

# HP ProtectTools

## User Guide

© Copyright 2009 Hewlett-Packard  
Development Company, L.P.

Bluetooth is a trademark owned by its proprietor and used by Hewlett-Packard Company under license. Java is a US trademark of Sun Microsystems, Inc. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. SD Logo is a trademark of its proprietor.

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: October 2009

Document Part Number: 572661-001

---

# Table of contents

## 1 Introduction to security

HP ProtectTools features .....	2
Achieving key security objectives .....	3
Protecting against targeted theft .....	3
Restricting access to sensitive data .....	3
Preventing unauthorized access from internal or external locations .....	3
Creating strong password policies .....	4
Additional security elements .....	5
Assigning security roles .....	5
Managing HP ProtectTools passwords .....	5
Creating a secure password .....	7
Backing up and restoring HP ProtectTools credentials .....	7

## 2 Getting started

Opening HP ProtectTools Administrative Console .....	9
Enabling security features .....	10
Enrolling your fingerprints .....	11
Setting up a smart card .....	12
Using Administrative Console .....	13

## 3 Configuring your system

Setting up authentication for your computer .....	15
Logon Policy .....	15
Session Policy .....	15
Settings .....	16
Managing users .....	17
Specifying device settings .....	18
Fingerprints .....	18
Smart card .....	18

## 4 Configuring your applications

General tab .....	20
Applications tab .....	21

## 5 Adding management tools

### 6 HP ProtectTools Security Manager

Setup procedures .....	24
Getting started .....	24
Registering credentials .....	24
Enrolling your fingerprints .....	24
Changing your Windows password .....	25
Setting up a smart card .....	25
Using the Security Manager dashboard .....	25
Opening HP ProtectTools Security Manager .....	26
General tasks .....	27
Password Manager .....	27
For web pages or programs where a logon has not yet been created .....	27
For web pages or programs where a logon has already been created .....	27
Adding logons .....	28
Editing logons .....	29
Using the logons menu .....	29
Organizing logons into categories .....	29
Managing your logons .....	30
Assessing your password strength .....	30
Password Manager icon settings .....	30
Settings .....	31
Credentials .....	31
Your personal ID card .....	32
Setting your preferences .....	32
Backing up and restoring your data .....	33
Adding applications .....	34
Security Applications Status .....	34

### 7 Drive Encryption for HP ProtectTools (select models only)

Setup procedures .....	36
Opening Drive Encryption .....	36
General tasks .....	37
Activating Drive Encryption .....	37
Deactivating Drive Encryption .....	37
Logging in after Drive Encryption is activated .....	37
Protect your data by encrypting your hard drive .....	38
Displaying encryption status .....	38
Advanced tasks .....	39
Managing Drive Encryption (administrator task) .....	39
Encrypting or decrypting individual drives .....	39
Backup and recovery (administrator task) .....	39

Creating backup keys .....	39
Performing a recovery .....	40

## 8 Privacy Manager for HP ProtectTools (select models only)

Setup procedures .....	42
Opening Privacy Manager .....	42
Managing Privacy Manager Certificates .....	42
Requesting and installing a Privacy Manager Certificate .....	42
Requesting a Privacy Manager Certificate .....	43
Obtaining a preassigned Privacy Manager Corporate Certificate .....	43
Installing a Privacy Manager Certificate .....	43
Viewing Privacy Manager Certificate details .....	44
Renewing a Privacy Manager Certificate .....	44
Setting a default Privacy Manager Certificate .....	44
Deleting a Privacy Manager Certificate .....	44
Restoring a Privacy Manager Certificate .....	45
Revoking your Privacy Manager Certificate .....	45
Managing Trusted Contacts .....	45
Adding Trusted Contacts .....	46
Adding a Trusted Contact .....	46
Adding Trusted Contacts using Microsoft Outlook contacts .....	47
Viewing Trusted Contact details .....	47
Deleting a Trusted Contact .....	48
Checking revocation status for a Trusted Contact .....	48
General tasks .....	49
Using Privacy Manager in Microsoft Outlook .....	49
Configuring Privacy Manager for Microsoft Outlook .....	49
Signing and sending an e-mail message .....	49
Sealing and sending an e-mail message .....	50
Viewing a sealed e-mail message .....	50
Using Privacy Manager in a Microsoft Office 2007 document .....	50
Configuring Privacy Manager for Microsoft Office .....	51
Signing a Microsoft Office document .....	51
Adding a signature line when signing a Microsoft Word or Microsoft Excel document .....	51
Adding suggested signers to a Microsoft Word or Microsoft Excel document .....	51
Adding a suggested signer's signature line .....	52
Encrypting a Microsoft Office document .....	52
Removing encryption from a Microsoft Office document .....	53
Sending an encrypted Microsoft Office document .....	53
Viewing a signed Microsoft Office document .....	53
Viewing an encrypted Microsoft Office document .....	54
Using Privacy Manager in Windows Live Messenger .....	54

Starting a Privacy Manager Chat session .....	54
Configuring Privacy Manager for Windows Live Messenger .....	55
Chatting in the Privacy Manager Chat window .....	55
Viewing chat history .....	56
Reveal all sessions .....	56
Reveal sessions for a specific account .....	57
View a session ID .....	57
View a session .....	57
Search sessions for specific text .....	57
Delete a session .....	57
Add or remove columns .....	58
Filter displayed sessions .....	58
Advanced tasks .....	59
Migrating Privacy Manager Certificates and Trusted Contacts to a different computer .....	59
Backing up Privacy Manager Certificates and Trusted Contacts .....	59
Restoring Privacy Manager Certificates and Trusted Contacts .....	59
Central administration of Privacy Manager .....	60

## 9 File Sanitizer for HP ProtectTools

Shredding .....	62
Free space bleaching .....	63
Setup procedures .....	64
Opening File Sanitizer .....	64
Setting a shred schedule .....	64
Setting a free space bleaching schedule .....	64
Selecting or creating a shred profile .....	65
Selecting a predefined shred profile .....	65
Customizing a shred profile .....	65
Customizing a simple delete profile .....	66
General tasks .....	67
Using a key sequence to initiate shredding .....	67
Using the File Sanitizer icon .....	68
Manually shredding one asset .....	68
Manually shredding all selected items .....	68
Manually activating free space bleaching .....	69
Aborting a shred or free space bleaching operation .....	69
Viewing the log files .....	69

## 10 Device Access Manager for HP ProtectTools (select models only)

Setup Procedures .....	71
Opening Device Access Manager .....	71
Configuring device access .....	71

Device administrators group .....	71
Simple Configuration .....	71
Starting background service .....	72
Device Class Configuration .....	73
Denying access to a user or group .....	74
Allowing access for a user or a group .....	75
Removing access for a user or a group .....	75
Allowing access to a class of devices for one user of a group .....	76
Allowing access to a specific device for one user of a group .....	76
Resetting the configuration .....	76
Advanced tasks .....	78
Controlling access to the configuration settings .....	78
Granting access to an existing group or user .....	78
Denying access to an existing group or user .....	79
Adding a new group or user .....	79
Removing group or user access .....	79
Related documentation .....	79

## 11 LoJack Pro for HP ProtectTools

## 12 Troubleshooting

HP ProtectTools Security Manager .....	81
Device Access Manager for HP ProtectTools .....	83
Miscellaneous .....	85

<b>Glossary .....</b>	<b>86</b>
-----------------------	-----------

<b>Index .....</b>	<b>90</b>
--------------------	-----------





---

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


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

- Enable or disable security features
- Enroll fingerprints for users of this computer
- Set up a smart card
- Specify required credentials for authentication
- Manage users of the computer
- Adjust device-specific parameters
- Configure installed Security Manager applications
- Add additional Security Manager applications

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
Credential Manager for HP ProtectTools	<ul style="list-style-type: none"><li>• Password Manager acts as a personal password vault, streamlining the logon process with the Single Sign On feature, which automatically remembers and applies user credentials.</li><li>• Single Sign On also offers additional protection by requiring combinations of different security technologies, such as a Java™ Card and biometrics, for user authentication.</li><li>• Password storage is protected through software encryption and can be enhanced through the use of security device authentication, such as Java Cards or biometrics.</li></ul> <p><b>NOTE:</b> Credential Manager functionality is found in the Password Manager option of HP ProtectTools Security Manager</p>
Drive Encryption for HP ProtectTools (select models only)	<ul style="list-style-type: none"><li>• Drive Encryption provides complete, full-volume hard drive encryption.</li><li>• Drive Encryption forces pre-boot authentication in order to decrypt and access the data.</li></ul>
Privacy Manager for HP ProtectTools (select models only)	<ul style="list-style-type: none"><li>• Privacy Manager utilizes advanced logon techniques to verify the source, integrity, and security of communication when e-mail, Microsoft® Office documents, or instant messaging (IM) is used.</li></ul>
File Sanitizer for HP ProtectTools	<ul style="list-style-type: none"><li>• File Sanitizer allows you to securely shred digital assets (sensitive information including application files, historical or Web-related content, or other confidential data) on your computer and periodically bleach the hard drive.</li></ul>
Device Access Manager for HP ProtectTools (select models only)	<ul style="list-style-type: none"><li>• Device Access Manager allows IT managers to control access to devices based on user profiles.</li><li>• Device Access Manager prevents unauthorized users from removing data using external storage media and from introducing viruses into the system from external media.</li><li>• The administrator can disable access to writeable devices for specific individuals or groups of users.</li></ul>

## Achieving key security objectives

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

- Protecting against targeted theft
- Restricting access to sensitive data
- Preventing unauthorized access from internal or external locations
- Creating strong password policies
- Addressing regulatory security mandates

### Protecting against targeted theft

An example of 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. See the following procedures:
  - Security Manager
  - Drive Encryption

### 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 writeable device such as a CD. The following feature helps restrict access to data:

- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be printed or copied from the hard drive onto removable media.

