicates that the user has configured the required security login method(s).

- **Tilde (~)** - Indicates that the user has not configured a required security login method and will be locked out of the computer when trying to log in. The user must run the setup wizard to configure the required login method(s).

- **Blank** - Indicates that a security login method is not required.

Specifying device settings

Within the Device application, you can configure the computer to automatically lock when a smart card is removed. However, the computer will lock only if the smart card was used as an authentication credential when logging on to Windows.

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the Administrative Console left pane, expand **Devices** and then click **Smart Card**.

3. Click the check box to enable or disable locking the computer upon smart card removal.

Configuring Applications Settings

The Settings window includes tools for configuring the behavior of Security Manager and its applications. To modify the settings:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the Administrative Console left pane, click **Settings**.

3. On the **General** tab, choose the general settings for HP ProtectTools Security Manager, then click the **Apply** button.

4. On the **Applications** tab, select the applications you want to enable or disable, then click the **Apply** button.

NOTE: Enabling or disabling an application may not take effect until the computer is restarted.

Encrypting Drives

Drive Encryption for HP ProtectTools allows you to encrypt computer hard drives, making the hard drive unreadable and inaccessible to any unauthorized person who might try to access it even if the drive has been removed from the computer or sent to a data recovery service.

To enable or disable Drive Encryption, click on the Setup Wizard in the Administrative Console.

For more information on using Drive Encryption for HP ProtectTools, refer to Drive Encryption for HP ProtectTools on page 29.

Managing Device Access

Device Access Manager for HP ProtectTools provides advanced security options to selectively disallow various types of devices that can compromise the security of your PC. For more information on using Device Access Manager for HP ProtectTools, refer to Device Access Manager for HP ProtectTools on page 53.

3 HP ProtectTools Security Manager

HP ProtectTools Security Manager allows you to significantly increase the security of your computer. Through the use of Security Manager applications, you can:

- Manage your logon and passwords

- Easily change your Windows password

- Set up authentication credentials, including a smart card

- Increase the privacy and security of e-mails, documents, and instant messaging

- Shred or bleach your hard drive

- View drive encryptions status

- View device access settings

- Activate theft recovery software

- Back up and restore Security Manager data

Logging in after Security Manager is configured

Login scenarios vary, depending on the levels of security and security login methods chosen by the Windows administrator during configuration. Several possible scenarios follow:

- If all levels of security have been configured and *all* security login methods are required, users must log in using all of the configured methods when the computer is first turned on. This action logs the user in to Windows.

- If all levels of security have been configured and *any* of the security login methods is permissible, users may log in using any one of the configured security login methods when the computer is first turned on. This action logs the user in to Windows.

- If the HP Drive Encryption and the HP Password Manager levels of security have been configured and *all* security login methods are required, users must log in using all of the configured methods when the HP Drive Encryption login screen opens. This action logs the user in to Windows.

- If the HP Drive Encryption and the HP Password Manager levels of security have been configured and *any* of the configured security login methods is permissible, users may log in using any one of the security login methods when the HP Drive Encryption login screen opens. This action logs the user in to Windows.

- If the HP Password Manager level of security has been configured and *all* of the security login methods are required, users must log in using all of the configured methods when the Password Manager login screen opens. This action logs the user in to Windows.

- If the HP Password Manager level of security option has been configured and *any* of the configured security login methods is permissible, users may log in using any one of the security login methods when the Password Manager login screen opens. This action logs the user in to Windows.

NOTE: If the HP Password Manager level of security has not been configured, users must still enter their Windows password at the Windows login screen, regardless of the security login methods that are required by other levels of security.

Managing passwords

Password Manager for HP ProtectTools creates and manages logons, which allow you to launch and log on to websites and programs by authenticating with your enrolled credentials.

For more information on managing passwords, refer to <u>Password Manager for HP ProtectTools on page 25</u>.

Setting credentials

You use your Security Manager Credentials to verify that you are really you. The local administrator of this computer can set up which credentials may be used to prove your identity when logging onto your Windows account, websites, or programs.

Available credentials can vary depending on the security device built in or connected to the computer. Each supported credential will have an entry in the Credentials group.

Changing your Windows password

Security Manager makes changing your Windows password simpler or quicker than doing it through the Windows Control panel.

To change your Windows password:

1. In HP ProtectTools Security Manager, click **Credentials** in the left pane.

2. Click **Windows Password**.

3. Type your current password in the **Current Windows password** box.

4. Type your new password in the **New Windows password** and **Confirm new password** boxes.

5. Click **Change**.

Setting up a Smart Card

Smart Card is an integrated part of Security Manager. Smart Card setup and configuration is used with the HP Smart Card keyboard. The Smart Card is a personal security device that protects authentication data requiring both the card and a PIN number to grant access – like using an ATM card with a PIN. The Smart Card can be used to access Password Manager, Drive Encryption PreBoot, or future third party access points. Smart Card options remain hidden until a Smart Card reader is detected.

With Smart Card security, you can accomplish the following tasks:

●   Access Smart Card Security features

●   Work with the Security Manager Setup utility to enable Smart Card authentication

●   Smart Card can be used as an authentication method in Drive Encryption preboot

●   Smart Card can be used in conjunction with other authentication methods

●   Administrative Console can initialize the PIN

Initializing the Smart Card

HP ProtectTools Security Manager can support a number of different Smart Cards. The number and type of characters used as PIN numbers may vary. The manufacturer of the Smart Card should provide tools to install a security certificate and management PIN that ProtectTools will use in its security algorithm.

NOTE: The manufacture's Smart Card software will often provide an unlock key. Most Smart Cards will lock themselves when the PIN is entered wrong 5 times. The key is used to unlock the card.

1. Once the Smart Card is set up with the manufacturer's software, insert the card into the reader.

2. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

3. In the Administrative Console, click **Devices**, click **Configure the use of the smart card**, then click the **Setup a Smart Card** tab.

4. Ensure that **Initialize the smart card** is selected.

5. Type in your **PIN** number, click the **Apply** button, then follow the onscreen instructions.

6. After the Smart Card has been successfully initialized, proceed to register the Smart Card.

Registering the Smart Card

After initializing the Smart Card, administrators can register the card as an authentication method in the Administrative Console or users can register it in Security Manager.

To register the Smart Card in the Administrative Console:

1. In the Administrative Console, click the **Setup Wizard** in the lower left corner.

2. In the **Welcome!** screen, click **Next** and enter your Windows password.

3. In the **SpareKey** window, click **Skip SpareKey Setup** (unless you want to update the SpareKey information.

4. In the **Enable security features** window, click **Next**.

5. In the **Choose your credential** window, ensure that **Smart card** is selected and click **Next**.

6. In the **Smart card** window, enter your **PIN** number and click **Next**.

7. Click **Finish**.

To register the Smart Card in Security Manager:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In Security Manager, expand **Credentials** and click **Smart Card**.

3. Enter your Windows password and **PIN** number, then click **Save**.

Managing communication privacy

Privacy Manager for HP ProtectTools enables you to use advanced security login (authentication) methods to verify the source, integrity, and security of communication when using e-mail, Microsoft Office documents, or instant messaging (IM).

For more information on Privacy Manager for HP ProtectTools, refer to Privacy Manager for HP ProtectTools on page 32.

Shredding or bleaching files

File Sanitizer for HP ProtectTools deletes files by overwriting them with meaningless data. This process, referred to as "shredding," greatly enhances information security by making the deleted files very difficult to recover. File Sanitizer further enhances information security by overwriting previously used space on the hard drive using a process referred to as "bleaching." Files deleted using File Sanitizer cannot be recovered by the Operating System or other commonly available file recovery software.

For more information on using File Sanitizer for HP ProtectTools, refer to File Sanitizer for HP ProtectTools on page 43.

Viewing drive encryption status

Drive Encryption is set up by the Windows Administrator in the Administrative Console. Users can view their encryptions status in Security Manager.

To view drive encryption status:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **Drive Encryption** > **Encryption Status**. The Encryption Status page shows if drive encryption is active or inactive and which drives are encrypted or not encrypted.

Viewing device access

Device Access is set up by the Windows Administrator in the Administrative Console. Users can view their device access setting in Security Manager.

To view device access settings:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, expand **Device Access Manager**.

3. To view which devices are denied access, click **Simple Configuration**. Devices with a check mark next to them are denied access.

4. To view which users or groups are denied access, click **Device Class Configuration**.

5. Click on a device to see which users or groups are denied or allowed access to a device.

Activating theft recovery

HP ProtectTools utilizes Computrace by Absolute Software to remotely monitor, manage, and track your computer. If your computer is lost or stolen, Absolute's Recovery Team will partner with law enforcement towards recovery.

For more information on using Computrace, refer to Computrace for HP ProtectTools on page 57.

Adding applications

Additional applications may be available to add new features to this program.

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, select the **Administration** drop-down menu and click **Discover More**.

    📝 **NOTE:**   If there is no **Discover More** link, it has been disabled by the administrator of your computer.

3. On the **Add Applications** tab, browse for additional applications.

4. On the **Updates and Messages** tab, you can stay informed about new applications and updates by clicking the **Keep me informed about new applications and updates** check box and setting a number of days to check for updates, or you can click the **Check Now** button to immediately check for updates.

Setting preferences

The Preferences page allows you to select the **Show icon on the taskbar** check box to display the Security Manager icon in the taskbar notification area (system tray).

