HP ProtectTools

Getting Started

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Bluetooth is a trademark owned by its proprietor and used by Hewlett-Packard Company under license. Intel is a trademark of Intel Corporation in the U.S. and other countries and is used under license. Microsoft, Windows, and Windows Vista are U.S. registered trademarks of Microsoft Corporation.

The information contained herein is subject to change without notice. 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.

First Edition: January 2011

Document Part Number: 638391-001

Table of contents

1 Introduction to security

HP ProtectTools Security Manager software provides security features that help protect against unauthorized access to the computer, networks, and critical data.

Application	Features
HP ProtectTools Administrative Console (for administrators	• Requires Microsoft Windows administrator rights to access. • Provides access to modules that are configured by an administrator and not available to users. • Allows initial security setup and configures options or requirements for all users.
HP ProtectTools Security Manager (for users)	• Allows users to configure options provided by an administrator. • Allows administrators to provide users limited control of some HP ProtectTools modules.

The software modules available for your computer may vary depending on your model.

HP ProtectTools software modules may be preinstalled, preloaded, or available for download from the HP Web site. For more information, visit http://www.hp.com.

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 Administrative Console (for administrators)	• Set up and configure levels of security and security logon methods using the Security Manager Setup Wizard. • Configure options hidden from users. • Configure Device Access Manager configurations and user access. • Add and remove HP ProtectTools users and view user status using administrator tools.
HP ProtectTools Security Manager (for users)	• Organize, set up, and change passwords. • Configure and change user credentials such as a Windows password, fingerprint, and smart card. • Configure and change File Sanitizer Shredding, Bleaching, and other settings. • View settings for Device Access Manager. • Configure Computrace for HP ProtectTools. • Configure preferences and Backup and Restore options.
Credential Manager for HP ProtectTools (Password Manager)	• Save, organize, and protect your user names and passwords. • Set up the logon screens of Web sites and programs for quick and secure access. • Save Web site user names and passwords by entering them into Password Manager. The next time you visit this site, Password Manager fills in and submits the information automatically. • Create stronger passwords for enhanced account security. Password Manager fills in and submits the information automatically.
Drive Encryption for HP ProtectTools (select models only)	• Provides complete, full-volume hard drive encryption. • Forces pre-boot authentication in order to decrypt and access the data.
File Sanitizer for HP ProtectTools	• Shreds digital assets (sensitive information including application files, historical or Web-related content, or other confidential data) on your computer and periodically bleaches deleted assets on the hard drive.
Device Access Manager for HP ProtectTools (select models only)	• Allows IT managers to control access to devices based on user profiles. • Prevents unauthorized users from removing data using external storage media, and from introducing viruses into the system from external media. • Allows administrators to disable access to writable devices for specific individuals or groups of users.

Module	Key features
Privacy Manager for HP ProtectTools (select models only)	• Used to obtain Certificates of Authority, which verify the source, integrity, and security of communication when using Microsoft e-mail and Microsoft Office documents.
Computrace for HP ProtectTools (purchased separately)	• Provides secure asset tracking. • Monitors user activity, as well as hardware and software changes. • Remains active even if the hard drive is reformatted or replaced. • Requires separate purchase of tracking and tracing subscriptions to activate.
Embedded Security for HP ProtectTools (select models only)	• Uses a Trusted Platform Module (TPM) embedded security chip to protect against unauthorized access to user data and credentials stored on a computer. • 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.

HP ProtectTools security product description and common use examples

Most of the HP ProtectTools security products have both user authentication (usually a password) and an administrative backup to gain access if passwords are lost, not available, or 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 than have it compromised. It is recommended that all data be backed up in a secure location.

Credential Manager for HP ProtectTools

Credential Manager (part of Security Manager) stores user names and passwords, and can be used to:

- Save login names and passwords for Internet access or e-mail.
- Automatically log the user in to a Web site or e-mail.
- Manage and organize authentications.
- Select a Web or network asset and directly access the link.
- View names and passwords when necessary.

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 a Web or network asset 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 in to a large number of client Web accounts, each of which uses 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.

Drive Encryption for HP ProtectTools

Drive Encryption is used to restrict access to the data on the entire computer hard drive or a secondary drive. Drive Encryption can also manage self-encrypting 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 requires pre-boot authentication before Windows login. Once set up, the hard drive cannot be accessed without a password before the operating system starts. The doctor could further enhance drive security by choosing to encrypt the data with the SED (self-encrypting drive) option.

Both Embedded Security for HP ProtectTools and Drive Encryption for HP ProtectTools do 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 the computer or domain using their personal user name 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 that data in 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 does not actually 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, and so on 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, and so on. 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 for 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 Manager, the information cannot be compromised or intercepted by an imposter.

Example 1: A stock broker wants to make sure that his e-mails only go to specific clients and that 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 ensure 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. A 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 LoJack Pro)

Computrace for HP ProtectTools (purchased separately) 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 computers 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 the 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.

Embedded Security for HP ProtectTools (select models only)

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 Platform 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.

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

Protecting against targeted theft

An example of targeted theft would be the theft of a computer containing confidential data and customer information at an airport security checkpoint. The following features help protect against targeted theft:

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. Refer to the following chapters:
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- The Personal Secure Drive feature, provided by the Embedded Security for HP ProtectTools module, encrypts sensitive data to help ensure that it cannot be accessed without authentication. Refer to the following chapter:
  - Embedded Security for HP ProtectTools
- Computrace can track the computer's location after a theft. Refer to the following chapter:
  - Computrace for HP ProtectTools

Restricting access to sensitive data

Suppose a contract auditor is working onsite 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 writable 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 writable devices so sensitive information cannot be printed or copied from the hard drive onto removable media.

Preventing unauthorized access from internal or external locations

Unauthorized access to an unsecured business computer presents a very real risk to corporate network resources such as information from financial services, an executive, or the 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. Refer to the following chapters:
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager helps ensure that an unauthorized user cannot get passwords or access to password-protected applications.
- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writable devices so sensitive information cannot be copied from the hard drive.
- File Sanitizer allows secure deletion of data by shredding critical files and folders or bleaching deleted assets on the hard drive (writing over data that has been deleted but is still recoverable).
- Privacy Manager allows you to obtain Certificates of Authority when using Microsoft e-mail or Microsoft Office documents, making the process of sending and saving important information safe and secure.

Creating strong password policies

If a company policy goes into effect that requires the use of strong password policy for dozens of Web-based applications and databases, Security Manager provides a protected repository for passwords and Single Sign On convenience.

Additional security elements

Assigning security roles

In managing computer security (particularly for large organizations), 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.

  NOTE: Many of the features in HP ProtectTools can be customized by the security officer in cooperation with HP. For more information, see the HP Web site at http://www.hp.com.

- 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 set the smart card PIN and use the card for authentication.

CAUTION: Administrators are encouraged to follow “best practices” in restricting end-user privileges and restricting user access.

Unauthorized users should not be granted administrative privileges.

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 the following module	Function
Windows Logon password	Windows® Control Panel or HP ProtectTools Security Manager	Can be used for manual logon and for authentication to access various Security Manager features.
Security Manager Backup and Recovery password	Security Manager, by individual user	Protects access to the Security Manager Backup and Recovery file.
Smart card PIN	Credential Manager	Can be used as multifactor authentication. Can be used as Windows authentication. Authenticates users of Drive Encryption, if the smart card token is selected.
Emergency Recovery Token password	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the embedded security chip.

HP ProtectTools password	Set in the following module	Function
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.
BIOS Administrator password	Computer Setup, by IT administrator	Protects access to the Computer Setup utility.

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 your 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 and restoring HP ProtectTools credentials

You can use the Backup and Restore feature of HP ProtectTools to select and back up HP ProtectTools credentials data and settings.

2 Getting started with the Setup Wizard

The Security Manager Setup Wizard guides you through enabling available security features that are applied to all users of this computer. You can also manage these features on the Security Features page of Administrative Console.

To set up security features through the Security Manager Setup Wizard:

1. Open HP ProtectTools Security Manager from the HP ProtectTools desktop gadget icon in Windows Sidebar or the taskbar icon in the notification area, at the far right of the taskbar.

The banner color at the HP ProtectTools desktop gadget icon indicates one of the following conditions:

- Red—HP ProtectTools has not been set up, or an error condition exists with one of the ProtectTools modules.
- Yellow—Check the Applications Status page in Security Manager for settings changes that must be made.
- Blue—HP ProtectTools has been set up, and it is working properly.

A message is displayed at the bottom of the gadget icon to indicate one of the following conditions:

- **Set up now**—The administrator must click the gadget icon to run the Security Manager Setup Wizard to configure authentication credentials for the computer.

  The Setup Wizard is an independent application.

- **Enroll now**—A user must click the gadget icon to run the Security Manager Getting Started Wizard to enroll authentication credentials.

  The Getting Started Wizard is displayed in the Security Manager dashboard.

- **Check now**—Click the gadget icon to display further details on the Security Applications Status page.

NOTE: The HP ProtectTools desktop gadget icon is not available in Windows XP.

– or –

Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**. In the left pane, click **Setup Wizard**.

2. Read the Welcome screen, and then click **Next**.

3. Verify your identity by typing your Windows password, and then click **Next**.

   If you have not yet created a Windows password, you are prompted to create one. A Windows password is required in order to protect your Windows account from access by unauthorized persons, and in order to use HP ProtectTools Security Manager features.

4. On the SpareKey page, select three security questions, enter an answer for each question, and then click **Next**.

   You can select different questions or change your answers on the SpareKey page under **Credential Manager** in the Security Manager dashboard.

NOTE: This SpareKey setup applies only to the administrative user.

5. Enable security features by selecting their check boxes, and then click **Next**.

   The more features that you select, the more secure your computer is.

NOTE: These settings apply to all users. If any check boxes are not selected, the Setup Wizard will not prompt users to register those credentials.

- **Windows Logon Security**—Protects your Windows accounts by requiring the use of specific credentials for access.
- **Drive Encryption**—Protects your data by encrypting your hard drives, making the information unreadable by those without proper authorization.
- **Pre-Boot Security**—Protects your computer by prohibiting access by unauthorized persons prior to Windows startup.

  NOTE: Pre-Boot Security is not available if the BIOS does not support it.

6. The Setup Wizard prompts you to register, or “enroll”, credentials.

   If neither a fingerprint reader, a smart card, nor a webcam is available, you are prompted to enter your Windows password. After enrolling, you may then use any enrolled credentials to verify your identity whenever authentication is required.

NOTE: Enrollment of these credentials applies only to the administrative user.

7. On the final page of the wizard, click **Finish**.

   The Security Manager dashboard Home page is displayed.

3 HP ProtectTools Security Manager Administrative Console

HP ProtectTools Security Manager software provides security features that help protect against unauthorized access to the computer, networks, and critical data. Administration of HP ProtectTools Security Manager is provided through the Administrative Console feature.

Additional applications are available (select models only) in the Security Manager dashboard to assist with recovery of the computer if it is lost or stolen.

Using the console, the local administrator can perform the following tasks:

- Enabling or disabling security features
- Specifying required credentials for authentication
- Managing users of the computer
- Adjusting device-specific parameters
- Configuring installed Security Manager applications
- Adding additional Security Manager applications

Opening HP ProtectTools Administrative Console

For administrative tasks, such as setting system policies or configuring software, open the console as follows:

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

  – or –

  In the left panel of Security Manager, click **Administration**, and then click **Administrative Console**.

Using Administrative Console

HP ProtectTools Administrative Console is the central location for administering HP ProtectTools Security Manager features and applications.

▲ To open HP ProtectTools Administrative Console, click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.

– or –

In the left panel of Security Manager, click **Administration**, and then click **Administrative Console**.

The console is composed of the following components:

- **Home**—Allows you to configure the following security options:
  - **Increase system security**
  - **Require strong authentication**
  - **Manage HP ProtectTools users**
  - **See how you can centrally manage HP ProtectTools**
- **System**—Allows you to configure the following security features and authentication for users and devices:
  - **Security**
  - **Users**
  - **Credentials**
- **Applications**—Allows you to configure settings for HP ProtectTools Security Manager and for Security Manager applications.
- **Data**—Provides an expanding menu of links to Security Manager applications that protect your data.
- **Central Management**—Displays tabs for accessing additional solutions, product updates, and messages.
- **Setup Wizard**—Guides you through setting up HP ProtectTools Security Manager.
- **About**—Displays information about HP ProtectTools Security Manager, such as the version number and copyright notice.
- **Main area**—Displays application-specific screens.

  ?—Displays the Administrative Console software Help. This icon is located at the top right of the window frame, next to the minimize and maximize icons.

Configuring your system

The **System** group is accessed from the menu panel on the left side of HP ProtectTools Administrative Console. You can use the applications in this group to manage the policies and settings for the computer, its users, and its devices.

The following applications are included in the **System** group:

- **Security**—Manage features, authentication, and settings governing how users interact with this computer.
- **Users**—Set up, manage, and register users of this computer.
- **Credentials**—Manage settings for security devices built into or attached to the computer.