### Preventing unauthorized access from internal or external locations

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

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. See the following procedures:
  - Password Manager
  - Drive Encryption
- 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 writeable devices so sensitive information cannot be copied from the hard drive.
- DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system.

## Creating strong password policies

If a mandate goes into effect that requires the use of strong password policy for dozens of Web-based applications and databases, 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 Java™ Cards, biometric readers, or USB tokens.

 **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 Java Cards, the IT administrator can enable Java Card BIOS security mode.
- User—Uses the security features. For example, if the security officer and IT administrator have enabled Java Cards for the system, the user can set the Java 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 this HP ProtectTools module	Function
Security Manager logon password	Security Manager	This password offers 2 options: <ul style="list-style-type: none"><li>• It can be used as a Security Manager logon to access Security Manager after logging on to Windows.</li><li>• It can be used to allow access to Windows and Security Manager simultaneously.</li></ul>
Security Manager recovery file password	Security Manager, by IT administrator	Protects access to the Security Manager recovery file.
Java™ Card PIN	Java Card Security	Protects access to the Java Card contents and authenticates users of the Java Card. When used for power-on authentication, the Java Card PIN also protects access to the

HP ProtectTools password	Set in this HP ProtectTools module	Function
		Computer Setup utility and to the computer contents.
		Authenticates users of Drive Encryption, if the Java Card token is selected.
Windows Logon password	Windows® Control Panel	Can be used for manual logon or saved on the Java Card.

## Creating a secure password

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

- Use passwords with more than 6 characters, preferably more than 8.
- Mix the case of letters throughout your password.
- Whenever possible, mix alphanumeric characters and include special characters and punctuation marks.
- Substitute special characters or numbers for letters in a key word. For example, you can use the number 1 for letters I or L.
- Combine words from 2 or more languages.
- Split a word or phrase with numbers or special characters in the middle, for example, "Mary2-2Cat45."
- Do not use a password that would appear in a dictionary.
- Do not use your name for the password, or any other personal information, such as birth date, pet names, or mother's maiden name, even if you spell it backwards.
- Change passwords regularly. You might change only a couple of characters that increment.
- If you write down your password, do not store it in a commonly visible place very close to the computer.
- Do not save the password in a file, such as an e-mail, on the computer.
- Do not share accounts or tell anyone your password.


## Backing up and restoring HP ProtectTools credentials

You can use Drive Encryption for HP ProtectTools to select and back up HP ProtectTools credentials.

---

## 2 Getting started

---

 **NOTE:** Administration of HP ProtectTools requires administrative privileges.

---

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

1. On the Welcome page, you can disable further display of the wizard by selecting one of the options.
2. After a week of setting up the computer, or when a user with administrative rights swipes a finger on the fingerprint reader for the first time, the HP ProtectTools Setup Wizard will start automatically to guide you through the basic steps in configuring the program. A video tutorial on setting up your computer starts automatically.
3. Follow the on-screen instructions until setup is complete.

If you do not complete the wizard, it will automatically launch twice more. After that, you can access the wizard from the notification balloon that appears near the taskbar notification area (unless you have disabled it as described in step 2 above) until setup has been completed.

To use the HP ProtectTools Security Manager applications, launch HP ProtectTools Security Manager from the Start menu or right-click the Security Manager icon in the notification area, located at the far right of the taskbar. HP ProtectTools Administrative Console and its applications are available to all users who share this computer.



## 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**.

For user tasks, such as registering fingerprints or using Security Manager, open the console as follows:

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

– or –

Double-click the **HP ProtectTools Security Manager** icon in the notification area, at the far right of the taskbar.

## Enabling security features

The Setup Wizard will ask you to verify your identity.

1. Read the “Welcome” screen, and then click **Next**.
2. Verify your identity, either by typing your Windows password if you do not have any enrolled fingerprints yet, or by scanning your fingerprint with the fingerprint reader. Click **Next**.


If your Windows password is blank, you will be asked 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.

The Setup Wizard will guide you through the process of enabling security features that apply to all users of the computer:

- Windows Logon Security protects your Windows account(s) by requiring the use of specific credentials for access.
- Drive Encryption protects your data by encrypting your hard drive(s), 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.

To enable a security feature, select the corresponding check box. The more features that you select, the more secure your computer will be.

---

 **NOTE:** Pre-Boot Security will not be available if your BIOS does not support it.


---

# Enrolling your fingerprints

If you have selected "Fingerprint" and if your computer has a fingerprint reader built in or connected, you will be guided through the process of setting up or "enrolling" your fingerprints:

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 the corresponding finger.

---

2. When you have selected a finger to enroll, you are prompted to scan that fingerprint until it 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 to 3 for another finger.
4. Click **Next**.

---

 **NOTE:** 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 dashboard, the changes you made are **not** saved.

---

## Setting up a smart card

If you have selected "Smart card" and if a smart card reader is built in or connected to your computer, the HP ProtectTools Setup Wizard will prompt you to set up a smart card PIN (personal identification number).

To set up a smart card PIN:

1. On the "Set up smart card" page, enter and confirm a PIN.

You can also change your PIN. Provide your old PIN and then choose a new one.

2. To continue, click **Next**.

# Using Administrative Console

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

The console is composed of the following components:

- **Tools**—Displays the following categories for configuring security on your computer:
  - **Home**—Allows you to select the security tasks to perform.
  - **System**—Allows you to configure security features and authentication for users and devices.
  - **Applications**—Displays general 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.
- **Management Tools**—Provides information on additional tools. The panel below displays the following choices:
  - **HP ProtectTools Setup Wizard**—Guides you through setting up HP ProtectTools Security Manager.
  - **Help**—Displays the Help file, which provides information about Security Manager and its preinstalled applications. Help for applications that you may add is provided within those applications.
  - **About**—Displays information about HP ProtectTools Security Manager, such as the version number and copyright notice.
- **Main area**—Displays application-specific screens.

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

---

## 3 Configuring your system

The System group is accessed from the Tools menu panel on the left side of the HP ProtectTools Administrative Console screen. 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.
- **Devices**—Manage settings for security devices built into or attached to the computer.

# Setting up authentication for your computer

Within the Authentication application, you can select which security features should be implemented on this computer, set policies governing access to the computer, and configure additional advanced settings. You can specify the credentials required to authenticate each class of user when logging into Windows or logging into Web sites and programs during a user session.

To set up authentication on your computer:

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

## Logon Policy

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

1. In the Tools menu, click **Security**, and then click **Authentication**.
2. On the **Logon Policy** tab, click a category of user.
3. Specify the authentication credential(s) required for the selected category of user. You must specify at least one credential.
4. Choose whether ANY (only one) of the specified credentials are required, or if ALL of the specified credentials are required in order to authenticate a user. You can also prevent any user from accessing the computer.
5. Click **Apply**.

## Session Policy

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

1. In the Tools menu, click **Security**, and then click **Authentication**.
2. On the **Session Policy** tab, click a category of user.
3. Specify the authentication credential(s) required for the selected category of user.
4. Choose whether ANY (only one) of the specified credentials are required, or if ALL of the specified credentials are required in order to authenticate a user. You can also require no authentication to access HP ProtectTools software.
5. Click **Apply**.

# Settings

You can allow one or more of the following security settings:

- **Allow One Step logon**—Allows users of this computer to skip Windows logon if authentication was performed at the BIOS or encrypted disk level.
- **Allow HP SpareKey authentication for Windows logon**—Allows users of this computer to use the HP SpareKey feature to log on to Windows despite any other authentication policy required by Security Manager.

To edit the settings:

1. Click to enable or disable a specific setting.
2. Click **Apply** to save the changes that you have made.



## 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 add additional users, click **Add**.

To delete a user, click the user, and then click **Delete**.

To enroll fingerprints or 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 click **View Policies**.

# Specifying device settings

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

## Fingerprints

The Fingerprints page has three tabs: Enrollment, Sensitivity, and Advanced.

### Enrollment

You can 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.

**⚠ WARNING!** All fingerprint data for all users, including administrators, will be erased. If the logon policy requires fingerprints only, all users may be prevented from logging on to the computer.

### Sensitivity

To adjust the sensitivity used by the fingerprint reader when it scans your fingerprints, move the slider.

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

### Advanced

You can configure the fingerprint reader to conserve power when the computer is running on battery power.

## Smart card

You can configure the computer to automatically lock when a smart card is removed. However, the computer will lock only if the smart card was used as an authentication credential when logging on to Windows. Removing a smart card that was not used to log on to Windows will not lock the computer.

▲ Select the check box to enable or disable locking the computer when the smart card is removed.

---

## 4 Configuring your applications

The Applications group is accessed from the Security Applications menu panel on the left side of HP ProtectTools Administrative Console. You can use Settings to customize the behavior of currently installed HP ProtectTools Security Manager applications.

To edit your application settings:

1. In the Tools menu, from the **Applications** group, click **Settings**.
2. Click to enable or disable a specific setting.
3. Click **Apply** to save the changes that you have made.