To access the Preferences page:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **Advanced**, and then click **Preferences**.

3. Check or uncheck the **Show icon on the taskbar** check box and click **Apply**.

Backup and Restore

It is a good practice to backup your Security Manager data on a regular basis. How often you back it up depends on how often the data changes. For instance, if you regularly add new logons on a daily basis, you should probably back up your data daily.

Backups can also be used to migrate from one computer to another, also sometimes called importing and exporting. Remember though, that only the data is backed up by this feature.

If you restore the backup file to another computer, or to the same computer after reinstalling the operating system, the system must have HP ProtectTools Security Manager already installed before restoring the data from the backup file.

Backing up your data

When you back up your data, you are saving your logons and credential information to an encrypted file, protected by a password that you enter.

To back up your data:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **Advanced**, and then click **Backup and Restore**.

3. Click **Back up data**.

4. Select the modules that you want to include in the backup. In most cases, you will want to select them all. Click **Next**.

5. Enter your password to verify your identity, then click the arrow button.

6. Enter a path and name for the storage file. By default, the file will be saved to your Documents folder. Click **Browse** to specify a different location. Click **Next**.

7. Enter and confirm a password to protect the file.

8. Click **Finish**.

Restoring your data

You restore your data from a password-protected, encrypted file that was previously created through Security Manager's Backup and Restore feature.

To restore your data:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **Advanced**, and then click **Backup and Restore**.

3. Click **Restore data**.

4. Enter the path and name for the storage file or click **Browse** and select the file.

5. Enter the password used to protect the file and click **Next**.

6. Select the modules whose data you want to restore. In most cases, this would be all of the modules listed. Click **Next**.

7. Click **Finish**.

Changing your Windows user name and picture

Your Windows user name and a picture are displayed in the upper left corner of Security Manager.

To change your user name and/or picture:

1. Click on the upper left section of Security Manager with your user name and picture.

2. To change your user name, type a name in the **Windows user name** box.

3. To change your picture, click the **Choose Picture** button and browse to select a picture.

4. Click the **Save** button to save your changes.

4 Password Manager for HP ProtectTools

Logging on to Windows, websites and programs is easier and more secure when you use Password Manager.

Password Manager allows you to set up the logon screens of websites and programs for quick and secure access. First, Password Manager learns about your logons and the specific data that you type in the input boxes of each logon screen. Then, once you are at a logon screen, after verifying your identity, Password Manager fills in and submits the data automatically.

For even faster access, you can display a menu of your logons by simply using a configurable Hot key combination (Ctrl-Alt-H is the default). On the menu, simply select a logon and Password Manager will launch the website or program, navigate to the logon screen and log you in automatically.

To verify your identity you will use your HP ProtectTools credentials, such as your Windows password or smart card, depending on your computer configuration. This means that you will use the same credentials to log on to all logon screens you have set up. You can therefore create stronger passwords that you don't have to write down or remember, and keep your accounts more secure.

Password Manager lets you see at a glance whether any of your passwords are a security risk and can automatically generate a strong, complex password to use for new sites.

With Password Manager you can also view your logons, including your passwords, and edit them at any time. Many Password Manager features are also available from the Password Manager icon that displays whenever the focus is on the logon screen of a program that has been set up or on any website logon screen. Clicking on the icon displays a context menu where you can choose from among the following options.

For web pages or programs where a logon has not yet been created:

The following options are shown on the context menu.

- Add [somedomain.com] to the Password Manager - Use to add a logon for the current logon screen.

- Open Password Manager - Launches Security Manager on the Password Manager page.

- Password Manager Icon settings - Allows you to specify conditions under which the Password Manager Icon displays.

- Help - Displays online help for the Password Manager application.

For web pages or programs where a logon has already been created:

The following options are shown on the context menu.

- Fill in logon data - places your logon data in the logon fields and then submits the page (if submission was specified when the logon was created or last edited).

- Edit logon - Allows you to edit your logon data for this website.

- Add logon - Use to add another logon for the same website or program.

- Open Password Manager - Launches the Security Manager dashboard on the Password Manager page.

- Help - Displays online help for the Password Manager application.

NOTE: The administrator of the computer may have set up Security Manager to require more than one credential when verifying your identity.

Adding logons

Adding a logon for a website or program is quick and simple. You enter the logon information for the site or program once, and from then on, Password Manager automatically enters the information for you. You can use these logons after browsing to the website or program, or simply select a logon from the Logons menu to have Password Manager open the website or program and log you on.

To add a logon:

1. Open the logon screen for a website or program.

2. Click the arrow on the Password Manager icon, and then select one of the following, depending on whether the logon screen is for a website or a program.

   - For a website - select **Add [domain name] to Password Manager**.

   - For a program - select **Add this logon screen to Password Manager**.

3. Enter your logon data. Logon fields on the screen, and their corresponding fields on the dialog are identified with a bold orange border. Other options for displaying this dialog are available, such as selecting Add Logon from the Password Manager **Manage** tab. Some options depend on the security devices connected to the computer; for example using the Ctrl-H Hot Key or inserting a smart card.

   - Click the arrows to the right of a logon field to populate it with one of several preformatted choices.

   - Optionally, click **Choose other fields** to add additional fields from the screen to your logon.

   - Deselect **Submit logon data** if you want the logon fields filled in but do not want them submitted.

   - If you want to view the password for this logon, click **Show password**.

4. Click **OK**. The plus sign is removed from the Password Manager icon, letting you know that the logon has been created.

5. Enter the Windows password and click the green arrow.

Now, every time that you go to that website or launch that program, the Password Manager icon will appear, indicating that you can use your registered credential(s) to log on.

Editing logons

To edit a logon:

1. Open the logon screen for a website or program.

2. Click the arrow on the Password Manager icon, and select **Edit logon** to display a dialog where you can edit your logon information. Logon fields on the screen, and their corresponding fields on the dialog, are identified with a bold orange border.

3. Enter the Windows password and click the green arrow.

4. Edit your logon information.

- Click the arrows to the right of a logon field to populate it with one of several preformatted choices.

- Optionally, click **Choose other fields** to add additional fields from the screen to your logon.

- Deselect **Submit account data** if you want the logon fields filled in but do not want them submitted.

- If you want to view the password for this logon, click Show password. The Windows password is required to see the password.

5. Click **OK**.

Using the Logons menu

Password Manager provides a fast, easy way to launch the websites and programs that you have created logons for. Simply double-clicking a program or website logon from the Logons menu, or on the **Manage** tab in Password Manager, will launch its logon screen and fill in your logon data. By default, the information is also immediately submitted to the website, although you can choose not to do so by deselecting **Submit account data** when initially setting up or editing the logon.

When you create a logon, it is automatically added to your Password Manager Logons menu.

To display the Logons menu, press the Password Manager Hot Key combination. Ctrl+Win+H is the default, but you can change the Hot Key combination from **Password Manager** > Windows password > green arrow > **Settings**.

Organizing logons into categories

Use categories to keep your logons in order. It's a simple matter of creating one or more categories and drag-and-dropping your logons into the desired categories.

To add a category:

1. In the Security Manager left pane, select **Password Manager**.

2. Select the **Manage** tab, and click **Add Category**.

3. Enter a name for the category.

4. Click **OK**.

To add a logon to a category:

1. Place your mouse pointer over the desired logon.

2. Press and hold the left mouse button.

3. Drag the logon into the list of categories. Categories will become highlighted as you move your mouse over them.

4. Release the mouse button when the desired category is highlighted.

Your logons are not moved to the category, but only copied to the selected category. That means that you can add the same logon to more than one category. And, you can always see all of your logon by clicking **All**.

Managing your logons

Password Manager makes managing your logon information - user names, passwords and multiple logon accounts - painless and intuitive, from one central location.

Your logons are listed on the **Manage** tab. Whenever multiple logons have been created for the same website, each logon is then listed under the website name and indented in the logon list.

To manage your logons:

In the Security Manager left pane, select **Password Manager** and click the **Manage** tab. Open the web site you want to edit.

● Add a logon - Click **Add Logon** and follow the on-screen instructions.

● Edit a logon - Select a logon and click **Edit**. Then change the logon data as desired.

● Delete a logon - Select a logon and click **Delete**.

To add an additional logon for a website or program:

1. Launch the logon screen for the website or program.

2. Click the Password Manager icon to display its shortcut menu.

3. Select **Add additional logon** and follow the on-screen instructions.

Assessing your password strength

Using strong passwords for logon to your websites and programs is an important aspect of protecting your identity.

Password Manager makes monitoring and improving your security easy with instant and automated analysis of the strength of each of the passwords used to log on to your to websites and programs. You can check the strength of the passwords you use for your logons on the Password Manager **Password Strength** tab.

Password Manager Icon settings

Password Manager attempts to identify logon screens for websites and programs. When it finds a logon screen that you have not created a logon for, Password Manager will prompt you to add a logon for the screen by displaying the Password Manager icon with a "+" sign.

The following settings are configurable:

● Always prompt - Select this option to have Password Manager prompt you to add a logon whenever a logon screen displays that does not already have a logon set up for it.

● Do not prompt for this screen - Select this option so that Password Manager will not prompt you again to add a logon for this specific logon screen.

● Never prompt - Select this option to ensure that Password Manager never prompts you for logon screens that have not been set up.