Setting up authentication for your computer

Within the Authentication application, you can set policies governing access to the computer. You can specify the credentials required to authenticate each class of user when logging on to Windows or logging on to Web sites and programs during a user session.

To set up authentication on your computer:

1. In the left panel of Administrative Console, click **Security**, and then click **Authentication**.
2. To configure logon authentication, click the **Logon Policy** tab, make changes, and then click **Apply**.
3. To configure session authentication, click the **Session Policy** tab, make changes, and then click **Apply**.

Logon Policy

To define policies governing the credentials required to authenticate a user when logging on to Windows:

1. In the left panel of Administrative Console, click **Security**, and then click **Authentication**.
2. On the **Logon Policy** tab, click the down arrow, and then select a category of user:
   - **For administrators of this computer**
   - **For users who are not administrators**
3. Specify the authentication credentials required for the selected category of user.
4. Choose whether ONE of the specified credentials is required, or if ALL of the specified credentials are required in order to authenticate a user.
5. Click **Apply**.

Session Policy

To define policies governing the credentials required to access HP ProtectTools applications during a Windows session:

1. In the left panel of Administrative Console, click **Security**, and then click **Authentication**.
2. On the **Session Policy** tab, click the down arrow, and then select a category of user:
   - **For administrators of this computer**
   - **For users who are not administrators**
3. Click the down arrow, and then select the authentication credentials required for the selected category of user:
   - **Require one of the specified credentials**

     NOTE: Clearing the check boxes for all of the credentials has the same effect as selecting **Do not require authentication**.
   - **Require all of the specified credentials**
   - **Do not require authentication**—Selecting this option clears all credentials from the window.
4. Click **Apply**.

Settings

1. Select the check box to enable the following setting, or clear the check box to disable it:

   Allow One Step logon—Allows users of this computer to skip Windows logon if authentication was performed at the BIOS or encrypted disk level.
2. Click **Apply**.

Managing users

Within the Users application, you can monitor and manage this computer's HP ProtectTools users.

All HP ProtectTools users are listed and verified against the policies set through Security Manager, and whether or not they have registered the appropriate credentials enabling them to meet those policies.

To manage users, select from the following settings:

- To add additional users, click **Add**.
- To delete a user, click the user, and then click **Delete**.
- To set up additional credentials for the user, click the user, and then click **Enroll**.
- To view the policies for a specific user, select the user, and then view the policies in the lower window.

Credentials

Within the Credentials application, you can specify settings available for any built-in or attached security devices recognized by HP ProtectTools Security Manager.

SpareKey

You can configure whether or not to allow SpareKey authentication for Windows logon, and manage the security questions that will be presented to users during their SpareKey enrollment.

1. Select the check box to enable or clear it to disable the use of SpareKey authentication for Windows logon.
2. Select the security questions that will be presented to users during their SpareKey enrollment. You can specify up to three custom questions, or you can allow users to type their own passphrase.
3. Click **Apply**.

Fingerprints

If a fingerprint reader is installed or connected to the computer, the Fingerprints page displays the following tabs:

- **Enrollment**—Choose the minimum and maximum number of fingerprints that a user is allowed to enroll.

  You can also clear all of the data from the fingerprint reader.

  CAUTION: Clearing all of the data from the fingerprint reader erases all fingerprint data for all users, including administrators. If the logon policy requires fingerprints only, all users may be prevented from logging on to the computer.

- **Sensitivity**—Move the slider to adjust the sensitivity used by the fingerprint reader when it swipes your fingerprints.

  If your fingerprint is not recognized consistently, you may need to select a lower sensitivity setting. A higher setting increases the sensitivity to variations in fingerprint swipes and therefore decreases the possibility of a false acceptance. The **Medium-High** setting provides a good mix of security and convenience.

- **Advanced**—Select one of the following options to configure the fingerprint reader to conserve power and to enhance visual feedback:

  - **Optimized**—The fingerprint reader activates when needed. You may observe a slight delay when the reader is used for the first time.
  - **Conserve power**—The fingerprint reader is slower to respond, but the setting requires less power.
  - **Full power**—The fingerprint reader is always ready to be used, but this setting uses the most power.

Smart card

If a smart card reader is installed or connected to the computer, the Smart card page has two tabs:

- **Settings**—Configure the computer to automatically lock when a smart card is removed.

NOTE: The computer locks only if the smart card was used as an authentication credential when logging on to Windows. Removing a smart card that was not used to log on to Windows does not lock the computer.

- **Administration**—Select from the following options:
  - **Initialize the smart card**—Prepares a smart card for use with HP Protect Tools. If a smart card has been previously initialized outside of HP ProtectTools (contains an asymmetric key-pair and associated certificate), it does not need to be initialized again, unless initialization with a specific certificate is desired.
  - **Change smart card PIN**—Enables you to change the PIN used with the smart card.
  - **Erase HP ProtectTools data only**—Erases only the HP ProtectTools certificate created during initialization of the card. No other data is erased from the card.
  - **Erase all data on the smart card**—Erases all data on the specified smart card. The card can no longer be used with HP ProtectTools or any other applications.

NOTE: Features that are not supported by your smart card are not available.

▲ Click **Apply**.

Face

If a webcam is installed or connected to the computer, and if the Face Recognition program is installed, you can set the security level for Face Recognition to balance the ease of use and the difficulty of breaching the security of the computer.

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. Click **Credentials**, and then click **Face**.
3. For more convenience, click the slider to move it to the left, or for more accuracy, click the slider to move it to the right.
   - **Convenience**—To make it easier for enrolled users to gain access in marginal situations, click the slider bar to move it to the **Convenience** position.
   - **Balance**—To provide a good compromise between security and usability, or if you have sensitive information or your computer is located in an area where unauthorized logon attempts can occur, click the slider bar to move it to the **Balance** position.
   - **Accuracy**—To make it more difficult for a user to gain access if enrolled scenes or current lighting conditions are below normal and less likely that a false acceptance can occur, click the slider bar to move it to the **Accuracy** position.
4. Click **Advanced**, and then configure additional security. For more information, refer to Advanced User Settings on page 37.
5. Click **Apply**.

Configuring your applications

You can use Settings to customize the behavior of currently installed HP ProtectTools Security Manager applications.

To edit your application settings:

1. In the left panel of Administrative Console, under **Applications**, click **Settings**.
2. Select the check box next to a specific setting to enable it, or clear the check box to disable the setting.
3. Click **Apply**.

General tab

The following settings are available on the **General** tab:

- **Do not automatically launch the Setup Wizard for administrators**—Select this option to prevent the wizard from automatically opening upon logon.
- **Do not automatically launch the Getting Started Wizard for users**—Select this option to prevent user setup from automatically opening upon logon.

Applications tab

The settings displayed here can change when new applications are added to Security Manager. The minimal settings shown by default are as follows:

- **Applications status**—Enables the status to be displayed for all applications.
- **Password Manager**—Enables Password Manager for all users of the computer.
- **Privacy Manager**—Enables Privacy Manager for all users of the computer.
- **Enable the Central Management link**—Allows all users of this computer to add applications to HP ProtectTools Security Manager by clicking **Central Management**.

To return all applications to their factory settings, click the **Restore Defaults** button.

Central Management

Additional applications may be available for adding new management tools to Security Manager. The administrator of this computer may disable this feature on the Settings page. The Central Management page has two tabs:

- **Business Solutions**—If an internet connection is available, you can access the DigitalPersona Web site (http://www.digitalpersona.com/) to check for new applications.
- **Updates and Messages**
  - To request information about new applications and updates, select the check box for **Keep me informed about new applications and updates.**
  - To set up a schedule for automatic updates, select the number of days.
  - To check for updates, click **Check Now**.

4 HP ProtectTools Security Manager

HP ProtectTools Security Manager allows you to significantly increase the security of your computer.

You can use preloaded Security Manager applications, as well as additional applications available for immediate download from the Web:

- Manage your logon and passwords.
- Easily change your Windows® operating system password.
- Set program preferences.
- Use fingerprints for extra security and convenience.
- Enroll one or more scenes for authentication.
- Set up a smart card for authentication.
- Back up and restore your program data.
- Add more applications.

Opening Security Manager

You can open Security Manager in any of the following ways:

- Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.
- Double-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar.
- Right-click the **HP ProtectTools** icon, and click **Open HP ProtectTools Security Manager**.
- Click the **HP ProtectTools** desktop gadget icon.
- Press the hotkey combination ctrl+Windows logo key+h to open the **Security Manager Quick Links** menu.

  For information on changing the hotkey combination, refer to Settings on page 33.

Using the Security Manager dashboard

The Security Manager dashboard is the central location for easy access to Security Manager features, applications, and settings.

▲ To open the Security Manager dashboard, click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Security Manager**.

The dashboard displays the following components:

- **ID Card**—Displays the Windows user name and a selected picture identifying the logged on user account.
- **Security Applications**—Displays an expanding menu of links for configuring the following categories of security:
  - **Home**—Manage passwords, set up your authentication credentials, or check the status of the security applications.
  - **Status**—Check the status of the HP ProtectTools security applications.

NOTE: Applications that are not installed on the computer are not displayed in the following list.

- **My Logons**—Manage your authentication credentials with Password Manager, Credential Manager, Password, SpareKey, Smart Card, Face, and Fingerprint.
- **My Data**—Manage the security of your data with Drive Encryption and File Sanitizer.
- **My Computer**—Manage the security of your computer with Device Access Manager.
- **My Communications**—Manage the security of your communications with Privacy Manager.
- **Administration**—Allows administrators to access the following options:
  - **Administrative Console**—Allows administrators to manage security and users.
  - **Central Management**—Allows administrators to access additional solutions, product updates, and messages.
- **Advanced**—Displays commands for accessing additional features, including:
  - **Preferences**—Allows you to personalize Security Manager settings.
  - **Backup and Restore**—Allows you to back up or restore data.
  - **About**—Displays information about HP ProtectTools Security Manager, such as the version number and copyright notice.
- **Main area**—Displays application-specific screens.
- **?**—Displays the Security Manager software Help. This icon is located at the top right of the window, next to the minimize and maximize icons.

Security Applications Status

You can view the status of your installed security applications in two locations:

- **HP ProtectTools desktop gadget**

  The banner color at the top of the HP ProtectTools gadget icon changes to reflect the overall security status of your installed security applications.

  - **Red**—Warning
  - **Yellow**—Attention: not configured
  - **Blue**—OK

  A message is displayed at the bottom of the gadget icon to indicate one of the following conditions:

  - **Set up now**—The administrator must click the gadget icon to run the Security Manager Setup Wizard to configure authentication credentials for the computer.

    The Setup Wizard is an independent application.

  - **Enroll now**—A user must click the gadget icon to run the Security Manager Getting Started Wizard to enroll authentication credentials.

    The Getting Started Wizard is displayed in the Security Manager dashboard.

  - **Check now**—Click the gadget icon to display further details on the Security Applications Status page.

- **Security Applications Status page**—Click **Status** on the Security Manager dashboard to display the overall status of your installed security applications and the specific status of each application.

My Logons

The applications included in this group assist you in managing various aspects of your digital identity.

- **Password Manager**—Creates and manages Quick Links, which allow you to launch and log on to Web sites and programs by authenticating with your Windows password, your fingerprint, or a smart card.
- **Credential Manager**—Provides a means to easily change your Windows password, enroll your fingerprints, or set up a smart card.

Administrators can add more applications by clicking **Administration**, and then clicking **Central Management** in the lower-left corner of the dashboard.

Password Manager

Logging on to Windows, Web sites, and applications is easier and more secure when you use Password Manager. You can use it to create stronger passwords that you do not have to write down or remember, and then log on easily and quickly with a fingerprint, smart card, or your Windows password.

Password Manager offers the following options:

- Add, edit, or delete logons from the **Manage** tab.
- Use Quick Links to launch your default browser and log on to any Web site or program, after it has been set up.
- Drag and drop to organize your Quick Links into categories.
- See at a glance whether any of your passwords are a security risk, and automatically generate a complex strong password to use for new sites.

The **Password Manager** icon is displayed in the upper-left corner of a Web page or application logon screen. When a logon has not yet been created for that Web site or application, a plus sign is displayed on the icon.

▲ Click the **Password Manager** icon to display a context menu where you can choose from the following options.

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

The following options are displayed on the context menu:

- **Add [somedomain.com] to the Password Manager**—Allows you to add a logon for the current logon screen.
- **Open Password Manager**—Launches Password Manager.
- **Icon settings**—Allows you to specify conditions in which the **Password Manager** icon is displayed.
- **Help**—Displays the Security Manager software Help.

For Web pages or programs where a logon has already been created

The following options are displayed 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 Web site.
- **Add Logon**—Allows you to add an account to a logon.
- **Open Password Manager**—Launches Password Manager.
- **Help**—Displays the Security Manager software Help.

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

Adding logons

You can easily add a logon for a Web site or a program by entering the logon information once. From then on, Password Manager automatically enters the information for you. You can use these logons after browsing to the Web site or program, or click a logon from the **Logons** menu to have Password Manager open the Web site or program and log you on.