## 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:

- **Security Manager**—Enables the Security Manager application for all users of the computer.
- **Enable the Discover more button**—Allows all users of this computer to add applications to HP ProtectTools Security Manager by clicking the **[+] Discover more** button.

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

---

## 5 Adding management tools

Additional applications may be available for adding new management tools to Security Manager. The administrator of this computer may disable this feature through the Settings application.

To add additional management tools, click **[+] Management tools**.

You can access the DigitalPersona Web site to check for new applications, or you can set up a schedule for automatic updates.

---

## 6 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
- Set up a smart card for authentication
- Back up and restore your program data
- Add more applications


# Setup procedures

## Getting started

The HP ProtectTools Setup Wizard is displayed automatically as the default page in HP ProtectTools Security Manager until setup has been completed.

To set up Security Manager, follow these steps:

---

 **NOTE:** If neither a fingerprint reader nor a smart card is available, perform only steps 1, 5, and 6.

---

1. On the “Welcome” page, click **Next**.
2. The following page lists the authentication methods that are available on this computer. Click **Next** to continue.
3. On the “Verify Your Identity” page, type your Windows password, and then click **Next**.
4. See one or more of the following topics depending on the configuration of your computer.
  - If a fingerprint reader is available, see [Enrolling your fingerprints on page 24](#).
  - If a smart card is available, see [Setting up a smart card on page 25](#).
5. If neither a fingerprint reader nor a smart card is available, you will be asked to enter your Windows password. You must use this password in the future whenever authentication is required.
6. On the final page of the wizard, click **Finish**.

The Security Manager dashboard is displayed.

## Registering credentials

You can use the “My Identity” page to register your various authentication methods, or credentials. After they have been registered, you can use these methods to log on to Security Manager.

## Enrolling your fingerprints


If your computer has a fingerprint reader built in or connected, the HP ProtectTools Setup Wizard will guide you through the process of setting up or “enrolling” your fingerprints.

1. Read the “Welcome” screen, and then click **Next**.
2. Verify your identity, either by typing your Windows password if you do not have any enrolled fingerprints yet, or by scanning your fingerprint with the fingerprint reader. Click **Next**.

If your Windows password is blank, you will be asked 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.

3. 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 the corresponding fingerprint.

---

4. When you have selected a finger to enroll, you are prompted to scan that fingerprint until it is successfully enrolled. An enrolled finger is highlighted in green on the outline.



5. You must enroll at least two fingers; index or middle fingers are preferable. Repeat steps 3 and 4 for another finger.
6. Click **Next**.

 **NOTE:** 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 dashboard, the changes you made are **not** saved.

---

## Changing your Windows password

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

To change your Windows password, follow these steps:

1. From the Security Manager dashboard, click **My Identity**, click **Credentials**, 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 a smart card

If a smart card reader is built in or connected to your computer, Security Manager will prompt you to set up a smart card PIN (personal identification number).

- To set up a smart card PIN—On the "Set up smart card" page, enter and confirm a PIN.
- To change your PIN—First type the old PIN and then choose a new one.

## Using the Security Manager dashboard

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

The dashboard is composed of 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:
  - **My Identity**
  - **My Data**
  - **My Computer**
- **Discover more**—Opens a page where you can find additional applications to enhance the security of your identity, data, and communications.
- **Main area**—Displays application-specific screens.

- **Administration**—Opens the HP ProtectTools Administrative Console.
- **Help button**—Displays information about the current screen.
- **Advanced**—Allows you to access the following options:
  - **Preferences**—Allows you to personalize Security Manager settings.
  - **Backup and Restore**—Allows you to back up or restore data.
  - **About**—Displays version information about Security Manager.

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

## Opening HP ProtectTools Security Manager

You can open HP ProtectTools 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 **Security Manager ID Card** gadget on the Windows Sidebar.
- Press the hot key combination **ctrl+alt+h** to open the Security Manager Quick Links menu.

## General tasks

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

- **Security 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.
- **Credentials**—Provides a means to easily change your Windows password, enroll your fingerprints, or set up a smart card.

To add more applications, click the [+] **Discover more** button in the lower-left corner of the dashboard. This button may be disabled by the administrator.

## 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 don't 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.

Many Password Manager features are also available from the Password Manager icon that is displayed when a web page or program logon screen has the focus. Click the icon to display a context menu where you can choose from among the following options.

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

The following options are shown on the context menu:


- **Add [somedomain.com] to the Password Manager**—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 Password Manager software help.

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

The following options are shown on the context menu:

- **Fill in logon data**—Places your logon data in the logon fields and then submits the page (if submission was specified when the logon was created or last edited).
- **Edit logon**—Allows you to edit your logon data for this Web site.

- **Add a New Account**—Allows you to add an account to a logon.
- **Open Password Manager**—Launches the Password Manager application.
- **Help**—Displays Password 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 website 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+alt+H** hot key, scanning your fingerprint, or inserting a smart card.
  - To populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
  - To add additional fields from the screen to your logon, click **Choose other fields**.
  - To have the logon fields filled in, but not submitted, clear the **Submit logon data** check box.
  - To view the password for this logon, click **Show password**.
4. Click **OK**.

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

Each time that you access that Web site or open that program, the Password Manager icon is displayed, indicating that you can use your registered credential(s) 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 populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
  - To add additional fields from the screen to your logon, click **Choose other fields**.
  - To have the logon fields filled in, but not submitted, clear the **Submit logon data** check box.
  - To view the password for this logon, click **Show password**.
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 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** hot key combination. ctrl+alt+h is the factory setting. To change the hot key combination, click **Password Manager**, and then click **Settings**.
2. Scan your fingerprint (on computers with a built-in or connected fingerprint reader).

## Organizing logons into categories

Use categories to keep your logons in order by creating one or more categories. 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 will be highlighted as you move your mouse over them.
4. Release the mouse button when the desired category is highlighted.

Your logons are not moved to the category, but only copied to the selected category. 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 our 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 website, 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.
- **Edit a logon**—Click a logon, click **Edit**, and then change the logon data.
- **Delete a logon**—Click a logon, and then click **Delete**.

To add an additional logon for a website or program:

1. Open the logon screen for the Web site or program.
2. Click the **Password manager** icon to display its shortcut menu.
3. Click **Add additional logon**, and then follow the onscreen 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 "+" sign.

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 displays that does not already have a logon set up.
- **Exclude this screen**—Select the checkbox so that Password Manager will not prompt you again to add a logon for this logon screen.

To access additional Password Manager settings, click **Password Manager**, and then click **Settings** on the Security Manager dashboard.

## 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+alt+H**—The default hot key that opens the Password Manager Quick Links menu is **ctrl+alt+H**. To change the hot key, 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.

## Credentials

You use your Security Manager credentials to verify that you are really you. The local administrator of this computer can set up which credentials may be used to prove your identity when logging 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. Each supported credential will have an entry in the **My Identity, Credentials** group.

Available credentials, requirements, and current status are listed, and may include the following:

- Fingerprints
- Password
- Smart card

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

## 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, and as a Windows Sidebar gadget.

Clicking your ID Card in the Windows Sidebar is one of the many ways to get quick access to Security Manager.

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. From the Security Manager dashboard, click the **ID Card** in the upper left corner.
2. Click the box displaying the name you entered for your account in Windows. The system will display your Windows user name for this account.
3. To change this name, type the new name, and then click the **Save** button.

To change the displayed picture:

1. From the Security Manager dashboard, click **My Identity**, and then click **ID Card** in the upper left corner.
2. Click the **Choose picture** button, click an image, and then click the **Save** button.

## 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

The following settings are available on the General tab:

#### Appearance—Show icon on taskbar

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

The following settings are available on the Fingerprint tab:

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

To assign a Quick Action to one of the listed keys:

- Click a **(Key)+Fingerprint** option, and then click one of the available tasks from the menu.




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

- **Enable sound feedback**—Security Manager gives you audio feedback when a fingerprint has been scanned, playing different sounds for specific program events. You may assign new sounds to these events through the Sounds tab in the Windows Control Panel, or disable sound feedback by clearing this option.
- **Show scan quality feedback**—By default, Security Manager shows an image of a fingerprint with a question mark whenever the quality of a fingerprint scan is insufficient to authenticate you. You can disable display of this image by clearing this option.

## 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. On the left panel click **Advanced**, and then click **Backup and Restore**.
2. Click **Back up data**.
3. Select the modules that you want to include in the backup. In most cases, you will want to select them all.
4. Enter a name for the storage file. By default, the file will be saved to your Documents folder. Click **Browse** to specify a different location.
5. Enter a password to protect the file.
6. Verify your identity.
7. Click **Finish**.

To restore your data:


1. On the left panel click **Advanced**, and then click **Backup and Restore**.
2. Click **Restore data**.
3. Select the previously created storage file. You can enter the path in the field provided, or click **Edit**.
4. Enter the password used to protect the file.
5. Select the modules whose data you want to restore. In most cases, this would be all of the modules listed.
6. Click **Finish**.

## Adding applications

Additional applications that provide new features for this program may be available.

From the Security Manager dashboard, click **[+] Discover more** to browse additional applications.

---

 **NOTE:** If there is no **[+] Discover more** link in the lower-left portion of the dashboard, it has been disabled by the administrator of this computer.

---

## Security Applications Status

The Security Manager Applications Status page displays the overall status of your installed security applications. It shows the applications that are set up and the setup status for each. The summary is displayed automatically when you open the Security Manager dashboard, or when you click **Security Applications**.