Additional Privacy Manager settings are available by selecting **Password Manager** > Windows password > green arrow > **Settings** in Security Manager.

5   Drive Encryption for HP ProtectTools

In today's world, a computer belonging to you or anyone on your staff could be stolen, and critical information about your company could be seriously compromised. Encrypting everything on your computer hard drive makes it unreadable and inaccessible to any unauthorized person who might try to access it even if the drive has been removed from the computer or sent to a data recovery service.

Drive Encryption for HP ProtectTools software is the industry's first full volume encryption capability to be provided out-of-the-box. It provides complete data protection by encrypting your hard drive. When Drive Encryption is activated, you must log in at the Drive Encryption login screen, which is displayed before Windows starts up.

NOTE: Drive Encryption for HP ProtectTools can be enabled through the Setup Wizard in the HP ProtectTools Administrative Console only.

NOTE: Drive Encryption is not supported on 64 bit operating systems when configured with RAID on systems that use an AMD processor.

Drive Encryption:

- Allows you to encrypt everything on your internal hard drives

- Gives you easy password access and pre-boot authentication

- Supports Microsoft Windows XP, Windows Vista, and Windows 7

- Makes use of the Trusted Platform Module (TPM) embedded security chip if equipped and configured with TPM

Various tasks can be performed in Drive Encryption for HP ProtectTools:

- Manage Drive Encryption

    ◦ Activate a TPM-protected password

    ◦ Encrypt or decrypt individual drives

    ◦ Activate a self encrypting drive (SED)

- Backup and Recovery

    ◦ Create backup keys

    ◦ Register for online recovery

    ◦ Manage an existing online recovery account

    ◦ Perform a recovery

CAUTION: If you decide to uninstall the Drive Encryption module or if you are using a backup and restore solution, you must first decrypt all encrypted drives. If you do not, you will not be able to access the data on encrypted drives unless you have registered with the Drive Encryption recovery service. Reinstalling the Drive Encryption module will not enable you to access the encrypted drives.

Setup procedures

Opening Drive Encryption

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. Click **Drive Encryption**.

General tasks

Activating Drive Encryption

Use the HP ProtectTools Administrative Console Setup Wizard to activate Drive Encryption.

Deactivating Drive Encryption

Use the HP ProtectTools Administrative Console Setup Wizard to deactivate Drive Encryption.

Logging in after Drive Encryption is activated

When you turn on the computer after Drive Encryption is activated and your user account is enrolled, you must log in at the Drive Encryption logon screen:

NOTE: If the Windows administrator has enabled Pre-boot Security in the HP ProtectTools Administrative Console, you will log in to the computer immediately after the computer is turned on, rather than at the Drive Encryption logon screen.

1. Select your user name, and then type your Windows password or Smart Card PIN.

2. Click **OK**.

NOTE: If you use a recovery key to log in at the Drive Encryption logon screen, you will also be prompted to select your Windows user name and type your password at the Windows logon screen.

Advanced tasks

Managing Drive Encryption (administrator task)

The Drive Encryption window allows Windows administrators to view and change the status of Drive Encryption (active or inactive) and to view the encryption status of all of the hard drives on the computer.

Activating a TPM-protected password

Use Embedded Security for HP ProtectTools to activate the TPM. After activation, logging in at the Drive Encryption logon screen requires the Windows user name and password.

NOTE: Because the password is protected by a TPM security chip, if the hard drive is moved to another computer, data cannot be accessed unless the TPM settings are migrated to that computer.

1. Use Embedded Security for HP ProtectTools to activate the TPM.

2. In the Administrative Console left pane, expand **Drive Encryption**, and click **Encryption Management**.

3. Select the **Enhance security with TPM** check box.

Encrypting or decrypting individual drives

1. In the Administrative Console left pane, expand **Drive Encryption**, and click **Encryption Management**.

2. Click the **Change Encryption** button.

3. In the Change Encryption dialog box, select or clear the check box next to each hard drive you want to encrypt or decrypt, and then click **OK**.

NOTE: When the drive is being encrypted or decrypted, the progress bar shows the time remaining to complete the process during the current session. If the computer is shut down or initiates Sleep or Hibernation during the encryption process and then restarts, the Time Remaining display resets to the beginning, but the actual encryption resumes where it last stopped. The time remaining and progress display will change more quickly to reflect the previous progress.

Backup and recovery (administrator task)

The Drive Encryption: Backup and Recovery window allows Windows administrators to back up and recover encryption keys.

Creating backup keys

CAUTION: Be sure to keep the storage device containing the backup key in a safe place, because if you forget your password or lose your Smart Card, this device provides your only access to your hard drive.

1. In the Administrative Console left pane, expand **Drive Encryption**, and click **Backup and Recovery**.

2. Click the **Backup Keys** button.

3. On the "Select Backup Disk" page, click the name of the device where you want to back up your encryption key, and then click **Next**.

4. Read the information on the next page that is displayed, and then click **Next**.

   The encryption key is saved on the storage device you selected.

5. Click **OK** when the confirmation dialog box opens.

NOTE: Refer to the Drive Encryption for HP ProtectTools Help file for information on managing and performing a recovery.

6   Privacy Manager for HP ProtectTools

Privacy Manager is a tool used to obtain Certificates of Authority, which verify the source, integrity, and security of communication when using Microsoft mail, Microsoft Office documents, and Instant Messenger.

Privacy Manager leverages the security infrastructure provided by HP ProtectTools Security Manager, which includes the following security logon methods:

- Windows password
- Smart card

You may use any of the above security logon methods in Privacy Manager.

Opening Privacy Manager

To open Privacy Manager:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **Privacy Manager**.

– or –

Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, highlight **Privacy Manager for HP ProtectTools**, and then click **Configuration**.

– or –

On the toolbar of a Microsoft Outlook e-mail message, click the down arrow next to **Send Securely**, and then click **Certificate Manager** or **Trusted Contact Manager**.

– or –

On the toolbar of a Microsoft Office document, click the down arrow next to **Sign and Encrypt**, and then click **Certificate Manager** or **Trusted Contact Manager**.

Setup procedures

Managing Privacy Manager Certificates

Manager Certificates protect data and messages using a cryptographic technology called public key infrastructure (PKI). PKI requires users to obtain cryptographic keys and a Privacy Manager Certificate issued by a certificate authority (CA). Unlike most data encryption and authentication software that only requires you to authenticate periodically, Privacy Manager requires authentication each time you sign an e-mail message or a Microsoft Office document using a cryptographic key. Privacy Manager makes the process of saving and sending your important information safe and secure.

Requesting and installing a Privacy Manager Certificate

Before you can use the Privacy Manager features, you must request and install a Privacy Manager Certificate (from within Privacy Manager) using a valid e-mail address. The e-mail address must be

set up as an account within Microsoft Outlook on the same computer from which you are requesting the Privacy Manager Certificate.

Requesting a Privacy Manager Certificate

1. In the Security Manager left pane, expand **Privacy Manager**, and click **Certificates**.

2. Click the **Request a Privacy Manager certificate** button.

3. On the "Welcome" page, read the text, and then click **Next**.

4. On the "License Agreement" page, read the license agreement.

5. Be sure that the check box next to **Check here to accept the terms of this license agreement** is selected, and then click **Next**.

6. On the "Your Certificate Details" page, enter the required information, and then click **Next**.

7. On the "Certificate Request Accepted" page, click **Finish**.

   You will receive an e-mail in Microsoft Outlook with your Privacy Manager Certificate attached.

Installing a Privacy Manager Certificate

1. When you receive the e-mail with your Privacy Manager Certificate attached, open the e-mail and click the **Setup** button, in the lower-right corner of the message.

2. Authenticate using your chosen security logon method.

3. On the "Certificate Installed" page, click **Next**.

4. On the "Certificate Backup" page, enter a location and name for the backup file, or click **Browse** to search for a location.

   △ **CAUTION:** Be sure that you save the file to a location other than your hard drive and put it in a safe place. This file should be for your use only, and is required in case you need to restore your Privacy Manager Certificate and associated keys.

5. Enter and confirm a password, and then click **Next**.

6. Authenticate using your chosen security logon method.

7. If you choose to begin the Trusted Contact invitation process, follow the on-screen instructions.

   – or –

   If you click Cancel, refer to Managing Trusted Contacts for information on adding a Trusted Contact at a later time.

Viewing Privacy Manager Certificate details

1. In the Security Manager left pane, expand **Privacy Manager** and click **Certificate Manager**.

2. Click a **Privacy Manager Certificate**.

3. Click **Certificate details**.

4. When you have finished viewing the details, click **OK**.

Renewing a Privacy Manager Certificate

When your Privacy Manager Certificate nears expiration, you will be notified that you need to renew it:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Certificate Manager**.

2. Click a **Privacy Manager Certificate**.

3. Click **Renew certificate**.

4. Follow the on-screen instructions to purchase a new Privacy Manager Certificate.

    NOTE: The Privacy Manager Certificate renewal process does not replace your old Privacy Manager Certificate. You will need to purchase a new Privacy Manager Certificate and install it using the same procedures as in Requesting and installing a Privacy Manager Certificate.

Setting a default Privacy Manager Certificate

Only Privacy Manager Certificates are visible from within Privacy Manager, even if additional certificates from other certificate authorities are installed on your computer.

If you have more than one Privacy Manager Certificate on your computer that was installed from within Privacy Manager, you can specify one as the default certificate:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Certificate Manager**.