To add a logon:

1. Open the logon screen for a Web site or program.
2. Click the arrow on the **Password Manager** icon, and then click one of the following, depending on whether the logon screen is for a Web site or a program:
   - For a Web site, click **Add [domain name] to Password Manager**.
   - For a program, click **Add this logon screen to Password Manager**.
3. Enter your logon data. Logon fields on the screen, and their corresponding fields on the dialog box, are identified with a bold orange border. You can also display this dialog box by clicking **Add Logon** from the **Password Manager Manage** tab. Some options depend on the security devices connected to the computer—for example, using the ctrl+Windows logo key+h hotkey, swiping your fingerprint, or inserting a smart card.
   a. To populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
   b. To view the password for this logon, click **Show password**.
   c. To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.
   d. To enable VeriSign VIP security, select the **I want VIP security on this site** check box.

      This option appears only for sites where VeriSign Identity Protection (VIP) is available. When supported by the site, you can also choose to have your VIP Security Code automatically filled in along with your usual method of authentication.
   e. Click **OK**, click the authentication method that you wish to use (fingerprints, password, or face), and then log on with the selected authentication method.

The plus sign is removed from the **Password Manager** icon to notify you that the logon has been created.

f. If Password Manager does not detect the logon fields, click **More fields**.

- Select the check box for each field that is required for logon, or clear the check box for any fields that are not required for logon.
- If Password Manager cannot detect all of the logon fields, a message is displayed asking if you want to continue. Click **Yes**.
- A dialog box opens with your logon fields filled in. Click the icon for each field and drag it to the appropriate logon field, and then click the button to sign into the Web site.

NOTE: Once you use the manual mode of entering the logon data for a site, you must continue to use this method to log on to the same Web site in the future.

NOTE: The manual mode of entering logon data is available only with Internet Explorer 8.

- Click **Close**.

Each time that you access that Web site or open that program, the **Password Manager** icon is displayed in the upper-left corner of a Web site or application logon screen, indicating that you can use your registered credentials to log on.

Editing logons

To edit a logon, follow these steps:

1. Open the logon screen for a Web site or program.
2. To display a dialog box where you can edit your logon information, click the arrow on the **Password Manager** icon, and then click **Edit logon**. Logon fields on the screen, and their corresponding fields on the dialog box, are identified with a bold orange border.

   You can also display this dialog box by clicking **Edit for the desired logon** on the **Password Manager Manage** tab.
3. Edit your logon information.

   - To select a **Username** logon field with one of the preformatted choices, click the down arrow to the right of the field.
   - To select a **Password** logon field with one of the preformatted choices, click the down arrow to the right of the field.
   - To enable VeriSign VIP security, select the **I want VIP security on this site** check box.

     This option appears only for sites where VeriSign VIP security is available. When supported by the site, you can also choose to have your VIP Security Code automatically filled in along with your usual method of authentication.
   - To add additional fields from the screen to your logon, click **More fields**.

- To view the password for this logon, click **Show password**.
- To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.

4. Click **OK**.

Using the Logons menu

Password Manager provides a fast, easy way to launch the Web sites and programs for which you have created logons. Double-click a program or Web site logon from the **Logons** menu, or from the **Manage** tab in Password Manager, to open the logon screen, and then fill in your logon data.

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

To display the **Logons** menu:

1. Press the **Password Manager** hotkey combination (ctrl+Windows logo key+h is the factory setting). To change the hotkey combination, on the Security Manager dashboard, click **Password Manager**, and then click **Settings**.
2. Swipe your fingerprint (on computers with a built-in or connected fingerprint reader), or enter your Windows password.

Organizing logons into categories

Create one or more categories to keep your logons in order. Then drag and drop your logons into the desired categories.

To add a category:

1. From the Security Manager dashboard, click **Password Manager**.
2. Click the **Manage** tab, and then 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 are highlighted as you move your mouse pointer 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. You can add the same logon to more than one category, and you can display all of your logons by clicking **All**.

Managing your logons

Password Manager makes it easy to manage your logon information for user names, passwords, and multiple logon accounts, from one central location.

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

To manage your logons:

▲ From the Security Manager dashboard, click **Password Manager**, and then click the **Manage** tab.

- **Add a logon**—Click **Add Logon** and follow the on-screen instructions.
- **Your logons**—Click an existing logon, select one of the following options, and then follow the on-screen instructions:
  - **Open**—Open a Web site or program for which you have an existing logon.
  - **Add**—Add a logon. For more information, refer to Adding logons on page 28.
  - **Edit**—Edit a logon. For more information, refer to Editing logons on page 29.
  - **Delete**—Delete a Web site or program for which you have an existing logon.
- **Add Category**—Click **Add Category**, and then follow the on-screen instructions. For more information, refer to Organizing logons into categories on page 30.

To add an additional logon for a Web site or program:

1. Open the logon screen for the Web site or program.
2. Click the **Password Manager** icon to display its context menu.
3. Click **Add Logon**, and then follow the on-screen instructions.

Assessing your password strength

Using strong passwords for logon to your Web sites 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 Web sites and programs.

Password Manager icon settings

Password Manager attempts to identify logon screens for Web sites and programs. When it detects a logon screen for which you have not created a logon, Password Manager prompts you to add a logon for the screen by displaying the **Password Manager** icon with a plus sign.

1. Click the icon arrow, and then click **Icon Settings** to customize how Password Manager handles possible logon sites.
   - **Prompt to add logons for logon screens**—Click this option to have Password Manager prompt you to add a logon when a logon screen is displayed that does not already have a logon set up.
   - **Exclude this screen**—Select the check box so that Password Manager does not prompt you again to add a logon for this logon screen.

To add a logon for a screen that has been previously excluded:

- While the previously excluded Web site logon or the program page is displayed, open the Security Manager dashboard, and then click **Password Manager**.
- Click **Add Logon**.

  The Add Logon dialog box opens with the Web site logon screen or program listed in the **Current screen** field.
- Click **Continue**.

  The Add Logon to Password Manager screen is displayed.
- Follow the on-screen instructions. For more information, refer to Adding logons on page 28.
- The **Password Manager** icon is displayed whenever this Web site logon or program screen is opened.

2. To disable the option for displaying a prompt to add logons for logon screens, select the check box.
3. To access additional Password Manager settings, click **Password Manager**, and then click **Settings** on the Security Manager dashboard.

VeriSign Identity Protection (VIP)

You can create VeriSign VIP Access tokens for use with VeriSign VIP-enabled Web sites. These tokens are used by Password Manager to create automated logons that incorporate use of the tokens dragged and dropped into VeriSign VIP-enabled logon screens or manually entered into specified fields.

You can enable VeriSign VIP and create a token from the Security Manager dashboard or at any VeriSign VIP-enabled Web site. In order to use the token, you must register it on each Web site where it will be used.

After registration and first use of a token, it may (optionally) be appended to and submitted with your regular logon credentials. For sites that do not allow appending the token, you can drag and drop or manually enter the token information.

To enable VeriSign VIP and create a VeriSign VIP token from the Security Manager dashboard:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.
2. Click **Password Manager**, and then click **VIP**.
3. Click **Get VIP**.

   A VeriSign VIP token is created and displayed on the VeriSign VIP page. The token will now be displayed whenever you access this page.

To enable VeriSign VIP and create a VeriSign VIP token from a Web site:

1. Password Manager alerts you whenever you visit a VeriSign VIP-enabled Web site.
2. Create a logon for the screen. For more information, refer to Adding logons on page 28.
3. In the Create Logon dialog box, select **I want additional account protection with VIP**.

To register a VeriSign VIP token for a Web site:

1. Log on to a VeriSign VIP-enabled Web site manually or with a Password Manager logon.
2. Click the displayed VeriSign VIP balloon to create a logon for this site.
3. In the Add Logon to Password Manager dialog box, select **I want VIP security on this site**.

   This option appears only for sites where VeriSign VIP security is available. When supported by the site, you can also choose to have your VIP Security Code automatically filled in along with your usual method of authentication.

Settings

You can specify settings for personalizing HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens**—The **Password Manager** icon with a plus sign is displayed whenever a Web site or program logon screen is detected, indicating that you can add a logon for this screen to the password vault. To disable this feature, in the Icon Settings dialog box, clear the check box beside **Prompt to add logons for logon screens**.
2. **Open Password Manager with ctrl+win+h**—The default hotkey that opens the **Password Manager Quick Links** menu is ctrl+Windows logo key+h. To change the hotkey, click this option and enter a new key combination. Combinations may include one or more of the following: ctrl, alt, or shift, and any alphabetic or numeric key.
3. Click **Apply** to save your changes.

Credential Manager

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

Available credentials can vary, depending on the security devices built into or connected to this computer. Supported credentials, requirements, and current status are displayed when you click **Credential Manager** under **My Logons**, and may include the following:

- Password
- SpareKey
- Fingerprints
- Smart card
- Face

To enroll or change a credential, click the link and follow the on-screen instructions.

Changing your Windows password

Security Manager makes changing your Windows password simpler and quicker than doing it through Windows Control Panel.

To change your Windows password, follow these steps:

1. From the Security Manager dashboard, click **Credential Manager**, and then click **Password**.
2. Enter your current password in the **Current Windows password** text box.
3. Type a new password in the **New Windows password** text box, and then type it again in the **Confirm new password** text box.
4. Click **Change** to immediately change your current password to the new one that you entered.

Setting up your SpareKey

The SpareKey allows you to gain access to your computer (on supported platforms) by answering three security questions from a list previously defined by the administrator.

HP ProtectTools Security Manager prompts you to set up your personal SpareKey during initial setup in the Getting Started Wizard.

To set up your SpareKey:

1. On the SpareKey page of the wizard, select three security questions, and then enter an answer for each question.
2. Click **Next**.

You can select different questions or change your answers on the SpareKey page under **Credential Manager**.

After your SpareKey is set up, you can access your computer using your SpareKey from a Pre-Boot logon screen or the Windows Welcome screen.

Enrolling your fingerprints

If your computer has a fingerprint reader built in or connected, HP ProtectTools Security Manager prompts you to set up or “enroll” your fingerprints during initial setup in the Getting Started Wizard. You can also enroll your fingerprints on the Fingerprint page under **Credential Manager** in the Security Manager dashboard.

1. An outline of two hands is displayed. Fingers that are already enrolled are highlighted in green. Click a finger on the outline.

NOTE: To delete a previously enrolled fingerprint, click its finger.

2. When you have selected a finger to enroll, you are prompted to swipe the finger until its fingerprint is successfully enrolled. An enrolled finger is highlighted in green on the outline.
3. You must enroll at least two fingers; index or middle fingers are preferable. Repeat steps 1 and 2 for another finger.
4. Click **Next**, and then follow the instructions on the screen.

CAUTION: When enrolling fingerprints through the Getting Started process, fingerprint information is not saved until you click **Next**. If you leave the computer inactive for a while, or close the program, the changes you made are **not** saved.

Setting up a smart card

Administrators must initialize and register the smart card before it can be used for authentication.

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 HP ProtectTools will use in its security algorithm.

NOTE: ActivIdentity software must be installed.

1. Insert the card into the reader.
2. Click **Start**, click **All Programs**, and then click **ActivClient PIN Initialization Tool**.
3. Enter and confirm a PIN.
4. Click **Next**.

   The smart card software will provide an unlock key. Most smart cards will lock themselves if the PIN is entered incorrectly 5 times. The key is used to unlock the card.
5. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
6. Click **Credentials**, and then click **Smart Card**.
7. Click the **Administration** tab.
8. Be sure that **Set up the smart card** is selected.
9. Enter your PIN, click **Apply**, and then follow the on-screen instructions.
10. After the smart card has been successfully initialized, you will need to register the smart card.

Registering the smart card

After initializing the smart card, administrators can register the card as an authentication method in HP ProtectTools Administrative Console:

1. Under **Central Management**, click **Setup Wizard**.
2. On the Welcome! page, click **Next**, and then enter your Windows password.
3. On the SpareKey page, click **Skip SpareKey Setup** (unless you want to update the SpareKey information).
4. On the Enable security features page, click **Next**.
5. On the Choose your credentials page, be sure that **Set up your smart card** is selected, and then click **Next**.
6. On the Smart card page, enter your PIN, and then click **Next**.
7. Click **Finish**.

Users can also register a smart card in Security Manager. For more information, refer to the Security Manager for HP ProtectTools software Help.

Configuring the smart card

If a smart card reader is installed or connected to the computer, the Smart card page has two tabs:

- **Settings**—Configure the computer to automatically lock when a smart card is removed.

NOTE: The computer locks only if the smart card was used as an authentication credential when logging on to Windows. Removing a smart card that was not used to log on to Windows does not lock the computer.

- **Administration**—Select from the following options:
  - **Initialize the smart card**—Prepares a smart card for use with HP Protect Tools. If a smart card has been previously initialized outside of HP ProtectTools (contains an asymmetric key-pair and associated certificate), it does not need to be initialized again, unless initialization with a specific certificate is desired.
  - **Change smart card PIN**—Enables you to change the PIN used with the smart card.
  - **Erase HP ProtectTools data only**—Erases only the HP ProtectTools certificate created during initialization of the card. No other data is erased from the card.
  - **Erase all data on the smart card**—Erases all data on the specified smart card. The card can no longer be used with HP ProtectTools or any other applications.