---

# 7 Drive Encryption for HP ProtectTools (select models only)

△ **CAUTION:** If you decide to uninstall the Drive Encryption module, you must first decrypt all encrypted drives. If you do not, you will not be able to access the data on encrypted drives unless you have registered with the Drive Encryption recovery service. Reinstalling the Drive Encryption module will not enable you to access the encrypted drives.


---

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 up.

The HP ProtectTools Setup Wizard allows Windows administrators to activate Drive Encryption, back up the encryption key, add and remove users, and deactivate Drive Encryption. Refer to the HP ProtectTools Security Manager software Help for more information.

The following tasks can be performed with Drive Encryption:

- Encryption Management
  - Encrypt or decrypt individual drives

 **NOTE:** Only internal hard drives can be encrypted.

---

- Recovery
  - Create backup keys
  - Perform a recovery

# Setup procedures


## Opening Drive Encryption

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


Use the HP ProtectTools Setup Wizard to activate Drive Encryption.

 **NOTE:** This wizard is also used to add and remove users.

---

– or –

1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click **Security**, and then click **Features**.
3. Select the **Drive Encryption** check box, and then click **Next**.
4. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt.
5. 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.

---

6. Under **External storage device on which to save encryption key**, select the check box for the storage device where the encryption key will be saved.
7. Click **Apply**.

Drive encryption begins.

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

## Deactivating Drive Encryption

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

– or –


1. Click **Start**, click **All Programs**, click **HP**, and then click **HP ProtectTools Administrative Console**.
2. In the left pane, click **Security**, and then click **Features**.
3. Clear the **Drive Encryption** check box, and then click **Apply**.

Drive decryption begins.

## 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:** If the Windows administrator has enabled Pre-boot Security in the HP ProtectTools Security Manager, you will 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 type your Windows password or Java™ Card PIN, or swipe a registered finger.
2. Click **OK**.

---

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


---

## Protect your data by encrypting your hard drive

Use the HP ProtectTools Setup Wizard to protect your data by encrypting your hard drive:

1. In Security Manager, click **Getting Started**, and then click the **Security Manager Setup** icon. A demonstration that describes the Security Manager features starts. (You can also start Security Manager from the “Drive Encryption” page.)
2. In the left pane, click **Drive Encryption**, and then click **Encryption Management**.
3. Click **Change Encryption**.
4. Select the drive or drives to be encrypted.

---


 **NOTE:** It is highly recommended that you encrypt the hard drive.

---

## Displaying encryption status

Users can display encryption status from HP ProtectTools Security Manager.

---

 **NOTE:** Changes to drive encryption status must be made by using the HP ProtectTools Administrative Console.

---

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

If Drive Encryption is active, the drive status displays one of the following status codes:

- Active
- Inactive
- Not encrypted
- Encrypted
- Encrypting
- Decrypting

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)

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


- If the status is Inactive, Drive Encryption has not yet been activated in HP ProtectTools Security Manager 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 Active, Drive Encryption has been activated and configured. The drive is in one of the following states:
  - Not encrypted
  - Encrypted
  - Encrypting
  - Decrypting

## Encrypting or decrypting individual drives

To encrypt one or more hard drives on the computer or decrypt a drive that has already been encrypted, use the Change Encryption feature:

1. Open **HP ProtectTools Administrative Console**, click **Drive Encryption**, and then click **Encryption Management**.
2. Click **Change Encryption**.
3. In the Change Encryption dialog box, select or clear the check box next to each hard drive you want to encrypt or decrypt, and then click **OK**.

---

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

---

## Backup and recovery (administrator task)

The "Recovery" Page allows administrators to back up and recover encryption keys.

**Local Drive Encryption Key Backup**—Allows you to back up encryption keys to removable media when Drive Encryption is activated.

## Creating backup keys

You can back up the encryption key for an encrypted drive onto 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 or lose your Java Card, this device provides your only access to your hard drive.

---


1. Open **HP ProtectTools Administrative Console**, click **Drive Encryption**, and then click **Recovery**.
2. Click **Backup Keys**.
3. On the “Select Backup Disk” page, select the check box for the device where you want to back up your encryption key, and then click **Next**.
4. Read the information on the next page that is displayed, and then click **Next**. The encryption key is saved on the storage device you selected.
5. When the confirmation dialog box opens, click **Finish**.

## Performing a recovery

To perform a recovery if you forget your password, follow these steps:

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 **Cancel**.
4. Click **Options** in the lower-left corner of the screen, and then 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.

---



---

## 8 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 communication when using e-mail, Microsoft® Office documents, or instant messaging (IM).


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

- Fingerprint authentication
- Windows® password
- HP ProtectTools Java™ Card

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

Privacy Manager requires the following:

- HP ProtectTools Security Manager 5.00 or higher
- Windows® 7, Windows Vista® or Windows XP operating system
- Microsoft Outlook 2007 or Microsoft Outlook 2003
- Valid e-mail account

 **NOTE:** A Privacy Manager Certificate (a digital certificate) must be requested and installed from within Privacy Manager before you can access the security features. For information on requesting a Privacy Manager Certificate, refer to [Requesting and installing a Privacy Manager Certificate on page 42](#).

# Setup procedures

## Opening Privacy Manager

To open Privacy Manager:

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

– 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**.

– or –

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

– or –

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

## 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.

You can perform the following tasks:

- Request and install a Privacy Manager Certificate
- View Privacy Manager Certificate details
- Renew Privacy Manager Certificates
- When multiple certificates are available, set a default Privacy Manager Certificate to be used by Privacy Manager
- Delete and revoke a Privacy Manager Certificate (advanced)

## Requesting and installing a Privacy Manager Certificate

Before you can use the Privacy Manager features, you must request and install a Privacy Manager Certificate (from within Privacy Manager) using a valid e-mail address. The e-mail address must be set up as an account within Microsoft Outlook on the same computer from which you are requesting the Privacy Manager Certificate.

## Requesting a Privacy Manager Certificate

1. Open Privacy Manager, and 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**.
8. Click **OK** to close the certificate.

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

## Obtaining a preassigned Privacy Manager Corporate Certificate

1. In Outlook, open the email that you received indicating that a Corporate Certificate has been preassigned to you.
2. Click **Obtain**.
3. You will receive an e-mail in Microsoft Outlook with your Privacy Manager Certificate attached.
4. To install the certificate, refer to [Installing a Privacy Manager Certificate on page 43](#)

## Installing a Privacy Manager Certificate

1. When you receive the e-mail with your Privacy Manager Certificate attached, open the e-mail and click the **Setup** button, in the lower-right corner of the message in Outlook 2007, 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 47](#).

– or –

If you click **Cancel**, refer to for [Adding a Trusted Contact on page 46](#) information on adding a Trusted Contact at a later time.

## Viewing Privacy Manager Certificate details

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


 **NOTE:** The Privacy Manager Certificate renewal process does not replace your old Privacy Manager Certificate. You will need to purchase a new Privacy Manager Certificate and install it using the same procedures as in [Requesting and installing a Privacy Manager Certificate on page 42](#).

## Setting a default Privacy Manager Certificate

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

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

1. Open Privacy Manager, and 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 45](#) for more information.

To delete a Privacy Manager Certificate:

1. Open Privacy Manager, and 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 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**.
6. Click **OK**.

Refer to [Installing a Privacy Manager Certificate on page 43](#) or [Backing up Privacy Manager Certificates and Trusted Contacts on page 59](#) 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 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 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>.

---

## 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 one or more e-mail addresses of the recipients you want to add as Trusted Contacts.
5. Edit the text and sign your name (optional).
6. Click **Send**.


---

 **NOTE:** If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click **OK** to launch the Certificate Request Wizard. Refer to [Requesting and installing a Privacy Manager Certificate on page 42](#) 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 and 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 All My Outlook Contacts**.

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

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

4. Edit the text and sign your name (optional).
5. Click **Send**.


---

 **NOTE:** If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click **OK** to launch the Certificate Request Wizard. Refer to [Requesting and installing a Privacy Manager Certificate on page 42](#) 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 and 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 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 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 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
- Windows Live Messenger

### 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 (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 (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 46](#) 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 47](#) 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 [Configuring Privacy Manager for Microsoft Outlook on page 49](#) 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

 **NOTE:** Privacy Manager can be used only with Microsoft Office 2007 documents.

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 42](#), [Managing Trusted Contacts on page 45](#), or [Configuring Privacy Manager for Microsoft Office on page 51](#) 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:** Because the owner of the document assigns suggested signers to his or her document, if the **Show sign date in signature line** and/or **Show signer's title in signature line** check boxes are not selected, the suggested signer will not be able to display the date and/or title in the signature line even if the suggested signer's document settings are configured to do so.

---

8. Click **OK**.

### Adding a suggested signer's signature line

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

To sign the document:

1. Double-click the appropriate signature line.
2. Authenticate using your chosen security 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 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 53](#). 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 normally would a regular e-mail with an attachment.


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

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

1. In Microsoft Outlook, click **New** or **Reply**.
2. Type your e-mail message.
3. Attach the Microsoft Office document.
4. Refer to [Sealing and sending an e-mail message on page 50](#) 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 Signature icon displays in the status bar at the bottom of the document window.

1. Click the **Digital Signatures** icon to toggle display of the Signatures dialog, 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 and 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. In addition, 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.