2. Click the Privacy Manager Certificate that you want to use as the default, and then click **Set default**.

3. Click **OK**.

NOTE: You are not required to use your default Privacy Manager Certificate. From within the various Privacy Manager functions, you can select any of your Privacy Manager Certificates to use.

Deleting a Privacy Manager Certificate

If you delete a Privacy Manager Certificate, you cannot open any files or view any data that you encrypted with that certificate. If you have accidentally deleted a Privacy Manager Certificate, you can restore it using the backup file that you created when you installed the certificate.

To delete a Privacy Manager Certificate:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Certificate Manager**.

2. Click the Privacy Manager Certificate you want to delete, and then click **Advanced**.

3. Click **Delete**.

4. When the confirmation dialog box opens, click **Yes**.

5. Click **Close**, and then click **Apply**.

Restoring a Privacy Manager Certificate

If you have accidentally deleted a Privacy Manager Certificate, you can restore it using the backup file that you created when you installed or exported the certificate:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Migration**.

2. Click the **Restore** button.

3. On the "Migration File" page, click **Browse** to search for the .dppsm file that you created when you installed or exported the Privacy Manager Certificate, and then click **Next**.

4. On the "Migration File Import" page, click **Finish**.

5. Click **Close**, and then click **Apply**.

NOTE: Refer to Installing a Privacy Manager Certificate or Exporting Privacy Manager Certificates and Trusted Contacts for more information.

Revoking your Privacy Manager Certificate

If you feel that the security of your Privacy Manager Certificate has been jeopardized, you may revoke your own certificate:

NOTE: A revoked Privacy Manager Certificate is not deleted. The certificate can still be used to view files that are encrypted.

1. In the Security Manager left pane, expand **Privacy Manager** and click **Certificate Manager**.

2. Click **Advanced**.

3. Click the Privacy Manager Certificate you want to revoke, and then click **Revoke**.

4. When the confirmation dialog box opens, click **Yes**.

5. Authenticate using your chosen security logon method.

6. Follow the on-screen instructions.

Managing Trusted Contacts

Trusted Contacts are users with whom you have exchanged Privacy Manager Certificates, enabling you to securely communicate with one another.

Adding Trusted Contacts

1. You send an e-mail invitation to a Trusted Contact recipient.

2. The Trusted Contact recipient responds to the e-mail.

3. You receive the e-mail response from the Trusted Contact recipient, and click **Accept**.

You can send Trusted Contact e-mail invitations to individual recipients or you can send the invitation to all the contacts in your Microsoft Outlook address book.

NOTE: To respond to your invitation to become a Trusted Contact, Trusted Contact recipients must have Privacy Manager installed on their computers or have the alternate client installed. For information on installing the alternate client, access the DigitalPersona website at http://DigitalPersona.com/PrivacyManager.

Adding a Trusted Contact

1. In the Security Manager left pane, expand **Privacy Manager** and click **Trusted Contacts**, and then click the **Invite Contacts** button.

   – or –

   In Microsoft Outlook, click the down arrow next to **Send Securely** on the toolbar, and then click **Invite Contacts**.

2. If the Select Certificate dialog box opens, click the Privacy Manager Certificate you want to use, and then click **OK**.

3. When the Trusted Contact Invitation dialog box opens, read the text, and then click **OK**.

   An e-mail is automatically generated.

4. Enter one or more e-mail addresses of the recipients you want to add as Trusted Contacts.

5. Edit the text and sign your name (optional).

6. Click **Send**.

   NOTE: If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click OK to launch the Certificate Request Wizard.

7. Authenticate using your chosen security logon method.

8. When you receive an e-mail response from a recipient accepting the invitation to become a Trusted Contact, click Accept in the lower-right corner of the e-mail.

   A dialog box opens, confirming that the recipient has been successfully added to your Trusted Contacts list.

9. Click **OK**.

Adding Trusted Contacts using your Microsoft Outlook address book

1. In the Security Manager left pane, expand **Privacy Manager**, click **Trusted Contacts**, and then click the **Invite Contacts** button.

   – or –

   In Microsoft Outlook, click the down arrow next to **Send Securely** on the toolbar, and then click **Invite All My Outlook Contacts**.

2. When the "Trusted Contact Invitation" page opens, select the e-mails address of the recipients you want to add as Trusted Contacts and then click **Next**.

3. When the "Sending Invitation" page opens, click **Finish**.

   An e-mail listing the selected Microsoft Outlook e-mail addresses is automatically generated.

4. Edit the text and sign your name (optional).

5. Click **Send**.

   NOTE: If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click **OK** to launch the Certificate Request Wizard.

6. Authenticate using your chosen security logon method.

7. When you receive an e-mail response from a recipient accepting the invitation to become a Trusted Contact, click Accept in the lower-right corner of the e-mail.

    A dialog box opens, confirming that the recipient has been successfully added to your Trusted Contacts list.

8. Click **OK**.

Viewing Trusted Contact details

1. In the Security Manager left pane, expand **Privacy Manager** and click **Trusted Contacts Manager**.

2. Click a Trusted Contact.

3. Click **Contact details**.

4. When you have finished viewing the details, click **OK**.

Deleting a Trusted Contact

1. In the Security Manager left pane, expand **Privacy Manager** and click **Trusted Contacts Manager**.

2. Click the Trusted Contact you want to delete.

3. Click **Delete contact**.

4. When the confirmation dialog box opens, click **Yes**.

Checking revocation status for a Trusted Contact

1. In the Security Manager left pane, expand **Privacy Manager** and click **Trusted Contacts Manager**.

2. Click a Trusted Contact.

3. Click the **Advanced** button.

    The Advanced Trusted Contact Management dialog box opens.

4. Click **Check Revocation**.

5. Click **Close**.

General tasks

Using Privacy Manager in Microsoft Office

After you install your Privacy Manager Certificate, a Sign and Encrypt button is displayed on the right side of the toolbar of all Microsoft Office 2007 Word, Excel, and PowerPoint documents.

NOTE: If you are using Microsoft Office 2007, you must have all the Microsoft updates applied otherwise some signed e-mails will go into the Junk E-mail folder.

Configuring Privacy Manager in a Microsoft Office document

1. Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, highlight **File Sanitizer**, and then click **Shred Now**.

2. When the confirmation dialog box opens, click **Yes**.

– or –

1. In the Security Manager left pane, expand **Privacy Manager** and click **Settings**, and then click the **Documents** tab.

   – or –

   On the toolbar of a Microsoft Office document, click the down arrow next to **Sign and Encrypt**, and then click **Settings**.

2. Select the actions you want to configure, and then click **OK**.

Signing a Microsoft Office document

1. In Microsoft Word, Microsoft Excel, or Microsoft PowerPoint, create and save a document.

2. Click the down arrow next to **Sign and Encrypt**, and then click **Sign Document**.

3. Authenticate using your chosen security logon method.

4. When the confirmation dialog box opens, read the text, and then click **OK**.

If you later decide to edit the document, follow these steps:

1. Click the **Office** button in the upper-left corner of the screen.

2. Click **Prepare**, and then click **Mark as Final**.

3. When the confirmation dialog box opens, click **Yes**, and continue working.

4. When you have completed your editing, sign the document again.

Adding a signature line when signing a Microsoft Word or Microsoft Excel document

Privacy Manager allows you to add a signature line when you sign a Microsoft Word or Microsoft Excel document:

1. In Microsoft Word or Microsoft Excel create and save a document.

2. Click the **Home** menu.

3. Click the down arrow next to **Sign and Encrypt**, and then click **Add Signature Line Before Signing**.

   NOTE: A check mark is displayed next to Add Signature Line Before Signing when this option is selected. By default, this option is enabled.

4. Click the down arrow next to **Sign and Encrypt**, and then click **Sign Document**.

5. Authenticate using your chosen security logon method.

Adding suggested signers to a Microsoft Word or Microsoft Excel document

You can add more than one signature line to your document by appointing suggested signers. A suggested signer is a user who is designated by the owner of a Microsoft Word or Microsoft Excel document to add a signature line to the document. Suggested signers can be you or another person who you want to sign your document. For example, if you prepare a document that needs to be signed by all members of your department, you can include signature lines for those users at the bottom of the final page of the document with instructions to sign by a specific date.

To add a suggested signer to a Microsoft Word or Microsoft Excel document:

1. In Microsoft Word or Microsoft Excel, create and save a document.

2. Click the **Insert** menu.

3. In the **Text** group on the toolbar, click the arrow next to **Signature Line**, and then click **Privacy Manager Signature Provider**.

   The Signature Setup dialog box opens.

4. In the box under **Suggested signer**, enter the name of the suggested signer.

5. In the box under **Instructions to the signer**, enter a message for this suggested signer.

   📝 **NOTE:** This message will appear in place of a title, and is either deleted or replaced by the user's title when the document is signed.

6. Select the **Show sign date in signature line** check box to show the date.

7. Select the **Show signer's title in signature line** check box to show the title.

   📝 **NOTE:** Because the owner of the document assigns suggested signers to his or her document, if the **Show sign date in signature line** and/or **Show signer's title in signature line** check boxes are not selected, the suggested signer will not be able to display the date and/or title in the signature line even if the suggested signer's document settings are configured to do so.

8. Click **OK**.

Adding a suggested signer's signature line

When suggested signers open the document, they will see their name in brackets, indicating that their signature is required.