NOTE: Features that are not supported by your smart card are not available.

▲ Click **Apply**.

Enrolling scenes for face logon

If your computer has a webcam built in or connected, HP ProtectTools Security Manager prompts you to set up or “enroll” your scenes during initial setup in the Getting Started Wizard. You can also enroll scenes on the Face logon page under **Credential Manager** in the Security Manager dashboard.

You must enroll one or more scenes in order to use face logon. After you have enrolled successfully, you can also enroll a new scene if you have experienced difficulty during logon because one or more of the following conditions have changed:

- Your face has changed significantly since your last enrollment.
- The lighting is quite different from any of your previous enrollments.
- You were wearing glasses (or not) during your last enrollment.

NOTE: If you are having difficulty enrolling scenes, try moving closer to the webcam.

To enroll a scene from the Getting Started Wizard:

1. On the Face page of the wizard, click **Advanced**, and then configure additional security. For more information, refer to Advanced User Settings on page 37.
2. Click **OK**.
3. Click **Start**, or if you have enrolled scenes previously, click **Enroll a new scene**.
4. If you did not select any additional security options, you are prompted to select an additional security option. Follow the on-screen instructions, and then click **Next**. For more information, refer to Advanced User Settings on page 37.

5. Click the **Camera** icon, and then follow the on-screen instructions to enroll your scene.

   Follow the on-screen instructions, and be sure to look at your image while the scenes are being captured.

6. Click **Next**.

7. Click **Finish**.

You can also enroll scenes from the Security Manager dashboard:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.

2. Under **My Logons**, click **Credential Manager**, and then click **Face**.

3. Click **Advanced**, and then configure additional security. For more information, refer to Advanced User Settings on page 37.

4. Click **OK**.

5. Click **Start**, or if you have enrolled scenes previously, click **Enroll a new scene**.

6. If you did not select any additional security options, you are prompted to select an additional security option. Follow the on-screen instructions, and then click **Next**. For more information, refer to Advanced User Settings on page 37.

7. Click the **Camera** icon, and then follow the on-screen instructions to enroll your scene.

   Follow the on-screen instructions, and be sure to look at your image while the scenes are being captured.

For more information, refer to the Face Recognition software Help by clicking the blue **?** icon at the top right of the Face logon page.

Advanced User Settings

These options are also displayed on the Additional Security page if no additional security has been selected.

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.

2. Under **My Logons**, click **Credential Manager**, and then click **Face**.

3. Click **Advanced** to configure the following security options:

   a. **Security** tab—Select one of the following options:

      - **No additional security**—Select this option if you do not wish to add additional security for face logon.

      - **Use PIN for additional security**—Select this option to require a user-specific PIN for face logon.

        - Click **Create PIN**.

        - Enter your Windows password.

        - Enter the new PIN, and then confirm the new PIN by reentering it.

Once a PIN is created, you can select from the following options: **Change**, **Reset**, or **Remove a PIN**.

- **Use Bluetooth for additional security**—Select this option to pair your Bluetooth-capable phone with Face Recognition. During Windows logon, once your face is authenticated, Face Recognition also verifies the presence of the paired Bluetooth phone. If the phone is present (with Bluetooth enabled), then you are allowed to log on to Windows.

  - Be sure that Bluetooth is enabled on both the computer and the phone.

    If a Bluetooth-enabled phone is not present, you are prompted to enable the paired Bluetooth phone and restart the logon process. After 30 seconds, the Face Recognition logon window is paused. To initiate the logon process, click the **Camera** icon. If the Bluetooth-enabled phone is not present, you can use your normal Windows password to log on.

  - Click **Add**.

  - When your Bluetooth device is displayed, select it, and then click **Next**.

Click **OK**.

b. **Other Settings** tab—Select the check boxes to enable one or more of the following options, or clear the check box to disable an option. These settings apply only to the current user.

- **Play sound on face recognition events**—Plays a sound when face logon succeeds or fails.
- **Prompt to update scenes when logon fails**—If face logon is unsuccessful but you enter your password successfully, you may be prompted to save a series of images to increase the chances of successful face logon in the future.
- **Prompt to enroll a new scene when logon fails**—If face logon is unsuccessful but you enter your password successfully, you may be prompted to enroll a new scene to increase the chances of successful face logon in the future.

Click **OK**.

Your personal ID card

Your ID card uniquely identifies you as the owner of this Windows account, showing your name and a picture of your choice. It is prominently displayed in the upper-left corner of Security Manager pages.

You can change the picture and the way that your name is displayed. By default, your full Windows user name and the picture you selected during Windows setup are shown.

To change the displayed name:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.
2. Click the ID card in the upper-left corner of the dashboard.
3. Click the box displaying your Windows user name for this account, type the new name, and then click **Save**.

To change the displayed picture:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.
2. Click the ID card in the upper-left corner of the dashboard.
3. Click **Choose picture**, click an image, and then click **Save**.

Setting your preferences

You can personalize settings for HP ProtectTools Security Manager. From the Security Manager dashboard, click **Advanced**, and then click **Preferences**. Available settings are displayed on two tabs: **General** and **Fingerprint**.

General tab

Appearance—Show icon in taskbar notification area

- To enable displaying the icon on the taskbar, select the check box.
- To disable displaying the icon on the taskbar, clear the check box.

Fingerprint tab

NOTE: The **Fingerprint** tab is available only if the computer has a fingerprint reader and the correct driver is installed.

- **Quick Actions**—Use Quick Actions to select the Security Manager task to be performed when you hold down a designated key while swiping your fingerprint.

  To assign a Quick Action to one of the listed keys, click a **(Key) + Fingerprint** option, and then select one of the available tasks from the menu.

- **Fingerprint Scan Feedback**—Displayed only when a fingerprint reader is available. Use this setting to adjust the feedback that occurs when you swipe your fingerprint.

  - **Enable sound feedback**—Security Manager gives you audio feedback when a fingerprint has been swiped, playing different sounds for specific program events. You may assign new sounds to these events through the **Sounds** tab in Windows Control Panel, or disable sound feedback by clearing this option.

  - **Show scan quality feedback**

    To display all swipes, regardless of quality, select the check box.

    To display only good-quality swipes, clear the check box.

Backing up and restoring your data

It is recommended that you back up 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 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 called importing and exporting.

NOTE: Only the data is backed up by this feature.

HP ProtectTools Security Manager must be installed on any computer that is to receive backed up data before the data can be restored from the backup file.

To back up your data:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.
2. In the left panel of the dashboard, 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 select all of the modules.
5. Verify your identity.
6. Enter a name for the storage file. By default, the file is saved to your Documents folder. Click **Browse** to specify a different location.
7. Enter a password to protect the file.
8. Click **Finish**.

To restore your data:

1. Open the Security Manager dashboard. For more information, refer to Opening Security Manager on page 24.
2. In the left panel of the dashboard, click **Advanced**, and then click **Backup and Restore**.
3. Click **Restore data**.
4. Select the previously created storage file. Enter the path in the field provided, or click **Browse**.
5. Enter the password used to protect the file.
6. Select the modules for which you want to restore data. In most cases, you will select all of the modules listed.
7. Verify your Windows password.
8. Click **Finish**.

5 Drive Encryption for HP ProtectTools (select models only)

Drive Encryption for HP ProtectTools provides complete data protection by encrypting your computer hard drive. When Drive Encryption is activated, you must log in at the Drive Encryption login screen, which is displayed before the Windows® operating system starts.

The HP ProtectTools Security Manager Setup Wizard allows Windows administrators to activate Drive Encryption, back up the encryption key, and select or deselect drive(s). Refer to the HP ProtectTools Security Manager software Help for more information.

The following tasks can be performed with Drive Encryption:

- Selecting Drive Encryption settings:
  - Activating a TPM-protected password
  - Encrypting or decrypting individual drives or partitions using software encryption
  - Encrypting or decrypting individual self-encrypting drives using hardware encryption
  - Adding further security by disabling Sleep or Standby to ensure that Drive Encryption pre-boot authentication is always required

NOTE: Only internal SATA and external eSATA hard drives can be encrypted.

- Creating backup keys
- Recovering a Drive Encryption key
- Enabling Drive Encryption pre-boot authentication using a password, registered fingerprint, or smart card PIN

Opening Drive Encryption

Administrators can access Drive Encryption from HP ProtectTools Administrative Console.

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click **Drive Encryption**.

General tasks

Activating Drive Encryption for standard hard drives

Standard hard drives are encrypted using software encryption. Follow these steps to activate Drive Encryption:

1. Use the HP ProtectTools Security Manager Setup Wizard to activate Drive Encryption.
2. Follow the on-screen instructions until the **Enable security features** page is displayed, and then continue with step 4 below.

– or –

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click the **+** icon to the left of **Security** to display the available options.
3. Click **Features**.
4. Select the **Drive Encryption** check box, and then click **Next**.

NOTE: If no hard drive is selected for encryption, Drive Encryption pre-boot authentication is activated, but the drive(s) will not be encrypted.

5. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt, and then click **Next**.
6. To back up the encryption key, insert the storage device into the appropriate slot.

NOTE: To save the encryption key, you must use a USB storage device with the FAT32 format. A floppy disk, USB memory stick, Secure Digital (SD) Memory Card, or MMC may be used for backup.

7. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
8. Click **Next**.

NOTE: The computer will restart.

Drive Encryption has been activated. Encryption of the drive might take a number of hours, depending on the size of the drive.

Refer to the HP ProtectTools Security Manager software Help for more information.

Activating Drive Encryption for self-encrypting drives

Self-encrypting drives meeting Trusted Computing Group's OPAL specification for self-encrypting drive management can be encrypted using either software encryption or hardware encryption. Follow these steps to activate Drive Encryption for self-encrypting drives:

1. Use the HP ProtectTools Security Manager Setup Wizard to activate Drive Encryption.
2. Follow the on-screen instructions until the **Enable security features** page is displayed, and then continue with step 4 under either “Software encryption” or “Hardware encryption” below.

NOTE: If your computer does not have a self-encrypting drive meeting Trusted Computing Group's OPAL specification for self-encrypting drive management, then the hardware encryption option is not available, and software encryption is used by default.

If there is a mix of self-encrypting drives and standard hard drives, then the hardware encryption option is not available, and software encryption is used by default.

– or –

Software encryption

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click the **+** icon to the left of **Security** to display the available options.
3. Click **Features**.
4. Select the **Drive Encryption** check box, and then click **Next**.
5. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt, and then click **Next**.
6. To back up the encryption key, insert the storage device into the appropriate slot.

   NOTE: To save the encryption key, you must use a USB storage device with the FAT32 format. A floppy disk, USB memory stick, Secure Digital (SD) Memory Card, or MMC may be used for backup.
7. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
8. Click **Apply**.

   NOTE: The computer will restart.

   Drive Encryption has been activated. Encryption of the drive might take a number of hours, depending on the size of the drive.

Hardware encryption

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click the **+** icon to the left of **Security** to display the available options.
3. Click **Features**.
4. Select the **Drive Encryption** check box, and then click **Next**.

   NOTE: If only one drive is shown, the drive check box is automatically selected and grayed out.

   If more than one drive is shown, the drive check boxes are automatically selected but not grayed out.

   The **Next** button is not available until at least one drive has been selected.

5. Be sure that the **Use hardware drive encryption** check box is selected at the bottom of the screen.
6. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt, and then click **Next**.
7. To back up the encryption key, insert the storage device into the appropriate slot.

NOTE: To save the encryption key, you must use a USB storage device with the FAT32 format. A floppy disk, USB memory stick, Secure Digital (SD) Memory Card, or MMC may be used for backup.

8. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
9. Click **Apply**.

NOTE: The computer will need to be restarted.

Drive Encryption has been activated. Encryption of the drive might take several minutes.

Refer to the HP ProtectTools Security Manager software Help for more information.

Deactivating Drive Encryption

Administrators can use the HP ProtectTools Security Manager Setup Wizard to deactivate Drive Encryption. Refer to the HP ProtectTools Security Manager software Help for more information.

▲ Follow the on-screen instructions until the **Enable security features** page is displayed, and then continue with step 4 below.

– or –

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click the **+** icon to the left of **Security** to display the available options.
3. Click **Features**.
4. Clear the **Drive Encryption** check box, and then click **Next**.

   Drive Encryption deactivation begins.

NOTE: If software encryption was used, decryption starts. It might take a number of hours, depending on the size of the drive. When decryption is complete, Drive Encryption is deactivated.

If hardware encryption was used, the drive is instantly decrypted, which might take a few minutes, and then Drive Encryption is deactivated.

Once the drive is deactivated, the computer will need to be restarted.

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 login screen:

NOTE: In a hardware encryption scenario, be sure that the computer is turned off. If the computer is not turned off and then restarted, the Drive Encryption pre-boot authentication screen is not displayed.