## Using Privacy Manager in Windows Live Messenger

Privacy Manager adds the following secure communications features to Windows Live Messenger:

- **Secure chat**—Messages are transmitted using the SSL/TLS (Secure Sockets Layer/Transport Layer Security) over XML protocol, the same technology that ensures the security of e-commerce transactions.
- **Recipient identification**—You can verify the presence and identity of a person before sending a message.
- **Signed messages**—You can electronically sign your messages. Then, if the message is tampered with, it will be marked as invalid when the recipient receives it.
- **Hide/show feature**—You can hide any or all messages in the Privacy Manager Chat window. You can also send a message where the content is hidden. Authentication is required before the message is displayed.
- **Secure chat history**—Logs of your chat sessions are encrypted before they are saved and require authentication in order to be viewed.
- **Automatic locking/unlocking**—You can lock and unlock the Privacy Manager Chat window or set it to lock automatically after a specified period of inactivity.

## Starting a Privacy Manager Chat session

 **NOTE:** In order to use Privacy Manager Chat, both parties must have Privacy Manager and a Privacy Manager Certificate installed. For details about installing a Privacy Manager Certificate, see [Requesting and installing a Privacy Manager Certificate on page 42](#).


1. To start Privacy Manager Chat in Windows Live Messenger, perform one of the following procedures:
  - a. Right-click an online contact in Live Messenger, and then select **Start an Activity**.
  - b. Click **Start Chat**.

– or –

  - a. Double-click an online contact in Live Messenger, and then select the **See a list of activities** menu.
  - b. Click **Action**, and then click **Start Chat**.

– or –

- a. Right-click the ProtectTools icon in the notification area, click **Privacy Manager for HP ProtectTools**, and then select **Start Chat**.
- b. In Live Messenger, click **Actions: Start an Activity**, and then select **Privacy Manager Chat**.

 **NOTE:** Each user must be online in Live Messenger, and the users must be displayed in each other's Live Messenger online window. Click to select an online user.

Privacy Manager sends an invitation to the contact to start Privacy Manager Chat. When the invited contact accepts, the Privacy Manager Chat window opens. If the invited contact does not have Privacy Manager, he or she will be prompted to download it.

2. Click **Start** to begin a secure chat.

## Configuring Privacy Manager for Windows Live Messenger

1. In Privacy Manager Chat, click the **Settings** button.

– or –

In Privacy Manager, click **Settings**, and then click the **Chat** tab.

– or –

In Privacy Manager Live Messenger History Viewer, click the **Settings** button.

2. To specify the amount of time Privacy Manager Chat waits before locking your session, select a number from the **Lock session after \_ minutes of inactivity** box.
3. To specify a history folder for your chat sessions, click **Browse** to search for a folder, and then click **OK**.
4. To automatically encrypt and save your sessions when you close them, select the **Automatically save secure chat history** check box.
5. Click **OK**.

## Chatting in the Privacy Manager Chat window

After starting Privacy Manager Chat, a Privacy Manager Chat window opens in Windows Live Messenger. Using Privacy Manager Chat is similar to using basic Windows Live Messenger, except that the following additional features are available in the Privacy Manager Chat window:

- **Save**—Click this button to save your chat session to the folder specified in your configuration settings. You can also configure Privacy Manager Chat to automatically save each session when it is closed.
- **Hide all** and **Show all**—Click the appropriate button to expand or collapse the messages shown in the Secure Communications window. You can also hide or show individual messages by clicking the message header.
- **Are you there?**—Click this button to request authentication from your contact.
- **Lock**—Click this button to close the Privacy Manager Chat window and return to the Chat Entry window. To display the Secure Communications window again, click **Resume the session**, and then authenticate using your chosen security login method.

- **Send**—Click this button to send an encrypted message to your contact.
- **Send signed**—Select this check box to electronically sign and encrypt your messages. Then, if the message is tampered with, it will be marked as invalid when the recipient receives it. You must authenticate each time you send a signed message.
- **Send hidden**—Select this check box to encrypt and send a message showing only the message heading. Your contact must authenticate to read the content of the message.

## Viewing chat history

The Privacy Manager Chat: Live Messenger History Viewer displays encrypted Privacy Manager Chat session files. Sessions may be saved by clicking **Save** in the Privacy Manager Chat window, or by configuring automatic saving on the Chat tab in Privacy Manager. In the viewer, each session shows the (encrypted) Contact Screen Name, and the date and time the session began and ended. By default, sessions are shown for all e-mail accounts that you have set up. You can use the **Display history for** menu to select only specific accounts to view.

The viewer allows you to perform the following tasks:

- [Reveal all sessions on page 56](#)
- [Reveal sessions for a specific account on page 57](#)
- [View a session ID on page 57](#)
- [View a session on page 57](#)
- [Search sessions for specific text on page 57](#)
- [Delete a session on page 57](#)
- [Add or remove columns on page 58](#)
- [Filter displayed sessions on page 58](#)

To start the Live Messenger History Viewer:

- ▲ In the notification area, at the far right of the taskbar, right-click the **HP ProtectTools** icon, click **Privacy Manager: for HP ProtectTools**, and then click **Live Messenger History Viewer**.

– or –

- ▲ In a Chat session, click **History Viewer** or **History**.

## Reveal all sessions

Revealing all sessions displays the decrypted Contact Screen Name for the currently selected session(s) and all sessions in the same account.

To reveal all of your saved chat history sessions:

1. In the Live Messenger History Viewer, right-click any session, and then select **Reveal All Sessions**.
2. Authenticate using your chosen security login method.  
The Contact Screen Names are decrypted.
3. Double-click any session to view its content.



## Reveal sessions for a specific account

Revealing a session displays the decrypted Contact Screen Name for the currently selected session.


To reveal a specific chat history session:

1. In the Live Messenger History Viewer, right-click any session, and then select **Reveal Session**.
2. Authenticate using your chosen security login method.

The Contact Screen Name is decrypted.

3. Double-click the revealed session to view its content.

---

 **NOTE:** Additional sessions encrypted with the same certificate will show an unlocked icon, indicating that you can view them by double-clicking any of those sessions without additional authentication. Sessions encrypted with a different certificate will show a locked icon, indicating that further authentication is required for those sessions before viewing the Contact Screen Names or contents.

---

## View a session ID

To view a session ID:

- ▲ In the Live Messenger History Viewer, right-click any revealed session, and select **View session ID**.

## View a session

Viewing a session opens the file for viewing. If the session has not been revealed (displaying the decrypted Contact Screen Name) previously, it is revealed at the same time.

To view a Live Messenger history session:

1. In the Live Messenger History Viewer, right-click any session, and then select **View**.
2. If prompted, authenticate using your chosen security login method.

The session content is decrypted.

## Search sessions for specific text

You can only search for text in revealed (decrypted) sessions that are displayed in the viewer window. These are the sessions where the Contact Screen Name is shown in plain text.

To search for text in chat history sessions:

1. In the Live Messenger History Viewer, click the **Search** button.
2. Enter the search text, configure any desired search parameters, and then click **OK**.

Sessions that contain the text are highlighted in the viewer window.

## Delete a session

1. Select a chat history session.
2. Click **Delete**.

## Add or remove columns

By default, the 3 most used columns are displayed in the Live Messenger History Viewer. You can add additional columns to the display, or you can remove columns from the display.

To add columns to the display:

1. Right-click on any column heading, and then select **Add/Remove Columns**.
2. Select a column heading in the left panel, and then click **Add** to move it to the right panel.

To remove columns from the display:

1. Right-click on any column heading, and then select **Add/Remove Columns**.
2. Select a column heading in the right panel, and then click **Remove** to move it to the left panel.

## Filter displayed sessions

A list of sessions for all of your accounts is displayed in the Live Messenger History Viewer. You can also filter displayed sessions for the following:

- Specific accounts. For details, refer to [Displaying sessions for a specific account on page 58](#).
- Range of dates. For details, refer to [Displaying sessions for a range of dates on page 58](#).
- Different folders. For details, refer to [Displaying sessions that are saved in a folder other than the default folder on page 58](#).

### Displaying sessions for a specific account

- ▲ In the Live Messenger History Viewer, select an account from the **Display history for** menu.

### Displaying sessions for a range of dates

1. In the Live Messenger History Viewer, click the **Advanced Filter** icon.  
The Advanced Filter dialog box opens.
2. Select the **Display only sessions within specified date range** check box.
3. In the **From date** and **To date** boxes, enter the day, month, and/or year, or click the arrow next to the calendar to select the dates.
4. Click **OK**.

### Displaying sessions that are saved in a folder other than the default folder

1. In the Live Messenger History Viewer, click the **Advanced Filter** icon.
2. Select the **Use an alternate history files folder** check box.
3. Enter the folder location, or click **Browse** to search for a folder.
4. Click **OK**.

## 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 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 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 Outlook and in Windows Live Messenger.

---

## 9 File Sanitizer for HP ProtectTools

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

---

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

---


# Shredding

Shredding is different than a standard Windows® delete (also known as a simple delete in File Sanitizer) in that when you shred an asset using File Sanitizer, an algorithm that obscures the data is invoked, which makes 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 the file (or asset).

When you choose a shred profile (High Security, Medium Security, or Low Security), a predefined list of assets and an erase method is automatically selected for shredding. You can also customize a shred profile, which allows you to specify the number of shred cycles, which assets to include for shredding, which assets to confirm before shredding, and which assets to exclude from shredding. For more information, refer to [Selecting or creating a shred profile on page 65](#).