To sign the document:

1. Double-click the appropriate signature line.

2. Authenticate using your chosen security logon method.

   The signature line will be shown according to the settings specified by the owner of the document.

Encrypting a Microsoft Office document

You can encrypt a Microsoft Office document for you and for your Trusted Contacts. When you encrypt a document and close it, you and the Trusted Contact(s) you select from the list must authenticate before opening it.

To encrypt a Microsoft Office document:

1. In Microsoft Word, Microsoft Excel, or Microsoft PowerPoint, create and save a document.

2. Click the **Home** menu.

3. Click the down arrow next to **Sign and Encrypt**, and then click **Encrypt Document**.

   The Select Trusted Contacts dialog box opens.

4. Click the name of a Trusted Contact who will be able to open the document and view its contents.

   📝 **NOTE:** To select multiple Trusted Contact names, hold down the Ctrl key and click the individual names.

5. Click **OK**.

6. Authenticate using your chosen security logon method.

If you later decide to edit the document, follow the steps in **Signing a Microsoft Office Document**. When the encryption is removed, you can edit the document. Follow the steps in this section to encrypt the document again.

Removing the encryption from a Microsoft Office document

When you remove encryption from a Microsoft Office document, you and your Trusted Contacts are no longer required to authenticate to open and view the contents of the document.

To remove encryption from a Microsoft Office document:

1. Open an encrypted Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document.

2. Authenticate using your chosen security logon method.

3. Click the **Home** menu.

4. Click the down arrow next to **Sign and Encrypt**, and then click **Remove Encryption**.

Sending an encrypted Microsoft Office document

You may attach an encrypted Microsoft Office document to an e-mail message without signing or encrypting the e-mail itself. To do this, create and send an e-mail with a signed or encrypted document just as you normally would a regular e-mail with an attachment.

However, for optimum security, it is recommended that you encrypt the e-mail when attaching a signed or encrypted Microsoft Office document.

To send a sealed e-mail with an attached signed and/or encrypted Microsoft Office document, follow these steps:

1. In Microsoft Outlook, click **New** or **Reply**.

2. Type your e-mail message.

3. Attach the Microsoft Office document.

4. Refer to Sealing and sending an e-mail message for further instructions.

Viewing a signed Microsoft Office document

NOTE: You do not need to have a Privacy Manager Certificate in order to view a signed Microsoft Office document.

When a signed Microsoft Office document is opened, a Signatures dialog box opens next to the document, displaying the name of the user who signed the document and the date it was signed. You can right-click the name to view additional details.

Viewing an encrypted Microsoft Office document

To view an encrypted Microsoft Office document from another computer, Privacy Manager must be installed on that computer. In addition, you must import the Privacy Manager Certificate that was used to encrypt the file.

A Trusted Contact wanting to view an encrypted Microsoft Office document must have a Privacy Manager Certificate, and Privacy Manager must be installed on his or her computer. In addition, the Trusted Contact must be selected by the owner of the encrypted Microsoft Office document.

Using Privacy Manager in Microsoft Outlook

When Privacy Manager is installed, a Privacy button is displayed on the Microsoft Outlook toolbar, and a Send Securely button is displayed on the toolbar of each Microsoft Outlook e-mail message.

📝 **NOTE:** If you are using Microsoft Office 2007, you must have all the Microsoft updates applied otherwise some signed e-mails will go into the Junk E-mail folder.

Configuring Privacy Manager for Microsoft Outlook

1. In the Security Manager left pane, expand **Privacy Manager** and click **Settings**, and then click the **E-mail** tab.

    – or –

    On the main Microsoft Outlook toolbar, click the down arrow next to **Privacy**, and then click **Settings**.

    – or –

    On the toolbar of a Microsoft e-mail message, click the down arrow next to **Send Securely**, and then click **Settings**.

2. Select the actions you want to perform when you send a secure e-mail, and then click **OK**.

Signing and sending an e-mail message

1. In Microsoft Outlook, click **New** or **Reply**.

2. Type your e-mail message.

3. Click the down arrow next to **Send Securely**, and then click **Sign and Send**.

4. Authenticate using your chosen security logon method.

Sealing and sending an e-mail message

Sealed e-mail messages that are digitally signed and sealed (encrypted) can only be viewed by people you choose from your Trusted Contacts list.

To seal and send an e-mail message to a Trusted Contact:

1. In Microsoft Outlook, click **New** or **Reply**.

2. Type your e-mail message.

3. Click the down arrow next to **Send Securely**, and then click **Seal for Trusted Contacts and Send**.

4. Authenticate using your chosen security logon method.

Viewing a sealed e-mail message

When you open a sealed e-mail message, the security label is displayed in the heading of the e-mail. The security label provides the following information:

● Which credentials were used to verify the identity of the person who signed the e-mail

● The product that was used to verify the credentials of the person who signed the e-mail

Advanced tasks

Migrating Privacy Manager Certificates and Trusted Contacts to a different computer

You can securely migrate your Privacy Manager Certificates and Trusted Contacts to a different computer. To do this, export them as a password-protected file to a network location or any removable storage device, and then import the file to the new computer.

Exporting Privacy Manager Certificates and Trusted Contacts

To export your Privacy Manager Certificates and Trusted Contacts to a password-protected file, follow these steps:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Migration**.

2. Click **Export migration file**.

3. On the "Select Data" page, select the data categories to be included in the migration file, and then click **Next**.

4. On the "Migration File" page, enter a file name or click **Browse** to search for a location, and then click **Next**.

5. Enter and confirm a password, and then click **Next**.

   📝 **NOTE:** Store this password in a safe place, because you will need it when you import the migration file.

6. Authenticate using your chosen security logon method.

7. On the "Migration File Saved" page, click **Finish**.

Importing Privacy Manager Certificates and Trusted Contacts

To import your Privacy Manager Certificates and Trusted Contacts to a password-protected file, follow these steps:

1. In the Security Manager left pane, expand **Privacy Manager** and click **Migration**.

2. Click **Import migration file**.

3. On the "Select Data" page, select the data categories to be included in the migration file, and then click **Next**.

4. On the "Migration File" page, enter a file name or click **Browse** to search for a location, and then click **Next**.

5. On the "Migration File Import" page, click **Finish**.

7 File Sanitizer for HP ProtectTools

File Sanitizer is a tool that allows you to securely erase critical files and folders (personal information or files, historical or Web-related data, or other data components) on your computer and periodically bleach your hard drive.

NOTE: File Sanitizer currently operates only on the hard drive.

About shredding

Deleting an asset in Windows does not completely remove the contents of the asset from your hard drive. Windows only deletes the reference to the asset. The content of the asset still remains on the hard drive until another asset overwrites that same area on the hard drive with new information.

Shredding is different than a standard Windows delete (also known as a simple delete in File Sanitizer) in that when you shred an asset, an algorithm that obscures the data is invoked, which makes it virtually impossible to retrieve the original asset.

When you choose a shred profile (High Security, Medium Security, or Low Security), a predefined list of assets and an erase method are automatically selected for shredding. You can also customize a shred profile, which allows you to specify the number of shred cycles, which assets to include for shredding, which assets to confirm before shredding, and which assets to exclude from shredding.

You can set up an automatic shred schedule, and you can also manually shred assets whenever you want.

About free space bleaching

Free space bleaching allows you to securely write random data over deleted assets, preventing users from viewing the original contents of the deleted asset.

NOTE: Free space bleaching is for those assets that you delete using the Windows Recycle Bin or when you manually delete an asset. Free space bleaching provides no additional security to shredded assets.

You can set an automatic free space bleaching schedule or you can manually activate free space bleaching using the HP ProtectTools icon in the notification area, at the far right of the taskbar.

Setup procedures

Opening File Sanitizer

To open File Sanitizer:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the Security Manager left pane, click **File Sanitizer**.

   – or –

● Double-click the **File Sanitizer** icon.

   – or –

● Right-click the HP ProtectTools icon in the notification area, at the far right of the taskbar, highlight **File Sanitizer**, and then click **Open File Sanitizer**.

Setting a free space bleaching schedule

NOTE: Free space bleaching is for those assets that you delete using the Windows Recycle Bin or for manually deleted assets. Free space bleaching provides no additional security to shredded assets.

To set a free space bleaching schedule:

1. In the Security Manager left pane, expand **File Sanitizer** and click **Bleaching**.

2. Select the **Activate Scheduler** check box, enter your Windows password, and then enter a day and time to bleach your hard drive.

3. Click the **Save** icon.

   NOTE: The free space bleaching operation can take a long time. Even though free space bleaching is performed in the background, your computer may run slower due to increased processor usage.

Setting a shred schedule

1. In the Security Manager left pane, expand **File Sanitizer** and click **Shred**.

2. Select a shred option:

   ● **Windows shutdown** — Choose this option to shred all selected assets when Windows shuts down.

      NOTE: When this option is selected, a dialog box is displayed at shutdown asking if you want to continue with shredding the selected assets or if you want to bypass the procedure. Click Yes to bypass the shred procedure or click No to continue with shredding. The Yes or No option must be selected quickly because Windows will close the software in preparation for shutting down and produce an error. If you select No in order to continue shredding, Windows may produce an error screen indicating that File Sanitizer is not responding. Allow File Sanitizer to complete the shred, then initiate the shutdown again.