NOTE: When waking from Sleep or Standby, Drive Encryption pre-boot authentication is not displayed for software or hardware encryption, unless it is disabled.

When waking from Hibernation, Drive Encryption pre-boot authentication is displayed.

NOTE: If the Windows administrator has enabled pre-boot Security in HP ProtectTools Security Manager, you can log in to the computer immediately after the computer is turned on, rather than at the Drive Encryption login screen.

1. Click your user name, and then enter your Windows password or smart card PIN, or swipe a registered finger.

NOTE: The following smart cards are supported:

Smart cards

- ActivIdentity 64K V2C Smart Card
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

PCMCIA readers

- Express Card 54 SCR3340 internal reader
- SCR 201
- SCR 243 (also HP branded)
- ActivCard
- Omnikey 4040
- Cisco

USB readers

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP Smart Card terminal

2. Click **OK**.

NOTE: If you use a recovery key to log in at the Drive Encryption login screen, you are prompted to authenticate with your password, smart card PIN, or registered finger at the Windows login screen.

Protect your data by encrypting your hard drive

It is highly recommended that you use the HP ProtectTools Security Manager Setup Wizard to protect your data by encrypting your hard drive:

1. In the left pane, click the **+** icon to the left of **Drive Encryption** to display the available options.
2. Click **Settings**.
3. For software-encrypted drives, select the drive partitions to be encrypted.

NOTE: This also applies to a mixed-drive scenario where one or more standard hard drives and one or more self-encrypting drives are present.

– or –

▲ For hardware-encrypted drives, select the drive(s) to be encrypted. At least one drive must be selected.

Displaying encryption status

Users can display encryption status from HP ProtectTools Security Manager.

NOTE: Administrators can change Drive Encryption status by using HP ProtectTools Administrative Console.

1. Open HP ProtectTools Security Manager.
2. Under **My Data**, click **Drive Encryption**.

   In a software encryption scenario, one of the following status codes is displayed under **Drive Status**:

   - Enabled
   - Disabled
   - Not encrypted
   - Encrypted
   - Encrypting
   - Decrypting

   In a hardware encryption scenario, the following status code is displayed under **Drive Status**:

   - Encrypted

   If the hard drive is in the process of being encrypted or decrypted, a progress bar displays the percentage completed and the time remaining to complete the encryption or decryption.

Advanced tasks

Managing Drive Encryption (administrator task)

Administrators can use the Settings page under Drive Encryption to view and change the status of Drive Encryption (enabled, inactive, or hardware encryption was activated) and to view the encryption status of all of the hard drives on the computer.

NOTE: Hardware encryption cannot be changed on the Settings page.

- If the status is Disabled, Drive Encryption has not yet been activated by the Windows administrator and is not protecting the hard drive. Use the HP ProtectTools Security Manager Setup Wizard to activate Drive Encryption.
- If the status is Enabled, Drive Encryption has been activated and configured. The drive is in one of the following states:

Software encryption

- Not encrypted
- Encrypted
- Encrypting
- Decrypting

Hardware encryption

- Encrypted

Encrypting or decrypting individual drives (software encryption only)

Administrators can use the Settings page to encrypt one or more hard drives on the computer or decrypt a drive that has already been encrypted.

1. Open HP ProtectTools Administrative Console.
2. In the left pane, click the **+** icon to the left of **Drive Encryption** to display the available options.
3. Click **Settings**.
4. Under **Drive Status**, select or clear the check box next to each hard drive you want to encrypt or decrypt, and then click **Apply**.

NOTE: When the drive is being encrypted or decrypted, the progress bar displays the time remaining to complete the process during the current session.

If the computer is shut down or initiates Sleep/Standby or Hibernation during the encryption process and then restarts, the time remaining on the progress bar resets to the beginning, but the actual encryption resumes where it last stopped. The progress bar, shown as a percentage, and the time remaining change more quickly to reflect the previous progress.

NOTE: Dynamic partitions are not supported. If a partition is displayed as available, but it cannot be encrypted when selected, the partition is dynamic. A dynamic partition results from shrinking a partition to create a new partition within Disk Management.

A warning is displayed if a partition will be converted to a dynamic partition.

Backup and recovery (administrator task)

When Drive Encryption is activated, administrators can use the Encryption Key Backup page to back up encryption keys to removable media and to perform a recovery.

Backing up encryption keys

Administrators can back up the encryption key for an encrypted drive on a removable storage device.

CAUTION: Be sure to keep the storage device containing the backup key in a safe place, because if you forget your password, lose your smart card, or do not have a finger registered, this device provides your only access to your hard drive.

1. Open HP ProtectTools Administrative Console.
2. In the left pane, click the **+** icon to the left of **Drive Encryption** to display the available options.
3. Click **Encryption Key Backup**.
4. Insert the storage device being used to back up the encryption key.
5. Under **Drive**, select the check box for the device where you want to back up your encryption key.
6. Click **Backup Keys**.
7. Read the information on the page that is displayed, and then click **Next**. The encryption key is saved on the storage device you selected.

Recovering encryption keys

Administrators can recover an encryption key from the removable storage device where it was saved previously:

1. Turn on the computer.
2. Insert the removable storage device that contains your backup key.
3. When the Drive Encryption for HP ProtectTools login dialog box opens, click **Options**.
4. Click **Recovery**.
5. Select the file that contains your backup key or click **Browse** to search for it, and then click **Next**.
6. When the confirmation dialog box opens, click **OK**.

   Your computer starts.

NOTE: It is highly recommended that you reset your password after performing a recovery.

6 Privacy Manager for HP ProtectTools (select models only)

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

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

- Fingerprint authentication
- Windows® password
- Smart card
- Face recognition

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

Opening Privacy Manager

To open Privacy Manager:

- To access Outlook-specific features in Microsoft Outlook, click **Send Securely** in the **Privacy** group on the **Message** tab.
- To access most features in Microsoft Office documents, click **Sign and Encrypt** in the **Privacy** group on the **Home** tab.
- To access additional features, access the HP ProtectTools Security Manager dashboard.
  - Click **Start**, click **All Programs**, click **HP**, click **HP ProtectTools Security Manager**, and then click **Privacy Manager**.

    – or –
  - Click the **HP ProtectTools** desktop gadget icon.

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

Setup procedures

Managing Privacy Manager Certificates

Privacy 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.

Certificate Manager allows you to perform the following tasks:

- Requesting a Privacy Manager Certificate on page 53
- Obtaining a preassigned Corporate Privacy Manager Certificate on page 54
- Setting a default Privacy Manager Certificate on page 55
- Importing a third-party certificate on page 54
- Viewing Privacy Manager Certificate details on page 55
- Renewing a Privacy Manager Certificate on page 55
- Setting a default Privacy Manager Certificate on page 55
- Deleting a Privacy Manager Certificate on page 56
- Restoring a Privacy Manager Certificate on page 56
- Revoking your Privacy Manager Certificate on page 56

Requesting 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.

1. Open Privacy Manager, and then click **Certificates**.
2. Click **Request a Privacy Manager Certificate**.
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.

Obtaining a preassigned Corporate Privacy Manager Certificate

1. In Outlook, open the e-mail that you received indicating that a Corporate Certificate has been preassigned to you.
2. Click **Obtain**.

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

To install the certificate, refer to Setting up a Privacy Manager Certificate on page 54.

Setting up a Privacy Manager Certificate

1. When you receive the e-mail with your Privacy Manager Certificate attached, open the e-mail, and then click the **Setup** button in the lower-right corner of the message in Outlook 2007 or Outlook 2010, or in the upper-left corner in Outlook 2003.
2. Authenticate using your chosen security login 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 login method.
7. If you choose to begin the Trusted Contact invitation process, follow the on-screen instructions beginning with step 2 of the topic Adding Trusted Contacts using Microsoft Outlook contacts on page 58.

   – or –

   If you click **Cancel**, refer to Managing Trusted Contacts on page 57 for information on adding a Trusted Contact at a later time.

Importing a third-party certificate

You may be able to import a third-party certificate into Privacy Manager through the Certificate Import Wizard.

To use this feature, the **Allow use of third-party certificates** setting in HP ProtectTools Administrative Console must have been enabled on the Settings page under **Privacy Manager**.

1. Open Privacy Manager, and then click **Certificates**.
2. Select the **Certificate Manager** tab, and then click **Import certificates**.

   This button is not displayed if importing certificates is not allowed.

3. Choose whether to import a certificate already installed on this computer or a certificate stored as a PFX (Personal Information Exchange/PKCS#12) file, and then click **Next**.

   - To import a certificate installed on this computer, select the desired certificate, and then click **Next**.
   - To select a PFX certificate, click **Browse**, navigate to the location of the PFX file, and then click **Next**. Type the PFX file password, and then click **Next**.

4. When the import process is complete, click **Next**.
5. You are given the option to back up the imported certificate.

   It is recommended that you back up your certificate to a location other than your computer's hard drive.

Viewing Privacy Manager Certificate details

1. Open Privacy Manager, and then click **Certificates**.
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. Open Privacy Manager, and then click **Certificates**.
2. Click **Renew certificate**.
3. Follow the on-screen instructions to obtain a new Privacy Manager Certificate.

NOTE: The Privacy Manager Certificate renewal process does not replace your old Privacy Manager Certificate. You must obtain a new Privacy Manager Certificate and install it using the same procedures as in Requesting a Privacy Manager Certificate on page 53.

For corporate certificates issued by your company using Microsoft Certificate Authority, the CA administrator must renew your certificate using the same private key as the original certificate, or issue you a new certificate using the same private key.

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 installed from within Privacy Manager, you can specify one as the default certificate:

1. Open Privacy Manager, and then click **Certificates**.
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. Refer to Restoring a Privacy Manager Certificate on page 56 for more information.

To delete a Privacy Manager Certificate:

1. Open Privacy Manager, and then click **Certificates**.
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

During installation of your Privacy Manager Certificate, you are required to create a backup copy of the certificate. You may also create a backup copy from the Migration page. This backup copy can be used when migrating to another computer, or to restore a certificate to the same computer.

1. Open Privacy Manager, and then click **Migration**.
2. Click **Restore**.
3. On the Migration File page, click **Browse** to search for the .dppsm file that you created during the backup process, and then click **Next**.
4. Enter the password you used when you created the backup, and then click **Next**.
5. Click **Finish**.

Refer to Setting up a Privacy Manager Certificate on page 54 or Backing up Privacy Manager Certificates and Trusted Contacts on page 66 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. Open Privacy Manager, and then click **Certificates**.
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 login 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.

Trusted Contacts Manager allows you to perform the following tasks:

- View Trusted Contact details
- Delete Trusted Contacts
- Check revocation status for Trusted Contacts (advanced)

Adding Trusted Contacts

Adding Trusted Contacts is a 3-step process:

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 then 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.

Refer to the following sections to add Trusted Contacts.

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 Web site at http://digitalpersona.com/privacymanager/download.

Adding a Trusted Contact

1. Open Privacy Manager, click **Trusted Contacts Manager**, and then click **Invite Contacts**.

   – 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 the 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. Refer to Requesting a Privacy Manager Certificate on page 53 for more information.

7. Authenticate using your chosen security login method.

NOTE: When the e-mail is received by the Trusted Contact recipient, the recipient must open the e-mail, click **Accept** in the lower-right corner of the e-mail, and then click **OK** when the confirmation dialog box opens.

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 Microsoft Outlook contacts

1. Open Privacy Manager, click **Trusted Contacts Manager**, and then click **Invite Contacts**.

   – or –

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

2. When the Trusted Contact Invitation page opens, select the e-mail addresses 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. Refer to Requesting a Privacy Manager Certificate on page 53 for more information.

6. Authenticate using your chosen security login method.

NOTE: When the e-mail is received by the Trusted Contact recipient, the recipient must open the e-mail, click **Accept** in the lower-right corner of the e-mail, and then click **OK** when the confirmation dialog box opens.

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. Open Privacy Manager, and then click **Trusted Contacts**.
2. Click a Trusted Contact.
3. Click **Contact details**.
4. When you have finished viewing the details, click **OK**.

Deleting a Trusted Contact

1. Open Privacy Manager, and then click **Trusted Contacts**.
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

To see if a Trusted Contact has revoked their Privacy Manager Certificate:

1. Open Privacy Manager, and then click **Trusted Contacts**.
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

You can use Privacy Manager with the following Microsoft products:

- Microsoft Outlook
- Microsoft Office

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. When you click the down arrow next to **Privacy** or **Send Securely**, you can choose from the following options:

- **Sign and send message** (Send Securely button only)—This option adds a digital signature to the e-mail and sends it after you authenticate using your chosen security login method.
- **Seal for Trusted Contacts and send message** (Send Securely button only)—This option adds a digital signature, encrypts the e-mail, and sends it after you authenticate using your chosen security login method.
- **Invite contacts**—This option allows you to send a Trusted Contact invitation. Refer to Adding a Trusted Contact on page 57 for more information.
- **Invite Outlook contacts**—This option allows you to send a Trusted Contact invitation to all the contacts in your Microsoft Outlook address book. Refer to Adding Trusted Contacts using Microsoft Outlook contacts on page 58 for more information.
- **Open the Privacy Manager software**—Certificates, Trusted Contacts, and Settings options allow you to open the Privacy Manager software to add, view, or change current settings. Refer to Managing Privacy Manager Certificates on page 53, Managing Trusted Contacts on page 57, or Configuring Privacy Manager for Microsoft Outlook on page 60 for more information.