You can set up an automatic shred schedule, and you can also manually shred assets whenever you want. For more information, refer to [Setting a shred schedule on page 64](#), [Manually shredding one asset on page 68](#), or [Manually shredding all selected items on page 68](#).

---

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

---

You can set an automatic free space bleaching schedule or you can manually activate free space bleaching using the **HP ProtectTools** icon in the notification area, at the far right of the taskbar. For more information, refer to [Setting a free space bleaching schedule on page 64](#) or [Manually activating free space bleaching on page 69](#).

# Setup procedures

## Opening File Sanitizer

To open File Sanitizer:

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

– or –


- ▲ Double-click the **File Sanitizer** icon located 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**.


## Setting a shred schedule

---


 **NOTE:** For information on selecting a predefined shred profile or creating a shred profile, refer to [Selecting or creating a shred profile on page 65](#).

**NOTE:** For information on manually shredding assets, refer to [Manually shredding one asset on page 68](#).

---

1. Open File Sanitizer, and click **Shred**.
  2. Select a shred option:
    - **Windows shutdown**—Choose this option to shred all selected assets when Windows shuts down.
- 
-  **NOTE:** When this option is selected, a dialog box is displayed at shutdown, asking if you want to continue with shredding 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**—Choose this option to shred all selected Web-related assets, such as browser URL history, when you open a Web browser.
  - **Web browser quit**—Choose this option to shred all selected Web-related assets, such as browser URL history, when you close a Web browser.
  - **Key sequence**—Choose this option to initiate shredding using a key sequence.
  - **Scheduler**—Select the **Activate Scheduler** check box, enter your Windows password, and then enter a day and time to shred selected assets.

---


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

---

3. Click **Apply**, and then click **OK**.

## Setting a free space bleaching schedule

---

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


---



To set a free space bleaching schedule:

1. Open File Sanitizer, and click **Free Space Bleaching**.
2. Select the **Activate Scheduler** check box, enter your Windows password, and then enter a day and time to bleach your hard drive.
3. Click **Apply**, and then click **OK**.

---

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

---

## Selecting or creating a shred profile

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

### Selecting a predefined shred profile

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

To select a predefined shred profile:


1. Open File Sanitizer, and click **Settings**.
2. Click a predefined shred profile.
3. Click **View Details** to view the list of assets that are selected for shredding.
4. Under **Shred the following**, select the check box next to each asset that you want to confirm before shredding.
5. Click **Apply**, and then click **OK**.

### 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, and click **Settings**, click **Advanced Security Settings**, and then click **View Details**.
2. Specify the number of shred cycles.


---

 **NOTE:** The selected number of shredding cycles will be performed for each asset. For example, if you choose 3 shred cycles, an algorithm that obscures the data is executed 3 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. Select the assets you want to shred:
  - a. Under **Available shred options**, click an asset, and then click **Add**.
  - b. To add a custom asset, click **Add Custom Option**, and then browse or type the path to the file name or folder. Click **Open**, and then click **OK**. Under **Available shred options**, click the custom asset, and then click **Add**.


---

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

---

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


---

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

---

5. To protect files or folders from automatic shredding, under **Do not shred the following**, click **Add** and then browse or type the path to the file name or folder. Click **Open**, and then click **OK**.

---

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


---

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

## Customizing a simple delete profile

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

---


 **NOTE:** If you use the simple delete option, free space bleaching can be performed occasionally on the assets that have been deleted manually or by using the Windows Recycle Bin.

---

To customize a simple delete profile:

1. Open File Sanitizer, click **Settings**, click **Simple Delete Setting**, and then click **View Details**.
2. Select the assets you want to delete:
  - a. Under **Available delete options**, click an asset, and then click **Add**.
  - b. To add a custom asset, click **Add Custom Option**, enter a file name or folder name, and then click **OK**. Click the custom asset, and then click **Add**.

---

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

---

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


---

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

---

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

---

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

---


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

## 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 67](#).
- 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 68](#).
- 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 68](#) or [Manually shredding all selected items on page 68](#).
- 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 69](#).
- 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 69](#).
- 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 69](#).

---

 **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

To specify a key sequence, follow these steps:

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


To abort the operation:

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

## Viewing the log files

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

---

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

---

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

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

---

# 10 Device Access Manager for HP ProtectTools (select models only)

Windows® operating system administrators use Device Access Manager for HP ProtectTools 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.
- Users are also organized into groups, such as the predefined Device Administrator group, or groups can be defined using the Computer Management option in the Administrative Tools section of the Control Panel.
- Device access can be granted or denied on the basis of group membership.
- For device classes such as CD-ROM drives and DVD drives, read access and write access can be allowed or denied separately.

Limited users can also be granted permission to read and modify the device access control policy.

# Setup Procedures

## Opening Device Access Manager

To open Device Access Manager, follow these steps:

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

## Configuring device access

Device Access Manager for HP ProtectTools offers three views:


- The Simple Configuration view is used to allow or deny access to classes of devices for members of the Device Administrators group.
- The Device Class Configuration view is used to grant or deny access to types of devices or specific devices for specific users or groups.
- The User Access Settings view is used to specify which users can view or modify the Simple Configuration and Device Class Configuration information.

## Device administrators group

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

The system administrator can implement a simple device access control policy by denying access to a set of device classes unless a user is classified as trusted (regarding device access). The recommended way to distinguish between “device trusted” users and “not device trusted” users is to make all “device trusted” users a member of the Device Administrators group. Granting members of the Device Administrators group access to devices via the Simple Configuration or Device Class Configuration views will therefore ensure that “device trusted” users have full access to the specified set of device classes.

---

 **NOTE:** Adding a user to the Device Administrators group does not automatically allow the user to access devices. However, the Simple Configuration view can be used to grant access to the required set of device classes for “device trusted” users.

---


To add users to the Device Administrators group, follow these steps:

- For Windows 7, Vista, or XP Professional, use the standard “Local Users and Groups” MMC snap-in.
- For home versions of Windows 7, Vista®, or XP, from a privileged account, type the following in a command prompt window:

```
c:\> net localgroup "Device Administrators" username /ADD
```

## Simple Configuration

Administrators and authorized users can use the Simple Configuration view to modify access to the following classes of devices for all non–Device Administrators:

 **NOTE:** In order to use this view to read device access information, the user or group must be granted "read" access in the **User Access Settings** view. In order to use this view to modify device access information, the user or group must be granted "change" access in the **User Access Settings** view.


- All removable media (diskettes, USB flash drives, etc.)
- All DVD/CD-ROM drives
- All serial and parallel ports
- All Bluetooth® devices
- All infrared devices
- All modem devices
- All PCMCIA 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 the values back to simple settings, click the check box to clear it or set it, and then click **Yes** to confirm.


3. Click the **Save** icon.

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

4. Click **OK**.

### Starting background service

Before device profiles can be applied, HP ProtectTools Security Manager opens a dialog box to ask if you would like to start the HP ProtectTools Device Locking/Auditing background service. Click **Yes**. The background service starts and will thereafter start automatically whenever the system boots.

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

Administrators can also start or stop this service:

1. Clicking **Start**, and then click **Control Panel**.
2. Click **Administrative Tools**, and then click **Services**.
3. Search for the **HP ProtectTools Device Locking/Auditing** service.



Stopping the Device Locking/Auditing service does not stop the 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 ftdlock`.

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

## Device Class Configuration


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

 **NOTE:** In order to use this view to read device access information, the user or group must be granted "read" access in the **User Access Settings** view. In order to use this view to modify device access information, the user or group must be granted "change" access in the **User Access Settings** view.

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 user or group selected 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 of 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.

As for other devices and classes, read and write access rights can be inherited. For instance, 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 blank, then the access control entry has no effect on read access to the device. It neither grants nor denies read access to the device.

**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 read 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, 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 to be denied access.
4. Click **Deny** next to a user or group.
5. Click the **Save** icon.

---

 **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, 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 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 access for this user or group.
8. Click the **Save** icon.

## Removing access 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 the **Save** icon.

## 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, 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**, 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 the **Save** icon.

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

Administrators can grant a user 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. Click **Add**. The **Select Users or Groups** dialog box opens.
4. Click **Advanced**, and then click **Find Now** to search for the user's group that is to be denied access to all devices in the class.
5. Click the group, and then click **OK**.
6. Navigate to the specific device under the device class to which access is to be allowed for the user.
7. Click **Add**. The **Select Users or Groups** dialog box opens.
8. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
9. Click the user to be allowed access, and then click **OK**.
10. Click **Allow** to grant this user access.
11. Click the **Save** icon.

## 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, follow these steps:


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

# Advanced tasks

## Controlling access to the configuration settings

In the **User Access Settings** view, administrators specify the groups or users who are allowed to use the Simple Configuration and the Device Class Configuration pages.


---

 **NOTE:** A user or group must have "Full User Administrator rights" in order to modify the settings in the User Access Settings view.

---

- A user or group must be granted "View (Read-only) Configuration Settings" access in the User Access Settings view in order to view the Simple Configuration and Device Class Configuration information.
- A user or group must be granted "Change Configuration Settings" access in the User Access Settings view in order to change the Simple Configuration and Device Class Configuration information.

---

 **NOTE:** Even members of the Administrators group must be granted "read" access to view the Simple Configuration and Device Class Configuration views and granted "change" access to change data using the Simple Configuration and Device Class Configuration views.