   ● **Web browser open** — Choose this option to shred all selected Web-related assets, such as browser URL history, when you open a Web browser.

   ● **Web browser quit** — Choose this option to shred all selected Web-related assets, such as browser URL history, when you close a Web browser.

   ● **Key sequence** — Choose this option to initiate shredding using a key sequence.

   ● **Scheduler** — Select the Activate Scheduler check box, enter your Windows password, and then enter a day and time to shred selected assets.

3. Click the **Save** icon.

Selecting or creating a shred profile

You can specify a method of erasure and select the assets to shred by selecting a predefined profile or by creating your own profile.

Selecting a predefined shred profile

When you choose a predefined shred profile (High Security, Medium Security, or Low Security), a predefined erasure method and list of assets are automatically selected. You can click the View Details button to view the predefined list of assets that are selected for shredding.

To select a predefined shred profile:

1. In the Security Manager left pane, expand **File Sanitizer** and click **Settings**.

2. Click a predefined shred profile.

3. Click **View Details** to view the list of assets that are selected for shredding.

4. Under **Shred the following**, select the check box next to each asset that you want to confirm before shredding.

5. Click **Apply**.

Customizing an advanced security shred profile

When you create a shred profile, you specify the number of shred cycles, which assets to include for shredding, which assets to confirm before shredding, and which assets to exclude from shredding:

1. In the Security Manager left pane, expand **File Sanitizer**, click **Settings**, select **Advanced Security Settings**, and then click **View Details**.

2. Specify the number of shred cycles.

   📝 **NOTE:** The selected number of shredding cycles will be performed for each asset. For example, if you choose 3 shred cycles, an algorithm that obscures the data is executed 3 different times. If you choose the higher security shred cycles, shredding may take a significant length of time; however, the higher the number of shred cycles you specify, the more secure the computer is.

3. Select the assets you want to shred:

   a. Under **Available shred options**, click an asset, and then click **Add**.

   b. To add a custom asset, click **Add Custom Option**, enter or browse to a file name or folder name, and then click **OK**. Click the custom asset, and then click **Add**.

      📝 **NOTE:** To delete an asset from the available shred options, click the asset, and then click **Delete**.

4. Under **Shred the following**, select the check box next to each asset that you want to confirm before shredding.

   📝 **NOTE:** To remove an asset from the shred list, click the asset, and then click **Remove**.

5. Under **Do not shred the following**, click **Add** to select the specific assets that you want to exclude from shredding.

6. When you finish configuring the shred profile, click **Apply**.

Customizing a simple delete profile

The simple delete profile performs a standard asset delete without shredding. When you customize a simple delete profile, you specify which assets to include for a simple delete, which assets to confirm before a simple delete is executed, and which assets to exclude from a simple delete:

📝 **NOTE:** It is highly recommended that you run free space bleaching regularly if you use the simple delete option.

1. In the Security Manager left pane, expand **File Sanitizer**, click **Settings**, select **Simple Delete Settings**, and then click **View Details**.

2. Select the assets you want to delete:

   a. Under **Available delete options**, click an asset, and then click **Add**.

   b. To add a custom asset, click **Add Custom Option**, enter or browse to a file name or folder name, and then click **OK**. Click the custom asset, and then click **Add**.

   📝 **NOTE:** To delete an asset from the available delete options, click the asset, and then click **Delete**.

3. Under **Delete the following**, select the check box next to each asset that you want to confirm before deleting.

   📝 **NOTE:** To remove an asset from the delete list, click the asset, and then click **Remove**

4. Under **Do not delete the following**, click **Add** to select the specific assets that you want to exclude from shredding.

5. When you finish configuring the simple delete profile, click **Apply**.

General tasks

Using a key sequence to initiate shredding

To specify a key sequence, follow these steps:

1. In the Security Manager left pane, expand **File Sanitizer** and click **Shred**.

2. Select the **Key sequence** check box.

3. Enter a character in the available box, and then select the **CTRL**, **ALT**, or **SHIFT** box, or select all three.

   For example, to initiate automatic shredding using the S key and Ctrl+Shift, enter S in the box, and then select the **CTRL** and **SHIFT** options.

📝 **NOTE:** Be sure to select a key sequence that is different from other key sequences you have configured.

To initiate shredding using a key sequence:

1. Hold down the Ctrl, Alt, or Shift key (or whichever combination you specified) while pressing your chosen character.

2. If a confirmation dialog box opens, click **Yes**.

Using the File Sanitizer icon

⚠ **CAUTION:** Shredded assets cannot be recovered. Carefully consider which items you select for manual shredding.

1. Navigate to the document or folder you want to shred.

2. Drag the asset to the File Sanitizer icon on the desktop.

3. When the confirmation dialog box opens, click **Yes**.

Manually shredding one asset

⚠ **CAUTION:**   Shredded assets cannot be recovered. Carefully consider which items you select for manual shredding.

1. Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, highlight **File Sanitizer**, and then click **Shred One**.

2. When the Browse dialog box opens, navigate to the asset you want to shred, and then click **Open**.

    📝 **NOTE:**   The asset you select can be a single file or folder.

3. When the confirmation dialog box opens, click **Yes**.

    – or –

1. Right-click the **File Sanitizer** icon on the desktop, and then click **Shred One**.

2. When the Browse dialog box opens, navigate to the asset you want to shred, and then click **OK**.

3. When the confirmation dialog box opens, click **Yes**.

– or –

1. In the Security Manager left pane, expand **File Sanitizer** and click **Shred**.

2. Click the **Browse** button.

3. When the Browse dialog box opens, navigate to the asset you want to shred, and then click **Open**.

4. When the confirmation dialog box opens, click **Yes**.

Manually shredding all selected items

1. Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, highlight **File Sanitizer**, and then click **Shred Now**.

2. When the confirmation dialog box opens, click **Yes**.

    – or –

1. Right-click the **File Sanitizer** icon on the desktop, and then click **Shred Now**.

2. When the confirmation dialog box opens, click **Yes**.

Manually activating free space bleaching

1. Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, highlight **File Sanitizer**, and then click **Bleach Now**.

2. A notification bubble will appear verifying that a bleach operation has begun.

– or –

1. In the Security Manager left pane, expand **File Sanitizer** and click **Bleaching**.

2. Click **Bleach Now**.

3. A notification bubble will appear verifying that a bleach operation has begun.

Aborting a shred or free space bleaching operation

When a shred or free space bleaching operation is in progress, a message above the HP ProtectTools Security Manager icon in the notification area is displayed. The message provides details on the shred or free space bleaching process (percentage complete), and gives you the option to abort the operation.

To abort the operation:

▲ Click the message, and then click **Stop** to cancel the operation.

Viewing the log files

Each time a shred or free space bleaching operation is performed, log files of any errors or failures are generated. The log files are always updated according to the latest shred or free space bleaching operation.

NOTE: Files that are successfully shredded or bleached do not appear in the log files.

One log file is created for shred operations and another log file is created for free space bleaching operations. Both log files are located on the hard drive at:

● C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_ShredderLog.txt

● C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_DiskBleachLog.txt

8 Embedded Security for HP ProtectTools

NOTE: The integrated Trusted Platform Module (TPM) embedded security chip must be installed in your computer to use Embedded Security for HP ProtectTools. Most HP commercial desktop computers include the Infineon TPM, which is the only common criteria certified chip to meet TCG specifications.

Embedded Security for HP ProtectTools protects against unauthorized access to user data or credentials. This software module provides the following security features:

- Enhanced Microsoft Encryption File System (EFS) file and folder encryption (EFS is not available on Windows Home versions)

- Creation of a personal secure drive (PSD) for protecting user data

- Data management functions, such as backing up and restoring the key hierarchy

- Support for third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations when using the Embedded Security software

The TPM embedded security chip enhances and enables other HP ProtectTools Security Manager security features. For example, Drive Encryption for HP ProtectTools can use the embedded chip as an authentication factor when the user logs on to Windows.

Setup procedures

CAUTION: To reduce security risk, it is highly recommended that your IT administrator immediately initialize the embedded security chip. Failure to initialize the embedded security chip could result in an unauthorized user, a computer worm, or a virus taking ownership of the computer and gaining control over the owner tasks, such as handling the emergency recovery archive, and configuring user access settings.

Follow the steps in the following 2 sections to enable and initialize the embedded security chip.

Installing Embedded Security for HP ProtectTools (if necessary)

To install Embedded Security for HP ProtectTools:

1. Click **Start**, click **All Programs**, and click **Install Embedded Security for HP ProtectTools**.

2. **Accept** the UAC warning.

3. Click **Next**, then enter User Name & Organization name if appropriate.

4. Click **Next**, click **Install**, and click **Finish** when complete.

5. Select **Yes** or **No** for the reboot request.

Enabling the embedded security chip in Computer Setup

The embedded security chip can be enabled in the Quick Initialization Wizard or in the Computer Setup utility as described below.

To enable the embedded security chip in Computer Setup:

1. Open Computer Setup by turning on or restarting the computer, and then pressing F10 while the "F10 = ROM Based Setup" message is displayed in the lower-left corner of the screen.

2. If you have not set an administrator password, use the arrow keys to select **Security**, select **Setup password**, and then press Enter.