Configuring Privacy Manager for Microsoft Outlook

1. Open Privacy Manager, click **Settings**, and then click the **E-mail** tab.

   – or –

   On the main Microsoft Outlook toolbar, click the down arrow next to **Send Securely** (**Privacy** in Outlook 2003), 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** (**Privacy** in Outlook 2003), and then click **Sign and Send**.

4. Authenticate using your chosen security login 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** (**Privacy** in Outlook 2003), and then click **Seal for Trusted Contacts and Send**.

4. Authenticate using your chosen security login 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

Using Privacy Manager in a Microsoft Office 2007 document

After you install your Privacy Manager Certificate, a Sign and Encrypt button is displayed on the right side of the toolbar of all Microsoft Word, Microsoft Excel, and Microsoft PowerPoint documents. When you click the down arrow next to **Sign and Encrypt**, you can choose from the following options:

- **Sign Document**—This option adds your digital signature to the document.
- **Add Signature Line Before Signing** (Microsoft Word and Microsoft Excel only)—By default, a signature line is added when a Microsoft Word or Microsoft Excel document is signed or encrypted. To turn this option off, click **Add Signature Line** to remove the check mark.
- **Encrypt Document**—This option adds your digital signature and encrypts the document.
- **Remove Encryption**—This option removes encryption from the document.
- **Open the Privacy Manager software**—Certificates, Trusted Contacts, and Settings options allow you to open the Privacy Manager software to add, view, or change current settings. Refer to Managing Privacy Manager Certificates on page 53, Managing Trusted Contacts on page 57, or Configuring Privacy Manager for Microsoft Office on page 62 for more information.

Configuring Privacy Manager for Microsoft Office

1. Open Privacy Manager, 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 login 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 login 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: The owner of the document assigns suggested signers to his or her document. The **Show sign date in signature line** and/or **Show signer's title in signature line** check boxes must be selected in order for the suggested signer to be able to display the date and/or title in the signature line.

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 login 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 then click the individual names.

5. Click **OK**.

If you later decide to edit the document, follow the steps in Removing encryption from a Microsoft Office document on page 64. When the encryption is removed, you can edit the document. Follow the steps in this section to encrypt the document again.

Removing 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 login 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 would for 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 on page 61 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 Digital Signatures icon is displayed in the status bar at the bottom of the document window.

1. Click the **Digital Signatures** icon to toggle display of the Signatures dialog box, which displays the name of all users who signed the document and the date each user signed it.
2. To view additional details about each signature, right-click a name in the Signatures dialog box, and then select **Signature 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. You must also restore the Privacy Manager Certificate that was used to encrypt the file.

If your certificate has been lost, in order to view an encrypted Microsoft Office document, you must restore 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.

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 another computer, or back up your data for safekeeping. To do this, back up the data as a password-protected file to a network location or any removable storage device, and then restore the file to the new computer.

Backing up Privacy Manager Certificates and Trusted Contacts

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

1. Open Privacy Manager, and then click **Migration**.
2. Click **Backup**.
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 restore the migration file.

6. Authenticate using your chosen security login method.
7. On the Migration File Saved page, click **Finish**.

Restoring Privacy Manager Certificates and Trusted Contacts

To restore your Privacy Manager Certificates and Trusted Contacts on a different computer as part of the migration process, or to the same computer, follow these steps:

1. Open Privacy Manager, and then click **Migration**.
2. Click **Restore**.
3. On the Migration File page, click **Browse** to search for the file, and then click **Next**.
4. Enter the password you used when you created the backup file, and then click **Next**.
5. On the Migration File page, click **Finish**.

Central administration of Privacy Manager

Your installation of Privacy Manager may be part of a centralized installation that has been customized by your administrator. One or more of the following features may be either enabled or disabled:

- **Certificate use policy**—You may be restricted to the use of Privacy Manager Certificates issued by Comodo, or you may be allowed to use digital certificates issued by other certificate authorities.
- **Encryption policy**—Encryption capabilities may be individually enabled or disabled in Microsoft Office or Microsoft Outlook.

7 File Sanitizer for HP ProtectTools

File Sanitizer allows you to securely shred assets (for example: personal information or files, historical or Web-related data, or other data components) on your computer and to periodically bleach deleted assets on your hard drive.

NOTE: This version of File Sanitizer supports the computer hard drive only.

Shredding

Shredding is different than a standard Windows® delete (also known as a simple delete in File Sanitizer). When you shred an asset using File Sanitizer, the files are overwritten with meaningless data, making it virtually impossible to retrieve the original asset. A Windows simple delete may leave the file (or asset) intact on the hard drive or in a state where forensic methods could be used to recover it.

When you choose a shred profile (**High Security**, **Medium Security**, or **Low Security**), a predefined list of assets and an erasure method are automatically selected for shredding. You can also customize a shred profile, by specifying the number of shred cycles, which assets to include for shredding, which assets to confirm before shredding, and which assets to exclude from shredding. For more information, refer to Selecting or creating a shred profile on page 73.

You can set an automatic shred schedule, or you can manually activate shredding using the **HP ProtectTools** icon in the notification area, at the far right of the taskbar. For more information, refer to Setting a shred schedule on page 72, Manually shredding one asset on page 77, or Manually shredding all selected items on page 77.

NOTE: A .dll file is shredded and removed from the system only if it has been moved to the Recycle Bin.

Free space bleaching

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.

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 can be performed occasionally for assets that you delete by selecting **Simple Delete Settings** in File Sanitizer, by moving the assets to the Windows Recycle Bin, or by deleting the assets manually. 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. For more information, refer to Setting a free space bleaching schedule on page 72 or Manually activating free space bleaching on page 78.

Opening File Sanitizer

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

– or –

- Double-click the **File Sanitizer** icon on your desktop.

– or –

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

Setup procedures

Setting a shred schedule

You can select a predefined shred profile or create your own shred profile. For more information, refer to Selecting or creating a shred profile on page 73. You can also shred assets manually at any time. For more information, refer to Using a key sequence to initiate shredding on page 76.

NOTE: A scheduled task starts at a specific time. If the system is turned off or is in Sleep/Standby at the scheduled time, File Sanitizer will not attempt to relaunch the task.

1. Open File Sanitizer, and then click **Shred**.
2. Select one or more shred options:
   - **Windows shutdown**—Shreds all selected assets when Windows shuts down.

     NOTE: A dialog box opens at shutdown, asking if you want to continue with shredding selected assets or if you want to bypass the procedure.

     Click **Yes** to bypass the shred procedure, or click **No** to continue with shredding.
   - **Web browser open**—Shreds all selected Web-related assets, such as browser URL history, when you open a Web browser.
   - **Web browser quit**—Shreds all selected Web-related assets, such as browser URL history, when you close a Web browser.
   - **Key sequence**—Allows you to specify a key sequence to initiate shredding. For details, refer to Using a key sequence to initiate shredding on page 76.

   NOTE: A .dll file is shredded and removed from the system only if it has been moved to the Recycle Bin.
3. To schedule a future time to shred selected assets, select the **Activate Scheduler** check box, enter your Windows password, and then select a day and time.
4. Click **Apply**.

Setting a free space bleaching schedule

Free space bleaching can be performed occasionally for assets that you delete by selecting **Simple Delete Settings** in File Sanitizer, by moving the assets to the Windows Recycle Bin, or by deleting the assets manually. Free space bleaching provides no additional security to shredded assets.

NOTE: A scheduled task starts at a specific time. If the system is turned off or is in Sleep/Standby at the scheduled time, File Sanitizer will not attempt to relaunch the task.

1. Open File Sanitizer, and then click **Bleaching**.
2. To schedule a future time to bleach deleted assets on your hard drive, select the **Activate Scheduler** check box, enter your Windows password, and then select a day and time.
3. Click **Apply**.

NOTE: The free space bleaching operation can take a significant length of time. Although free space bleaching is performed in the background, increased processor usage may affect your computer's performance.

Selecting or creating a shred profile

You can specify an erasure method 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, a predefined erasure method and list of assets are automatically selected. You can also view the predefined list of assets that are selected for shredding.

1. Open File Sanitizer, and then click **Settings**.
2. Click a predefined shred profile:
   - **High Security**
   - **Medium Security**
   - **Low Security**
3. To view the assets that are selected for shredding, click **View Details**.
   a. **Selected items will be shredded, and a confirmation message will be displayed. Unselected items will be shredded without a confirmation message.**—Select the check box to display a confirmation message before shredding the item, or clear the check box to shred the item without displaying a confirmation message.

   NOTE: Even if the check box for an asset is cleared, the asset will be shredded.

   b. Click **Apply**.
4. Click **Apply**.

Customizing a 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. Open File Sanitizer, click **Settings**, click **Advanced Security Settings**, and then click **View Details**.
2. Select the number of shred cycles.

NOTE: The selected number of shred cycles will be performed for each asset. For example, if you choose 3 shred cycles, an algorithm that obscures the data is executed 3 separate 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 that you specify, the less likely it is that the data can be retrieved.

3. To select the assets to be shredded:
   a. Under **Available shred options**, click an asset, and then click **Add**.
   b. To add a custom asset, click **Add Custom Option**, and then browse or type the path to the file or folder.
   c. Click **Open**, and then click **OK**.
   d. Under **Available shred options**, click the custom asset, and then click **Add**.

To remove an asset from the available shred options, click the asset, and then click **Delete**.

4. **Selected items will be shredded, and a confirmation message will be displayed. Unselected items will be shredded without a confirmation message.**—Select the check box to display a confirmation message before shredding the item, or clear the check box to shred the item without displaying a confirmation message.

NOTE: Even if the check box for an asset is cleared, the asset will be shredded.

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

5. To protect files or folders from automatic shredding:

   a. Under **Do not shred the following**, click **Add**, and then browse or type the path to the file or folder.

   b. Click **Open**, and then click **OK**.

   To remove an asset from the exclusions list, click the asset, and then click **Delete**.

6. Click **Apply**.

Customizing a simple delete profile

The simple delete profile performs a standard asset delete without shredding. You can customize a simple delete profile by specifying which assets to include, which assets to confirm before deleting, and which assets to exclude.

NOTE: If you select **Simple Delete Settings**, free space bleaching can be performed occasionally on the assets that have been deleted manually or by using the Windows Recycle Bin.

1. Open File Sanitizer, click **Settings**, click **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**, browse or type the path to the file or folder, and then click **OK**.

   c. Click the custom asset, and then click **Add**.

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

3. **Selected items will be shredded, and a confirmation message will be displayed. Unselected items will be shredded without a confirmation message.**—Select the check box to display a confirmation message before shredding the item, or clear the check box to shred the item without displaying a confirmation message.

NOTE: Even if the check box for an asset is cleared, the asset will be shredded.

To remove an asset from the delete list, click the asset, and then click **Remove**.

4. To protect assets from automatic deleting:

   a. Under **Do not delete the following**, click **Add**, and then browse or type the path to the file or folder.

   b. Click **Open**, and then click **OK**.

   To remove an asset from the exclusions list, click the asset, and then click **Delete**.

5. Click **Apply**.

General tasks

You can use File Sanitizer to perform the following tasks:

- Use a key sequence to initiate shredding—This feature allows you to create a key sequence (for example, ctrl+alt+s) to initiate shredding. For details, refer to Using a key sequence to initiate shredding on page 76.
- Use the File Sanitizer icon to initiate shredding—This feature is similar to the drag-and-drop feature in Windows. For details, refer to Using the File Sanitizer icon on page 77.
- Manually shred a specific asset or all selected assets—These features allows you to manually shred items without waiting for the regular shred schedule to be invoked. For details, refer to Manually shredding one asset on page 77 or Manually shredding all selected items on page 77.
- Manually activate free space bleaching—This feature allows you to manually activate free space bleaching. For details, refer to Manually activating free space bleaching on page 78.
- Abort a shred or free space bleaching operation—This feature allows you to stop the shred or free space bleaching operation. For details, refer to Aborting a shred or free space bleaching operation on page 78.
- View the log files—This feature allows you to view shred and free space bleaching log files, which contain any errors or failures from the last shred or free space bleaching operation. For details, refer to Viewing the log files on page 78.

NOTE: The shred or free space bleaching operation can take a significant length of time. Even though shredding and free space bleaching are performed in the background, your computer may run slower due to increased processor usage.

Using a key sequence to initiate shredding

1. Open File Sanitizer, and then click **Shred**.
2. Select the **Key sequence** check box.
3. Enter a character in the available box.
4. Select either the **CTRL** box or the **ALT** box, and then select the **SHIFT** box.

   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 shift key and either the ctrl key or the alt 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, click **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 **OK**.

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. Open File Sanitizer, and then 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 **OK**.
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, click **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**.