---

**NOTE:** After evaluating the access levels for all users and groups, if a user does not have either Allow or Deny selected for a particular access level, the user is denied access at that level.


---

## Granting access to an existing group or user

To grant permission for an existing group or user to view or change the configuration settings, follow these steps:

1. In the left pane of **HP ProtectTools Administrative Console**, click **Device Access Manager**, and then click **User Access Settings**.
2. Click a group or user to be allowed access.
3. Under **Permissions**, click **Allow** for each type of permission to be granted for the selected group or user:

---

 **NOTE:** The permissions granted are cumulative. For example, a user who is granted "Change Configuration Settings," is automatically granted "View (Read-only) Configuration Settings" permission. A user who is granted "Full User Administrator Rights" is also granted "Change Configuration Settings" and "View (Read-only) Configuration Settings" permissions.

---

- Full User Administrator Rights
  - Change Configuration Settings
  - View (Read-only) Configuration Settings
4. Click the **Save** icon.

## Denying access to an existing group or user

To deny permission for an existing group or user to view or change the configuration settings, follow these steps:

1. In the left pane of **HP ProtectTools Administrative Console**, click **Device Access Manager**, and then click **User Access Settings**.
2. Click a group or user to be denied access.
3. Under **Permissions**, click **Deny** for each type of permission to be denied for the selected group or user:
  - Full User Administrator Rights
  - Change Configuration Settings
  - View (Read-only) Configuration Settings
4. Click the **Save** icon.

## Adding a new group or user

To grant permission for a new group or user to view or change the configuration settings, follow these steps:

1. In the left pane of **HP ProtectTools Administrative Console**, click **Device Access Manager**, and then click **User Access Settings**.
2. Click **Add**. The **Select Users or Groups** dialog box opens.
3. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
4. Click a group or user, click **OK**, and then click **OK** again.
5. Click **Allow** to grant this user access.
6. Click the **Save** icon.

## Removing group or user access

To remove permission for a group or user to view or change the configuration settings, follow these steps:

1. In the left pane of **HP ProtectTools Administrative Console**, click **Device Access Manager**, and then click **User Access Settings**.
2. Click a group or user, and then click **Remove**.
3. Click the **Save** icon.

## Related documentation

Device Access Manager for HP ProtectTools is compatible with the enterprise product HP ProtectTools Enterprise Device Access Manager. When working with the enterprise product, Device Access Manager for HP ProtectTools allows read only access to its own features.

More information about Device Access Manager for HP ProtectTools is available on the Web at <http://www.hp.com/hps/security/products>.

---


# 11 LoJack Pro for HP ProtectTools

Computrace LoJack Pro, powered by Absolute Software (purchased separately), addresses the growing problem of computers that are lost or stolen.

Activating this software enables the Computrace agent, which remains active in your computer even if the hard drive is reformatted or replaced.

LoJack Pro permits remote monitoring, management, and tracking of your computer. If your computer should be lost or stolen, Absolute's Recovery Team will assist in its recovery.\*

---

 **NOTE:** \*This feature is dependent upon geographic location. Please refer to the Absolute Software subscription agreement for additional details.

---



# 12 Troubleshooting

## HP ProtectTools Security Manager

Short description	Details	Solution
Smart cards and USB tokens are not available in Security Manager if installed after the Security Manager installation.	<p>In order to use smart cards or USB tokens in Security Manager, the supporting software (drivers, PKCS#11 providers, etc.) must be installed prior to Security Manager installation.</p> <p>If you already have Security Manager installed do the following steps after installing smart card or token supporting software:</p>	<p>Log on to Password Manager.</p> <p>In HP ProtectTools Security Manager, click <b>Password Manager</b>, click <b>Credentials</b>, and then click <b>Smart Card</b></p> <p>Restart your computer if prompted.</p>
Some application Web pages create errors that prevent the user from performing or completing tasks.	Some Web-based applications stop functioning and report errors due to the disabling functionality pattern of Single Sign On. For example, an ! in a yellow triangle is observed in Internet Explorer, indicating an error has occurred.	<p>Security Manager Single Sign On does not support all software Web interfaces. Disable Single Sign On support for the specific Web page by turning off Single Sign On support. See complete documentation on Single Sign On, which is available in the Security Manager software Help files.</p> <p>If a specific Single Sign On cannot be disabled for a given application, call HP technical support and request 3rd-level support through your HP Service contact.</p>
The option to <b>Browse for Virtual Token</b> is not displayed during the logon process.	The user cannot move the location of a registered virtual token in Password Manager because the option to browse was removed to reduce security risks.	The browse option was removed because it allowed non-users to delete and rename files and take control of Windows.
Domain administrators cannot change Windows password even with authorization.	This happens after a domain administrator logs on to a domain and registers the domain identity with Password Manager using an account with Administrator's rights on the domain and the local PC. When the domain administrator attempts to change the Windows password from Password Manager, the administrator gets an error logon failure: <b>User account restriction</b> .	Password Manager cannot change a domain user's account password through <b>Change Windows password</b> . Security Manager can only change the local PC account passwords. The domain user can change his/her password through the <b>Change password</b> option of <b>Windows security</b> , but, since the domain user does not have a physical account on the local PC, Password Manager can only change the password used to log on.
Password Manager has incompatibility issues with Corel WordPerfect 12 password GINA.	If the user logs on to Password Manager, creates a document in WordPerfect, and saves with password protection, Password Manager cannot detect or recognize, either manually or automatically, the password GINA.	HP is researching a workaround for future product enhancements.

Short description	Details	Solution
Password Manager does not recognize the <b>Connect</b> button on screen.	If the Single Sign On credentials for Remote Desktop Connection (RDP) are set to <b>Connect</b> , when Single Sign On is relaunched, it always enters <b>Save As</b> instead of <b>Connect</b> .	HP is researching a workaround for future product enhancements.
The user is unable to log on to Password Manager after transitioning from sleep mode to hibernation on Windows XP Service Pack 1 only.	After allowing system to transition into hibernation and sleep mode, the Administrator or user is unable to log on to Password Manager and the Windows logon screen remains displayed no matter which logon credential (password, fingerprint, or Java Card) is selected.	<p>Update Windows to Service Pack 2 via Windows Update. Refer to Microsoft knowledge base article 813301 at <a href="http://www.microsoft.com">http://www.microsoft.com</a> for more information on the cause of the issue.</p> <p>In order to log on, the user must select Password Manager and log on. After logging on to Password Manager, the user is prompted to log on to Windows (the user may have to select the Windows logon option) to complete the logon process.</p> <p>If the user logs on to Windows first, then the user must manually log on to Password Manager.</p>
The security <b>Restore Identity</b> process loses association with virtual token.	When user restores identity, Password Manager can lose the association with the location of the virtual token at logon screen. Even though Password Manager has the virtual token registered, the user must reregister the token to restore the association.	<p>This is currently by design.</p> <p>When uninstalling Security Manager without keeping identities, the system (server) part of the token is destroyed, so the token cannot be used anymore for logging on, even if the client part of the token is restored through identity restore.</p> <p>HP is investigating long-term options for resolution.</p>

# Device Access Manager for HP ProtectTools

**Users have been denied access to devices within Device Access Manager, but the devices are still accessible.**

- **Explanation**—Simple Configuration and/or Device Class Configuration have been used within Device Access Manager to deny users access to devices. Despite being denied access, users can still access the devices.
- **Solution:**
  - Verify that the HP ProtectTools Device Locking service has started.
  - As an administrative user, click **Control Panel**, and then click **System and Maintenance**. In the Administrative Tools window, click **Services**, and search for the **HP ProtectTools Device Locking/Auditing** service. Be sure that the service is started and that the startup type is **Automatic**

**A user has unexpected access to a device, or a user is unexpectedly denied access to a device.**

- **Explanation**—Device Access Manager has been used to deny users access to some devices and allow users access to other devices. When the user is using the system, they can access devices they believe Device Access Manager has denied and are denied access to devices they believe Device Access Manager should allow.
- **Solution:**
  - Use the Device Class Configuration within Device Access Manager to investigate the user's device settings.
  - Click **Security Manager**, click **Device Access Manager**, and then click **Device Class Configuration**. Expand the levels in the Device Class tree and review the settings applicable to this user. Check for any “Deny” permissions that may be set on the user or any Windows Group of which they may be a member, e.g., Users, Administrators.

**Allow or deny—which takes precedence?**

- **Explanation**—Within Device Class Configuration, the following configuration has been set:
  - The Allow permission has been granted to a Windows group (e.g., BUILTIN\Administrators) and the Deny permission has been granted to another Windows group (e.g., BUILTIN\Users) at the same level in the device class hierarchy (e.g., DVD/CD-ROM Drives).
  - If a user is a member of both those groups (e.g., Administrator), which takes precedence?
- **Solution:**
  - The user is denied access to the device. Deny takes precedence over Allow.
  - Access is denied because of the way in which Windows works out the effective permission for the device. One group is denied, and one group is allowed, but the user is a member of both groups. The user is denied because denying access is given precedence over allowing access.

- One workaround is to deny the Users group at the DVD/CD-ROM Drives level and to allow the Administrators group at the level below DVD/CD-ROM Drives.
- An alternate workaround is to create specific Windows groups, one for allowing access to DVD/CD and one for denying access to DVD/CD. Specific users would then be added to the appropriate group.