3. Type your password in the **New password** and **Verify new password** boxes, and then press F10.

4. In the **Security** menu, use the arrow keys to select **TPM Embedded Security**, and then press Enter.

5. Select **Embedded security device state** and change to **Enable**.

6. Press F10 to accept the changes to the Embedded Security configuration.

7. To save your preferences and exit Computer Setup, use the arrow keys to select **File**, and click **Save Changes and Exit**. Then follow the on-screen instructions.

Initializing the embedded security chip

In the initialization process for Embedded Security, you will perform the following tasks:

●   Set an owner password for the embedded security chip that protects access to all owner functions on the embedded security chip.

●   Set up the emergency recovery archive, which is a protected storage area that allows reencryption of the Basic User Keys for all users.

To initialize the embedded security chip:

1. Right-click the HP ProtectTools Security Manager icon in the notification area, at the far right of the taskbar, and then select **Embedded Security Initialization**.

    The HP ProtectTools Embedded Security Initialization Wizard opens.

2. Follow the on-screen instructions.

Setting up the basic user account

Setting up a basic user account in Embedded Security accomplishes the following tasks:

●   Produces a Basic User Key that protects encrypted information, and sets a Basic User Key password to protect the Basic User Key.

●   Sets up a personal secure drive (PSD) for storing encrypted files and folders.

△ **CAUTION:**   Safeguard the Basic User Key password. Encrypted information cannot be accessed or recovered without this password.

To set up a basic user account and enable the user security features:

1. If the Embedded Security User Initialization Wizard is not open, click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the left pane, click **Embedded Security**, and then click **User Settings**.

3. In the right pane, under **Embedded Security Features**, click **Configure**.

    The Embedded Security User Initialization Wizard opens.

4. Follow the on-screen instructions.

NOTE: To use secure e-mail, you must first configure the e-mail client to use a digital certificate that is created with Embedded Security. If a digital certificate is not available, you must obtain one from a certification authority. For instructions on configuring your e-mail and obtaining a digital certificate, refer to the e-mail client software Help.

General tasks

After the basic user account is set up, you can perform the following tasks:

- Encrypting files and folders
- Sending and receiving encrypted e-mail

Using the Personal Secure Drive

After setting up the PSD, you are prompted to type the Basic User Key password at the next logon. If the Basic User Key password is entered correctly, you can access the PSD directly from Windows Explorer.

Encrypting files and folders

When working with encrypted files, consider the following rules:

- Only files and folders on NTFS partitions can be encrypted. Files and folders on FAT partitions cannot be encrypted.
- System files and compressed files cannot be encrypted, and encrypted files cannot be compressed.
- Temporary folders should be encrypted, because they are potentially of interest to hackers.
- A recovery policy is automatically set up when you encrypt a file or folder for the first time. This policy ensures that if you lose your encryption certificates and private keys, you will be able to use a recovery agent to decrypt your information.

NOTE: Encrypting files and folders is not supported on Windows Home versions.

To encrypt files and folders:

1. Right-click the file or folder that you want to encrypt.
2. Click **Encrypt**.
3. Click one of the following options:
   - **Apply changes to this folder only**
   - **Apply changes to this folder, subfolders, and files**
4. Click **OK**.

Sending and receiving encrypted e-mail

Embedded Security enables you to send and receive encrypted e-mail, but the procedures vary depending upon the program you use to access your e-mail. For more information, refer to the Embedded Security software Help, and the software Help for your e-mail program.

Advanced tasks

Backing up and restoring

The Embedded Security backup feature creates an archive that contains certification information to be restored in case of emergency.

Creating a backup file

To create a backup file:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the left pane, click **Embedded Security**, and then click **Backup**.

3. In the right pane, click **Configure**. The HP Embedded Security for HP ProtectTools Backup Wizard opens.

4. Follow the on-screen instructions.

Restoring certification data from the backup file

To restore data from the backup file:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the left pane, click **Embedded Security**, and then click **Backup**.

3. In the right pane, click **Restore all**. The HP Embedded Security for HP ProtectTools Backup Wizard opens.

4. Follow the on-screen instructions.

Changing the owner password

To change the owner password:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

2. In the left pane, click **Embedded Security**, and then click **Advanced**.

3. In the right pane, under **Owner Password**, click **Change**.

4. Type the old owner password, and then set and confirm the new owner password.

5. Click **OK**.

Resetting a user password

An administrator can help a user to reset a forgotten password. For more information, refer to the software Help.

Migrating keys with the Migration Wizard

Migration is an advanced administrator task that allows the management, restoration, and transfer of keys and certificates.

For details on migration, refer to the Embedded Security software Help.

9 Device Access Manager for HP ProtectTools

This security tool is available to administrators only. Device Access Manager for HP ProtectTools has the following security features that protect against unauthorized access to devices attached to your computer system:

- Device profiles that are created for each user to define device access

- Device access that can be granted or denied on the basis of group membership

NOTE: Device Access Manager uses Windows Local Users and Groups to manage access. Windows Home versions do not support Local Users and Groups, therefore Device Access Manager will not function properly. However, Device Access Manager will work in Microsoft Windows Vista Home version if you use DOS commands for the user setup. Refer to the Device Access Manager help file for instructions.

Starting background service

For device profiles to be applied, the HP ProtectTools Device Locking/Auditing background service must be running. When you first attempt to apply device profiles, HP ProtectTools Administrative Console opens a dialog box to ask if you would you like to start the background service. Click **Yes** to start the background service and set it to start automatically whenever the system boots.

Simple configuration

Device Access Manager creates a new User Group during initialization called Device Administrators for accessing or exploring devices as an administrator. Place users in this group that you want to have administrative access to the devices you control through Device Access Manager Simple Configuration.

This feature allows you to deny access to the following classes of devices:

- USB devices for all non-Device Administrators

- All removable media (floppy disks, personal music players, pen drives, etc.) for all non-Device Administrators

- All DVD/CD-ROM drives for all non-Device Administrators

- All serial and parallel ports for all non-Device Administrators

To deny access to a class of device for all non-Device Administrators:

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the left pane, click **Device Access Manager**, and then click **Simple Configuration**.

3. In the right pane, select the check box of a device to deny access.

4. Click the **Save** icon.

NOTE: If background service is not running, it attempts to start now. Click **Yes** to allow it.

5. Click **OK**.

Device class configuration (advanced)

More selections are available to allow specific users or groups of users to be granted or denied access to types of devices.

Adding a user or a group

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the left pane, expand **Device Access Manager**, and then click **Device Class Configuration**.

3. In the device list, click the device class that you want to configure.

4. Click **Add**. The **Select Users or Groups** dialog box opens.

5. Click **Advanced**, and then click **Find Now** to search for users or groups to add.

6. Click a user or a group to be added to the list of available users and groups, and then click **OK**.

7. Click **OK**.

Removing a user or a group

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the left pane, expand **Device Access Manager**, and then click **Device Class Configuration**.

3. In the device list, click the device class that you want to configure.

4. Click the user or group you want to remove, and then click **Remove**.

Denying or allowing access to a user or group

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

2. In the left pane, expand **Device Access Manager**, and then click **Device Class Configuration**.

3. In the device list, click the device class that you want to configure.

4. Under **User/Groups**, click the user or group to be denied access.

5. Click **Deny** next to the user or group to be denied access.

6. Click the **Save** icon, and then click **OK**.

Just In Time Authentication (JITA) Configuration

The JITA Configuration page allows the administrator to view and modify lists of users and groups that are allowed to access devices using just-in-time authentication (JITA). JITA enabled users will be able to access some devices which policies created on the Device Class Configuration or Simple Configurations view have restricted.

Scenario: A Simple Configuration policy is configured to deny all non-Device Administrators access to the DVD/CD-ROM drive.

Result: A JITA enabled user attempts to access the DVD/CD-ROM drive, they receive the same access denied message as a non JITA enabled user. In addition, another popup will display asking for the users credentials. Once the user successfully authenticates to Security Manager they will be granted access to the DVD/CD-ROM drive.

The JITA period can be authorized for a set number of minutes or 0 minutes. A JITA period of 0 minutes will not expire; the user will have access to the device from the time they authenticate until the time they log off the system.

The JITA period can also be extendable. In this scenario, 1 minute before their JITA period is about to expire they can click the prompt and extend their access without having to re-authenticate.

Whether the user is given a limited or unlimited JITA period, as soon as they log off the system or switch their user and login as someone else, the JITA period expires. The next time the user logs in and attempts to access a JITA enabled device they will be prompted for their credentials. At present JITA is available for the following device classes:

- DVD/CD-ROM
- Removable Media

This section provides information about the following topics:

- Creating a JITA for a user or group
- Creating an extendable JITA for a user or group
- Disabling a JITA for a User or Group

Creating a JITA for a user or group

Administrators can allow users or group access to devices using just-in-time authentication.

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **JITA Configuration**.
2. From the devices drop-down menu, select either **removable media** or **DVD/CD-ROM drives**.
3. Using the **+** button, add a user or group to the JITA configuration.
4. Click the **Enabled** check box.
5. Set the JITA period to the required time.
6. Click the **Apply** button.

The selected user can now login, authenticate to Security Manager and access the device.

Creating an extendable JITA for a user or group

Administrators can allow users or group access to devices using just-in-time authentication.

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **JITA configuration**.
2. From the devices drop-down menu, select either **removable media** or **DVD/CD-ROM drives**.
3. Using the **+** button, add a user or group to the JITA configuration.
4. Click the **Enabled** check box.