– or –

1. Open File Sanitizer, and then click **Shred**.
2. Click the **Shred now** button.
3. 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, click **File Sanitizer**, and then click **Bleach Now**.
2. When the confirmation dialog box opens, click **Yes**.

– or –

1. Open File Sanitizer, and then click **Free Space Bleaching**.
2. Click **Bleach Now**.
3. When the confirmation dialog box opens, click **Yes**.

Aborting a shred or free space bleaching operation

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

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

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:

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

For 64-bit systems, the log files are located on the hard drive:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_DiskBleachLog.txt

8 Device Access Manager for HP ProtectTools (select models only)

HP ProtectTools Device Access Manager controls access to data by disabling data transfer devices.

NOTE: Some human interface/input devices, such as a mouse, keyboard, TouchPad, and fingerprint reader, are not controlled by Device Access Manager. For more information, refer to Unmanaged Device Classes on page 90.

Windows® operating system administrators use HP ProtectTools Device Access Manager to control access to the devices on a system and to protect against unauthorized access:

- Device profiles are created for each user, to define the devices that they are allowed or denied permission to access.
- Just-in-time authentication (JITA) allows predefined users to authenticate themselves in order to access devices which are otherwise denied.
- Administrators and trusted users can be excluded from the restrictions on device access imposed by Device Access Manager by adding them to the Device Administrators group. This group's membership is managed using Advanced Settings.
- Device access can be granted or denied on the basis of group membership or for individual users.
- For device classes such as CD-ROM drives and DVD drives, read access and write access can be allowed or denied separately.

Opening Device Access Manager

1. Log in as an administrator.
2. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
3. In the left pane, click **Device Access Manager**.

Users can view the HP ProtectTools Device Access Manager policy using HP ProtectTools Security Manager. This console provides a read-only view.

Setup Procedures

Configuring device access

HP ProtectTools Device Access Manager offers four views:

- **Simple Configuration**—Allow or deny access to classes of devices, based on membership in the Device Administrators group.
- **Device Class Configuration**—Allow or deny access to types of devices or specific devices for specific users or groups.
- **JITA Configuration**—Configure just-in-time authentication (JITA), allowing selected users access to DVD/CD-ROM drives or removable media by authenticating themselves.
- **Advanced Settings**—Configure a list of drive letters for which Device Access Manager will not restrict access, such as the C or system drive. Membership in the Device Administrators group can also be managed from this view.

Simple Configuration

Administrators can use the **Simple Configuration** view to allow or deny access to the following classes of devices for all non–device administrators:

- All removable media (diskettes, USB flash drives, and so on)
- All DVD/CD-ROM drives
- All serial and parallel ports
- All Bluetooth® devices
- All modem devices
- All PCMCIA/ExpressCard devices
- All 1394 devices

To allow or deny access to a class of devices for all non-device administrators, follow these steps:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Simple Configuration**.
2. In the right pane, to deny access, select the check box for a device class or a specific device. Clear the check box to allow access to that device class or specific device.

   If a check box is grayed out, values affecting the access scenario have been changed from within the **Device Class Configuration** view. To reset to the factory settings, click **Reset** in the **Device Class Configuration** view.
3. Click **Apply**.

   NOTE: If the background service is not running, a dialog box opens to ask if you would like to start it. Click **Yes**.
4. Click **OK**.

Starting the background service

The first time a new policy is defined and applied, the HP ProtectTools Device Locking/Auditing background service starts automatically, and it is set to start automatically whenever the system starts.

NOTE: A device profile must be defined before the background service prompt is displayed.

Administrators can also start or stop this service:

1. In Windows 7, click **Start**, click **Control Panel**, and then click **System and Security**.

   – or –

   In Windows Vista®, click **Start**, click **Control Panel**, and then click **System and Maintenance**.

   – or –

   In Windows XP, click **Start**, click **Control Panel**, and then click **Performance and Maintenance**.

2. Click **Administrative Tools**, and then click **Services**.
3. Select the **HP ProtectTools Device Locking/Auditing** service.
4. To start the service, click **Start**.

   – or –

   To stop the service if it is running, click **Stop**.

Stopping the Device Locking/Auditing service does not stop device locking. Two components enforce device locking:

- Device Locking/Auditing service
- DAMDrv.sys driver

Starting the service starts the device driver, but stopping the service does not stop the driver.

To determine whether the background service is running, open a command prompt window, and then type `sc query flcdlock`.

To determine whether the device driver is running, open a command prompt window, and then type `sc query damdrv`.

Device Class Configuration

Administrators can view and modify lists of users and groups that are allowed or denied permission to access classes of devices or specific devices.

The **Device Class Configuration** view has the following sections:

- **Device List**—Shows all the device classes and devices that are installed on the system or that may have been installed on the system previously.
  - Protection is usually applied for a device class. A selected user or group will be able to access any device in the device class.
  - Protection may also be applied to specific devices.
- **User List**—Shows all users and groups that are allowed or denied access to the selected device class or specific device.
  - The User List entry may be made for a specific user, or for a group in which the user is a member.
  - If a user or group entry in the User List is unavailable, the setting has been inherited from the device class in the Device List or from the Class folder.
  - Some device classes, such as DVD and CD-ROM, may be further controlled by allowing or denying access separately for read and write operations.

    For other devices and classes, read and write access rights can be inherited. For example, read access may be inherited from a higher class, but write access may be specifically denied for a user or group.

    NOTE: If the **Read** check box is cleared, the access control entry has no effect on read access to the device, but read access is not denied.

    NOTE: The Administrators group cannot be added to the User List. Instead, use the Device Administrators group.

    Example 1—If a user or group is denied write access for a device or class of devices:

    The same user, the same group, or a member of the same group can be granted write access or read+write access only for a device below this device in the device hierarchy.

    Example 2—If a user or group is allowed write access for a device or class of devices:

    The same user, the same group, or a member of the same group can be denied write access or read+write access only for the same device or a device below this device in the device hierarchy.

    Example 3—If a user or group is allowed read access for a device or class of devices:

    The same user, the same group, or a member of the same group can be denied read access or read+write access only for the same device or a device below this device in the device hierarchy.

    Example 4—If a user or group is denied read access for a device or class of devices:

    The same user, the same group, or a member of the same group can be granted access or read+write access only for a device below this device in the device hierarchy.

    Example 5—If a user or group is allowed read+write access for a device or class of devices:

The same user, the same group, or a member of the same group can be denied write access or read+write access only for the same device or a device below this device in the device hierarchy.

Example 6—If a user or group is denied read+write access for a device or class of devices:

The same user, the same group, or a member of the same group can be granted read access or read+write access only for a device below this device in the device hierarchy.

Denying access to a user or group

To prevent a user or group from accessing a device or a class of devices:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click the device class that you want to configure.
   - **Device class**
   - **All devices**
   - **Individual device**
3. Under **User/Groups**, click the user or group to be denied access, and then click **Deny**.
4. Click **Apply**.

NOTE: When deny and allow settings are set at the same device level for a user, denial of access takes precedence over allowing access.

Allowing access for a user or a group

To grant permission for a user or a group to access a device or a class of devices:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click one of the following:
   - **Device class**
   - **All devices**
   - **Individual device**
3. Click **Add**.

   The Select Users or Groups dialog box opens.
4. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
5. Click a user or a group to be added to the list of available users and groups, and then click **OK**.
6. Click **OK** again.
7. Click **Allow** to grant this user access.
8. Click **Apply**.

Allowing access to a class of devices for one user of a group

To allow a user to access a class of devices while denying access to all other members of that user's group:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click the device class that you want to configure.
   - **Device class**
   - **All devices**
   - **Individual device**
3. Under **User/Groups**, select the group to be denied access, and then click **Deny**.
4. Navigate to the folder below that of the required class, and then add the specific user.
5. Click **Allow** to grant this user access.
6. Click **Apply**.

Allowing access to a specific device for one user of a group

Administrators can allow access to a specific device while denying access to all other members of that user's group for all devices in the class:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click the device class that you want to configure, and then navigate to the folder below that.
3. Under **User/Groups**, click **Allow** next to the group to be granted access.
4. Click **Deny** next to the group to be denied access.
5. Navigate to the specific device to which access is to be allowed for the user in the device list.
6. Click **Add**.

   The Select Users or Groups dialog box opens.
7. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
8. Click a user to be allowed access, and then click **OK**.
9. Click **Allow** to grant this user access.
10. Click **Apply**.

Removing settings for a user or a group

To remove permission for a user or a group to access a device or a class of devices, follow these steps:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click the device class that you want to configure.
   - **Device class**
   - **All devices**
   - **Individual device**
3. Under **User/Groups**, click the user or group you want to remove, and then click **Remove**.
4. Click **Apply**.

Resetting the configuration

⚠ **CAUTION:** Resetting the configuration discards all device configuration changes that have been made and returns all settings to the values set at the factory.

To reset the configuration settings to the factory values:

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. Click **Reset**.
3. Click **Yes** to the confirmation request.
4. Click **Apply**.

JITA Configuration

JITA Configuration 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 for which policies created in the **Device Class Configuration** or **Simple Configuration** view have been 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 who attempts to access the DVD/CD-ROM drive receives the same “access denied” message as a non-JITA-enabled user. Then a balloon message is displayed, asking if the user would like JITA access. If the balloon is clicked, the Authenticate User dialog box opens. When the user enters credentials successfully, access is granted 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. Users 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 extended, if configured to do so. In this scenario, 1 minute before the JITA period is about to expire, users can click the prompt to extend their access without having to re-authenticate.

Whether the user is given a limited or unlimited JITA period, as soon as the user logs off the system or another user logs in, the JITA period expires. The next time the user logs in and attempts to access a JITA-enabled device, a prompt to enter credentials is displayed.

JITA is available for the following device classes:

- DVD/CD-ROM drives
- Removable media

Creating a JITA for a user or group

Administrators can allow users or groups to access 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 device's drop-down menu, select either **Removable media** or **DVD/CD-ROM drives**.
3. Click **+** to add a user or group to the JITA configuration.
4. Select the **Enabled** check box.
5. Set the JITA period to the required time.
6. Click **Apply**.

The user must log out and then log in again for the new JITA setting to be applied.

Creating an extendable JITA for a user or group

Administrators can allow user or group access to devices using just-in-time authentication that the user can extend before it expires.

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

The user must log out and then log in again for the new JITA setting to be applied.

Disabling a JITA for a user or group

Administrators can disable user 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 device's drop-down menu, select either **removable media** or **DVD/CD-ROM drives**.
3. Select the user or group whose JITA you wish to disable.
4. Clear the **Enabled** check box.
5. Click **Apply**.

When the user logs in and attempts to access the device, access is denied.

Advanced Settings

Advanced Settings provides the following functions:

- Management of the Device Administrators group
- Management of drive letters to which 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. Trusted users usually include system administrators. Refer to Device Administrators group on page 89 for more information.

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.

NOTE: The Device Access Manager background services must be running when the list of drive letters is configured.

To start these services:

1. Apply a Simple Configuration policy, such as denying all non-device administrators access to removable media.

   – or –

   Open a command prompt window with Administrator privileges, and then type:

   ```
   sc start flcdlock
   ```

   Press enter.

2. When the services are started, the drive list can be edited. Enter the drive letters of devices that you do not want Device Access Manager to control.

   The drive letters are displayed for physical hard disks or partitions.

NOTE: Whether or not the system drive (typically C) is in this list, access to it will never be denied for any user.

Device Administrators group

When Device Access Manager is installed, a Device Administrators group is created.

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. Trusted users usually include system administrators.

NOTE: Adding a user to the Device Administrators group does not automatically allow the user to access devices. In the **Device Class Configuration** view, if the Users group is denied access to a device, the Device Administrators group must be granted access in order for members of the group to have access to the device. However, the **Simple Configuration** view can be used to deny access to device classes for all users who are not members of the Device Administrators group.

To add users to the Device Administrators group:

1. In the **Advanced Settings** view, click **+**.
2. Enter the user name of the trusted user.

3. Click **OK**.
4. Click **Apply**.

Alternative methods for managing membership of this group include:

- For Windows 7 Professional or Windows Vista, users can be added to this group using the standard “Local Users and Groups” Microsoft Management Console (MMC) snap-in.
- For home versions of Windows 7, Windows Vista, or Windows XP, from an account with administrator privileges, type the following in a command prompt window:

  ```
  net localgroup "Device Administrators" username /add
  ```

  In this command, “username” is the user name for the user you wish to add to this group.

eSATA Support

In order for Device Access Manager to control eSATA devices, the following must be configured:

1. The drive must be connected when the system starts up.
2. Using the **Advanced Settings** view, ensure that the eSATA drive letter is not in the list of drives for which Device Access Manager will not deny access. If the eSATA drive letter is listed, delete the drive letter, and then click **Apply**.
3. The device can be controlled using the Removable Media device class, by using either the **Simple Configuration** view or the **Device Class Configuration** view.

Unmanaged Device Classes

HP ProtectTools Device Access Manager does not manage the following device classes:

- Input/output devices
  - Biometric
  - Mouse
  - Keyboard
  - Printer
  - Plug and play (PnP) printers
  - Printer upgrade
  - Infrared human interface devices
  - Smart card reader
  - Multi-port serial
  - Disk drive
  - Floppy disk controller (FDC)

- Hard disk controller (HDC)
- Human interface device (HID) class

- Power
  - Battery
  - Advanced power management (APM) support
- Miscellaneous
  - Computer
  - Decoder
  - Display
  - Processor
  - System
  - Unknown
  - Volume
  - Volume snapshot
  - Security devices
  - Security accelerator
  - Intel® unified display driver
  - Media driver
  - Medium changer
  - Multifunction
  - Legacard
  - Net client
  - Net service
  - Net trans
  - SCSI adapter

9 Theft recovery

Computrace for HP ProtectTools (purchased separately) allows you to 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 in locating and recovering 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 left pane of Security Manager, click **Theft Recovery**.
4. To launch the Computrace Activation Wizard, click **Activate Now**.
5. Enter your contact information and your credit card payment information, or enter a prepurchased Product Key.

The Activation Wizard securely processes the transaction and sets up your user account on the Absolute Software Customer Center Web site. 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 the Customer Center:

1. Go to https://cc.absolute.com/.
2. In the **Login ID** and **Password** fields, enter the credentials you received in the confirmation e-mail, and then click **Log in**.

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 information about Computrace for HP ProtectTools.

10 Embedded Security for HP ProtectTools (select models only)

NOTE: The integrated Trusted Platform Module (TPM) embedded security chip must be installed in your computer to use Embedded Security for HP ProtectTools.

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
- 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, Credential Manager 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 sections to enable and initialize the embedded security chip.

Enabling the embedded security chip in Computer Setup

The embedded security chip must be enabled in the Quick Initialization Wizard or in the Computer Setup utility.

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. Under **Embedded Security**, if the device is hidden, select **Available**.
6. Select **Embedded security device state**, and then change the setting to **Enable**.
7. Press f10 to accept the changes to the Embedded Security configuration.
8. To save your preferences and exit Computer Setup, use the arrow keys to select **File**, select **Save Changes and Exit**, and 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.

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.

Changing the Basic User Key password

To change the Basic User Key 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 **User Settings**.
3. In the right pane, under **Basic User password**, click **Change**.
4. Type the old password, and then set and confirm the new password.
5. Click **OK**.

Advanced tasks

Administrators can perform the following tasks in Embedded Security:

- Backing up and restoring Embedded Security credentials, Embedded Security settings, and Personal Secure Drives
- Changing the owner password
- Resetting a user password
- Securely migrating user security credentials from a source platform to a destination platform

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 Administrative Console**.
2. In the left pane, click **Embedded Security**, and then click **Backup**.
3. In the right pane, click **Configure**. The HP Embedded Security for 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 Administrative Console**.
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 ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.

Changing the owner password

Administrators can change the owner password:

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

11 Localized password exceptions

At the Preboot Security level and the HP Drive Encryption level, password localization support is limited, as described in the following sections.

Windows IMEs not supported at the Preboot Security level or the HP Drive Encryption level

In Windows, the user can choose an IME (input method editor) to enter complex characters and symbols, such as Japanese or Chinese characters, by using a standard western keyboard.

IMEs are not supported at the Preboot Security or HP Drive Encryption level. A Windows password cannot be entered with an IME at the Preboot Security or HP Drive Encryption login screen, and doing so may result in a lockout situation. In some cases, Microsoft® Windows does not display the IME when the user enters the password.

For example, for some Japanese installations of Windows XP, the default IME is called Microsoft IME Standard 2002 for Japanese, which actually translates to keyboard layout E0010411. However, this is an IME, not a keyboard layout. (The keyboard layout coding scheme is reserved by Microsoft for IMEs, which extend the concept of a keyboard layout). Since this is not a keyboard layout that can be represented in the typing environment for the BIOS Preboot Security password prompt or the HP Drive Encryption password prompt, any password typed with this IME is rejected by HP ProtectTools. Microsoft IME Standard 2002 for Japanese is also different from the “Common Name” in Microsoft Windows Vista®. Windows maps some IMEs to a keyboard layout. In such cases, the IME is supported by HP ProtectTools, because the underlying keyboard layout definition (the hexadecimal code) is used.

The solution is to switch to one of the following supported keyboard layouts that translates to keyboard layout 00000411:

- Microsoft IME for Japanese
- The Japanese keyboard layout
- Office 2007 IME for Japanese—If Microsoft or a third party uses the term IME or input method editor, the input method may not actually be an IME. This can cause confusion, but the software reads the hexadecimal code representation. Thus, if an IME maps to a supported keyboard layout, then HP ProtectTools can support the configuration.

⚠ **WARNING!** When HP ProtectTools is deployed, passwords entered with a Windows IME will be rejected.

Password changes using keyboard layout that is also supported

If the password is initially set with one keyboard layout, such as U.S. English (409), and then the user changes the password using a different keyboard layout that is also supported, such as Latin American (080A), the password change will work in HP Drive Encryption, but it will fail in the BIOS if the user uses characters that exist in the latter but not in the former (for example, ē).

NOTE: Administrators can resolve this problem by using the HP ProtectTools Manage Users feature to remove the user from HP ProtectTools, selecting the desired keyboard layout in the operating system, and then running the Security Manager Setup Wizard again for the same user. The BIOS stores the desired keyboard layout, and passwords that can be typed with this keyboard layout will be properly set in the BIOS.

Another potential issue is the use of different keyboard layouts that can all produce the same characters. For example, both the U.S. International keyboard layout (20409) and the Latin American keyboard layout (080A) can produce the character é, although different keystroke sequences might be required. If a password is initially set with the Latin American keyboard layout, then the Latin American keyboard layout is set in the BIOS, even if the password is subsequently changed using the U.S. International keyboard layout.

Special key handling

- Chinese, Slovakian, Canadian French and Czech

  When a user selects one of the preceding keyboard layouts and then enters a password (for example, abcdef), the same password must be entered while pressing the shift key for lower case and the shift key and caps lock key for upper case in BIOS Preboot Security and HP Drive Encryption. Numeric passwords must be entered using the numeric keypad.

- Korean

  When a user selects a supported Korean keyboard layout and then enters a password, the same password must be entered while pressing the right alt key for lower case and the right alt key and caps lock key for upper case in BIOS Preboot Security and HP Drive Encryption.

- Unsupported characters are listed in the following table:

Language	Windows	BIOS	Drive Encryption
Arabic	The ﻻ, ﻷ, and ﻹ keys generate two characters.	The ﻻ, ﻷ, and ﻹ keys generate one character.	The ﻻ, ﻷ, and ﻹ keys generate one character.
Canadian French	ç, è, à, and é with caps lock are Ç, È, À, and É in Windows.	ç, è, à, and é with caps lock are ç, è, à, and é in the BIOS Preboot Security.	ç, è, à, and é with caps lock are ç, è, à, and é in HP Drive Encryption.
Spanish	40a is not supported. It nevertheless works because the software converts it to c0a. However, because of subtle differences between the keyboard layouts, it is recommended that Spanish-speaking users change their Windows keyboard layout to 1040a (Spanish Variation) or 080a (Latin American).	n/a	n/a
US international	◦ The ¡, ¤, ‘, ’, ¥, and × keys on the top row are rejected. ◦ The å, ®, and Þ keys on the second row are rejected. ◦ The á, ð, and ø keys on the third row are rejected. ◦ The æ key on the bottom row is rejected.	n/a	n/a

Language	Windows	BIOS	Drive Encryption
Czech	◦ The ğ key is rejected. ◦ The į key is rejected. ◦ The ų key is rejected. ◦ The ė, ı, and ż keys are rejected. ◦ The ģ, ķ, ļ, ņ, and ţ keys are rejected.	n/a	n/a
Slovakian	The ż key is rejected.	◦ The š, ś, and ş keys are rejected when typed, but they are accepted when entered with the soft keyboard. ◦ The ţ dead key generates two characters.	n/a
Hungarian	The ż key is rejected.	The ţ key generates two characters.	n/a
Slovenian	The żŻ key is rejected in Windows, and the alt key generates a dead key in the BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, and Š keys are rejected in the BIOS.	n/a
Japanese	For Windows XP only, the standard Japanese keyboard layout, 411, is fully supported. One IME, commonly represented in Windows XP as Microsoft Standard IME 2002, normally would not be supported. However, empirical testing has demonstrated that this IME is a near duplicate of keyboard layout 411 when typing simple characters. The software therefore switches this IME to keyboard layout 411 when securing the BIOS and HP Drive Encryption with localized Japanese passwords. When available, Microsoft Office 2007 IME is a better choice. Despite the IME name, it is actually keyboard layout 411, which is supported.	n/a	n/a

What to do when a password is rejected

Passwords can be rejected for the following reasons:

- A user is using an IME that is not supported. This is a common issue with double-byte languages (Korean, Japanese, Chinese). To resolve this issue:

  1. Click **Start**, click **Control Panel**, and then click **Regional and Language Options**.
  2. Click the **Languages** tab.
  3. Click the **Details** button.
  4. On the **Settings** tab, click the **Add** button to add a supported keyboard (add U.S. keyboards under Chinese Input Language).
  5. Set the supported keyboard for default input.
  6. Restart HP ProtectTools, and then enter the password again.

- A user is using a character that is not supported. To resolve this issue:

  1. Change the Windows password so that it uses only supported characters. Unsupported characters are listed in Special key handling on page 104.
  2. Run the Security Manager Setup Wizard again, and then enter the new Windows password.

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 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.

ATM
Automatic Technology Manager, which allows network administrators to manage systems remotely at the BIOS level.

authentication
The 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.

background service
The HP ProtectTools Device Locking/Auditing background service, which must be running for device access control policies to be applied. It can be viewed from within the Services application under the Administrative Tools option in Control Panel. If it is not running, HP ProtectTools Security Manager attempts to start it when device access control policies are applied.

backup
Using the backup feature to save a copy of important program information to a location outside the program. It can then be used for restoring the information at a later date to the same computer or another one.

biometric
Category of authentication credentials that use a physical feature, such as a fingerprint, to identify a user.

certification authority (CA)
A service that issues the certificates required to run a public key infrastructure.

console
A central location where you can access and manage the features and settings in HP ProtectTools Administrative Console.

credentials

The means by which a user proves eligibility for a particular task in the authentication process.

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

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

dashboard
A central location where you can access and manage the features and settings in Security Manager for HP ProtectTools.

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

device access control policy
The list of devices for which a user is allowed or denied access.

device class
All devices of a particular type, such as drives.

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
A 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
Protects your data by encrypting your hard drive(s), making the information unreadable by those without proper authorization.

Drive Encryption logon screen
A logon screen that is displayed before Windows starts up. Users must enter their Windows user name and their 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 on again at the Windows logon screen.

DriveLock
A 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
A protected storage area that allows the reencryption of Basic User Keys from one platform owner key to another.

encryption
A 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.

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

fingerprint
A digital extraction of your fingerprint image. Your actual fingerprint image is never stored by Security Manager.

free space bleaching
The secure writing of random data over deleted assets to distort the contents of the deleted asset.

group
A group of users that have the same level of access or denial to a device class or a specific device.

HP SpareKey
A backup copy of the drive encryption key.

ID card
A Windows desktop gadget that serves to visually identify your desktop with your user name and chosen picture. Click the ID card to open HP ProtectTools Administrative Console.

identity
In HP ProtectTools Security Manager, a group of credentials and settings that is handled like an account or profile for a particular user.

JITA
Just-in-time authentication.

key sequence
A combination of specific keys that, when pressed, initiates an automatic shred—for example, ctrl+alt+s.

logon
An object within Security Manager that consists of a user name and password (and possibly other selected information) that can be used to log on to Web sites or other programs.

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

PIN
Personal identification number.

PKI
The Public Key Infrastructure standard that defines the interfaces for creating, using, and administering certificates and cryptographic keys.

power-on authentication
A security feature that requires some form of authentication, such as a smart card, security chip, or 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.

PSD

Personal secure drive, which provides a protected storage area for sensitive information.

reboot
The process of restarting the computer.

restore
A process that copies program information from a previously saved backup file into this program.

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.

SATA device mode
A data transfer mode between a computer and mass storage devices, such as hard drives and optical drives.

scene
A photo of an enrolled user to be used for authentication.

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

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.

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 remove 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.

Single Sign On
A feature that stores authentication information and allows you to use Security Manager to access Internet and Windows applications that require password authentication.

smart card
A small piece of hardware, similar in size and shape to a credit card, which stores identifying information about the owner. Used to authenticate the owner to a computer.

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.

token
See *security logon method*.

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

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 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.

USB token
A security device that stores identifying information about a user. Like a smart card or biometric reader, it is used to authenticate the owner to a computer.

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

virtual token
A security feature that works very much like a smart card and card reader. The token is saved either on the computer hard drive or in the Windows registry. When you log on with a virtual token, you are asked for a user PIN to complete the authentication.

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

Windows Logon Security
Protects your Windows account(s) by requiring the use of specific credentials for access.

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

Index