5. Set the JITA period to the required time.

6. Click the **Extendable** check box.

7. Click the **Apply** button.

The selected user can now login, authenticate to Security Manager and access the device. One minute before the JITA period is about to expire, the user will be prompted to extend their JITA period.

Disabling a JITA for a user or group

Administrators can disable a users or group access to devices using just-in-time authentication.

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **JITA configuration**.

2. From the devices drop-down menu, select either **removable media** or **DVD/CD-ROM drives**.

3. Select the User whose JITA you wish to disable.

4. Click the **Enabled** check box to clear it.

5. Click the **Apply** button.

Now when the user logs in and attempts to access the device they will be denied access.

Advanced Settings

The Advanced Setting page provides the following functionality:

● Management of the Device Administrators group

● Management of drive letters to which the Device Access Manager never denies access.

The Device Administrators group is used to exclude trusted users (trusted in terms of device access) from the restrictions imposed by a Device Access Manager policy. Suitable users are likely to include the system Administrators.

The Advanced Settings view also enables the Administrator to configure a list of drive letters to which Device Access Manager will not restrict access for any user. In order to configure the list of drive letters, the Device Access Manager background services need to be running. The easiest way to start these services is to apply a Simple Configuration policy, such as denying all non Device Administrators access to removable media.

10 Computrace for HP ProtectTools

Computrace for HP ProtectTools is a tool that can remotely monitor, manage, and track your computer.

Once activated, Computrace for HP ProtectTools is configured from the Absolute Software Customer Center. From the Customer Center, the administrator can configure Computrace for HP ProtectTools to monitor or manage the computer. If the system is misplaced or stolen, the Customer Center can assist local authorities to locate and recover the computer. If configured, Computrace can continue to function even if the hard drive is erased or replaced.

To activate Computrace for HP ProtectTools:

1. Connect to the Internet.

2. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

3. In the Security Manager left pane, click **Theft Recovery**.

4. To launch the Computrace Activation Wizard, click the **Activate Now** button.

5. Enter your contact information along with your credit card payment information or enter a pre-purchased Product Key.

The Activation Wizard securely processes the transaction and sets up your user account on the Absolute Software Customer Center website. Once complete, you receive a confirmation e-mail containing your Customer Center account information.

If you have previously run the Computrace Activation Wizard and your Customer Center user account already exists, you can purchase additional licenses by contacting your HP account representative.

To log in to Customer Center:

1. Go to https://cc.absolute.com/.

2. In the **Login ID** and **Password** fields, type the credentials you received in the confirmation e-mail, and then click the **Log in** button.

Using the Customer Center, you can:

●   Monitor your computers.

●   Protect your remote data.

●   Report the theft of any computer protected by Computrace.

Click **Learn More** for more details about Computrace for HP ProtectTools.

Glossary

activation.
The task that must be completed before any of the Drive Encryption features are accessible. Drive Encryption is activated using the HP ProtectTools Security Manager Administrative Console setup wizard. Only an administrator can activate Drive Encryption. The activation process consists of activating the software, encrypting the drive, creating a user account, and creating the initial backup encryption key on a removable storage device.

administrator.
See Windows administrator.

asset.
A data component consisting of personal information or files, historical and Web-related data, and so on, which is located on the hard drive.

authentication.
Process of verifying whether a user is authorized to perform a task such as accessing a computer, modifying settings for a particular program, or viewing secured data.

automatic shredding.
Scheduled shredding that the user sets in File Sanitizer for HP ProtectTools.

Automatic Technology Manager (ATM).
Allows network administrators to manage systems remotely at the BIOS level.

bleaching.
see **free space bleaching**.

certification authority.
Service that issues the certificates required to run a public key infrastructure.

credentials.
Method by which a user proves eligibility for a particular task in the authentication process.

cryptographic service provider (CSP).
Provider or library of cryptographic algorithms that can be used in a well-defined interface to perform particular cryptographic functions.

cryptography.
Practice of encrypting and decrypting data so that it can be decoded only by specific individuals.

decryption.
Procedure used in cryptography to convert encrypted data into plain text.

digital certificate.
Electronic credentials that confirm the identity of an individual or a company by binding the identity of the digital certificate owner to a pair of electronic keys that are used to sign digital information.

digital signature.
Data sent with a file that verifies the sender of the material, and that the file has not been modified after it was signed.

domain.
Group of computers that are part of a network and share a common directory database. Domains are uniquely named, and each has a set of common rules and procedures.

Drive Encryption key recovery service.
The SafeBoot Recovery Service. It stores a copy of the encryption key, enabling you to access your computer if you forget your password and do not have access to your local backup key. You must create an account with the service to set up online access to your backup key.

Drive Encryption logon screen.
A logon screen that is displayed before Windows starts up. Users must enter their Windows user name and the password or Smart Card PIN. Under most circumstances, entering the correct information at the Drive Encryption logon screen allows access directly into Windows without having to log in again at the Windows logon screen.

DriveLock
Security feature that links the hard drive to a user and requires the user to correctly type the DriveLock password when the computer starts up.

emergency recovery archive.
Protected storage area that allows the reencryption of basic user keys from one platform owner key to another.

Encryption File System (EFS).
System that encrypts all files and subfolders within the selected folder.

encryption.
Procedure, such as use of an algorithm, employed in cryptography to convert plain text into cipher text in order to prevent unauthorized recipients from reading that data. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard and public-key encryption.

free space bleaching.
The secure writing of random data over deleted assets on the hard drive to distort the contents of the deleted assets, making recovery of the data more difficult.

key sequence.
A combination of specific keys that, when pressed, initiates an automatic shred—for example, Ctrl+Alt+S.

manual shred.
Immediate shredding of an asset or selected assets, which bypasses the automatic shred schedule.

migration.
A task that allows the management, restoration, and transfer of Privacy Manager Certificates and Trusted Contacts.

network account.
Windows user or administrator account, either on a local computer, in a workgroup, or on a domain.

personal secure drive (PSD).
Provides a protected storage area for sensitive information.

power-on authentication.
Security feature that requires a password when the computer is turned on.

Privacy Manager certificate.
A digital certificate that requires authentication each time you use it for cryptographic operations, such as signing and encrypting e-mail messages and Microsoft Office documents.

Public Key Infrastructure (PKI)
Standard that defines the interfaces for creating, using, and administering certificates and cryptographic keys.

reboot.
Process of restarting the computer.

reveal.

A task that allows the user to decrypt one or more chat history sessions, displaying the Contact Screen Name(s) in plain text and making the session available for viewing.

revocation password.
A password that is created when a user requests a digital certificate. The password is required when the user wants to revoke his or her digital certificate. This ensures that only the user may revoke the certificate.

seal for trusted contacts.
A task that adds a digital signature, encrypts the e-mail, and sends it after you authenticate using your chosen security logon method.

security logon method.
The method used to log in to the computer.

Send Security button.
A software button that is displayed on the toolbar of Microsoft Outlook e-mail messages. Clicking the button allows you to sign and/or encrypt a Microsoft Outlook e-mail message.

shred cycle.
The number of times the shred algorithm is executed on each asset. The higher the number of shred cycles you select, the more secure the computer is.

shred profile.
A specified erasure method and list of assets.

shred.
The execution of an algorithm that obscures the data contained in an asset.

Sign and Encrypt button.
A software button that is displayed on the toolbar of Microsoft Office applications. Clicking the button allows you to sign, encrypt, or removing encryption in a Microsoft Office document.

signature line.
A placeholder for the visual display of a digital signature. When a document is signed, the signer's name and verification method are displayed. The signing date and the signer's title can also be included.

simple delete.
Deletion of the Windows reference to an asset. The asset content remains on the hard drive until obscuring data is written over it by free space bleaching.

Smart Card.
A removable card that is inserted into the computer. It contains identification information for logon. Logging in with a Smart Card at the Drive Encryption logon screen requires that you insert the Smart Card and type your user name and Smart Card PIN.

suggested signer.
A user who is designated by the owner of a Microsoft Word or Microsoft Excel document to add a signature line to the document.

Trusted Contact invitation.
An e-mail that is sent to a person, asking them to become a Trusted Contact.

Trusted Contact list.
A listing of Trusted Contacts.

Trusted Contact recipient.
A person who receives an invitation to become a Trusted Contact.

Trusted Contact.
A person who has accepted a Trusted Contact invitation.

trusted IM communication.

A communication session during which trusted messages are sent from a trusted sender to a Trusted Contact.

trusted message.
A communication session during which trusted messages are sent from a trusted sender to a Trusted Contact.

Trusted Platform Module (TPM) embedded security chip.
The generic term for the HP ProtectTools Embedded Security Chip. A TPM authenticates a computer, rather than a user, by storing information specific to the host system, such as encryption keys, digital certificates, and passwords. A TPM minimizes the risk that information on the computer will be compromised by physical theft or an attack by an external hacker.

trusted sender.
A Trusted Contact who sends signed and/or encrypted e-mails and Microsoft Office documents.

TXT.
Trusted Execution Technology. Hardware and firmware that provides security against attacks on a computer's software and data.

user.
Anyone enrolled in Drive Encryption. Non-administrator users have limited rights in Drive Encryption. They can only enroll (with administrator approval) and log in.

Windows administrator.
A user with full rights to modify permissions and manage other users.

Windows user account.
Profile for an individual authorized to log on to a network or to an individual computer.

Index

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com