**The Simple Configuration view has been used to define a device access control policy, but administrative users cannot access devices.**

- **Explanation**—Simple Configuration denies access for Users and Guests and allows Device Administrators.
- **Solution:** Add the Administrative user to the Device Administrators group.

## Miscellaneous

Software Impacted— Short description	Details	Solution
Security Manager— Warning received: <b>The security application can not be installed until the HP Protect Tools Security Manager is installed.</b>	All security applications such as Java Card Security and biometrics are extendable plug-ins for the Security Manager interface. Security Manager must be installed before an HP-approved security plug-in can be loaded.	The Security Manager software must be installed before installing any security plug-in.
HP ProtectTools Security Manager—Intermittently, an error is returned when closing the Security Manager interface.	Intermittently (1 in 12 instances), an error is created by using the close button in the upper right of the screen to close Security Manager before all plug-in applications have finished loading.	<p>This is related to a timing dependency on plug-in services load time when closing and restarting Security Manager. Since PTHOST.exe is the shell housing the other applications (plug-ins), it depends on the ability of the plug-in to complete its load time (services). Closing the shell before the plug-in has had time to complete loading is the root cause.</p> <p>Allow Security Manager to complete the services loading message (seen at top of Security Manager window) and all plug-ins listed in left column. To avoid failure, allow a reasonable time for these plug-ins to load.</p>
HP ProtectTools— Unrestricted access or uncontrolled administrator privileges pose security risk.	<p>Numerous risks are possible with unrestricted access to the client PC, including the following:</p> <ul style="list-style-type: none"> <li>• Deletion of PSD</li> <li>• Malicious modification of user settings</li> <li>• Disabling of security policies and functions</li> </ul>	<p>Administrators are encouraged to follow “best practices” in restricting end-user privileges and restricting user access.</p> <p>Unauthorized users should not be granted administrative privileges.</p>

---

# 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** 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.

**authorized user** A user who has been granted permission on the User Access Settings view to view or modify configuration settings on the Simple Configuration or Device Class Configuration views.

**automatic shredding** Scheduled shredding that the user sets in File Sanitizer.

**back up** 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.

**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 the Control Panel. If it is not running, the HP ProtectTools Security Manager attempts to start it when device access control policies are applied.

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

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

**chat history session** An encrypted file that contains a record of both sides of a conversation in a chat session.

**console** A central location where you can access and manage this program's features and settings.

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

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

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

**dashboard** A central location where you can access and manage this program's features and settings.

**decryption** 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** 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 the password or Java Card PIN. Under most circumstances, entering the correct information at the Drive Encryption logon screen allows access directly into Windows without having to log in again at the Windows logon screen.

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

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

**encryption** 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)** 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** Backup copy of drive encryption key.

**ID card** A Windows Sidebar 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 the HP ProtectTools Security Manager, a group of credentials and settings that is handled like an account or profile for a particular user.

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

**key sequence** A combination of specific keys that, when pressed, initiates an automatic shred—for example, [ctrl+alt+s](#).

**Live Messenger History Viewer** A Privacy Manager Chat component that allows you to search for and view encrypted chat history sessions.

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

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

**power-on authentication** Security feature that requires some form of authentication, such as a Java 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** Process of restarting the computer.

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

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

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

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

**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 login method** The method used to log in to the computer.

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

**shred** 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 removing encryption in a Microsoft Office document.

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



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

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

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

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

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

**TXT** Trusted Execution Technology.

**USB token** Security device that stores identifying information about a user. Like a Java 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 in.

**virtual token** Security feature that works very much like a Java 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** Profile for an individual authorized to log on to a network or to an individual computer.

# Index

- A**
  - aborting a shred or bleach operation 69
  - access
    - allowing 75
    - controlling 70
    - denying 74
    - denying to existing groups or users 79
    - granting to existing groups or users 78
    - preventing unauthorized 3
  - activating
    - Drive Encryption 37
    - free space bleaching 69
  - adding
    - group 79
    - signature line 51
    - suggested signer's signature line 52
    - suggested signers 51
    - user 79
  - allowing access 75
  - Applications tab settings 21, 34
  - applications, configuring 19
  - authentication 15
- B**
  - background service 72
  - backing up
    - data 33
    - HP ProtectTools credentials 7
    - Privacy Manager
      - Certificates 59
      - Trusted Contacts 59
    - backing up 39
- C**
  - central administration 60
  - certificate, preassigned 43
  - chat history, viewing 56
  - chatting in the Communications window 55
  - configuration
    - controlling access 78
    - device class 73
    - resetting 76
    - settings 78
    - simple 71
  - configuring
    - applications 19
    - device access 71
    - HP ProtectTools Administrative Console 14
    - Privacy Manager for a Microsoft Office document 51
    - Privacy Manager for Microsoft Outlook 49
    - Privacy Manager for Windows Live Messenger 55
  - controlling device access 70
  - creating
    - backup keys 39
    - shred profile 65
  - credentials 31, 32
  - credentials, registering 24
  - customizing
    - shred profile 65
    - simple delete profile 66
- D**
  - dashboard settings 25
  - data
    - backing up 33
    - restoring 33
    - restricting access to 3
  - deactivating Drive Encryption 37
  - decrypting drives 35, 39
  - defining
    - which assets to confirm before deleting 66
    - which assets to confirm before shredding 66
  - denying access 74
  - Device Access Manager for HP ProtectTools
    - opening 71
    - troubleshooting 83
  - device class
    - allowing access for a user 76
    - configuration 73
  - device settings
    - fingerprint 18
    - smart card 18
    - specifying 18
  - device, allowing access for a user 76
  - digital certificate
    - deleting 44
    - installing 43
    - receiving 43
    - renewing 44
    - requesting 43
    - restoring 45
    - revoking 45
    - setting a default 44
    - viewing details 44
  - Drive Encryption for HP ProtectTools
    - activating 37
    - backup and recovery 39
    - deactivating 37
    - decrypting individual drives 39
    - encrypting individual drives 39
    - logging in after Drive Encryption is activated 37

- managing Drive Encryption 39
  - opening 36
- E**
- e-mail message
    - Sealing for Trusted Contacts 50
    - signing 49
    - viewing a sealed message 50
  - e-mailing an encrypted Microsoft Office document 53
  - encrypting
    - drives 35, 38, 39
    - Microsoft Office document 52
  - encryption status, displaying 38
  - Excel, adding a signature line 51
  - excluding assets from automatic deletion 66
- F**
- features, HP ProtectTools 2
  - File Sanitizer for HP ProtectTools
    - icon 68
    - opening 64
    - setup procedures 64
  - fingerprints
    - enrolling 11, 24
    - settings 18
  - free space bleaching 64
- G**
- General tab, settings 20
  - group
    - allowing access 75
    - denying access 74
    - removing 75
- H**
- HP ProtectTools Administrative Console
    - configuring 14
    - opening 9
    - using 13
  - HP ProtectTools features 2
  - HP ProtectTools Security Manager
    - opening 26
    - recovery file password 5
    - setup procedures 24
    - Setup Wizard 8
    - troubleshooting 81
- I**
- ID card 32
- J**
- Java Card Security for HP ProtectTools, PIN 5
- K**
- key security objectives 3
  - key sequence 67
- L**
- logging in to the computer 37
  - logons
    - adding 28
    - categories 29
    - editing 29
    - managing 30
    - menu 29
  - LoJack Pro for HP ProtectTools 80
- M**
- management tools, adding 22
  - managing
    - credentials 31
    - passwords 21, 27
    - users 17
  - manually shredding
    - all selected items 68
    - one asset 68
  - Microsoft Excel, adding a signature line 51
  - Microsoft Office
    - e-mailing an encrypted document 53
    - encrypting a document 52
    - removing encryption 53
    - signing a document 51
    - viewing a signed document 53
    - viewing an encrypted document 54
  - Microsoft Word, adding a signature line 51
- O**
- objectives, security 3
  - opening
    - Device Access Manager for HP ProtectTools 71
- P**
- Drive Encryption for HP ProtectTools 36
  - File Sanitizer for HP ProtectTools 64
  - HP ProtectTools Administrative Console 9
  - HP ProtectTools Security Manager 26
  - Privacy Manager for HP ProtectTools 42
- P**
- password
    - changing 25
    - guidelines 7
    - HP ProtectTools 5
    - managing 5
    - policies 4
    - secure 7
    - strength 30
  - Password Manager 27
  - predefined shred profile 65
  - preferences, setting 32
  - Privacy Manager
    - using in Windows Live Messenger 54
    - using with a Microsoft Office 2007 document 50
    - using with Microsoft Outlook 49
  - Privacy Manager Certificate
    - deleting 44
    - installing 43
    - receiving 43
    - renewing 44
    - requesting 43
    - restoring 45
    - revoking 45
    - setting a default 44
    - viewing details 44
  - Privacy Manager for HP ProtectTools
    - authentication methods 41
    - managing Privacy Manager certificates 42
    - managing trusted contacts 45
    - migrating Privacy Manager Certificates and Trusted Contacts to a different computer 59

- opening 42
- Privacy Manager
  - Certificate 42
  - security login methods 41
  - setup procedures 42
  - system requirements 41
- protecting assets from automatic shredding 66

## R

- recovery, performing 40
- registering credentials 24
- removing
  - encryption from a Microsoft Office document 53
  - group access 79
  - user access 79
- requesting a digital certificate 43
- resetting 76
- restoring
  - data 33
  - HP ProtectTools credentials 7
  - Privacy Manager Certificates and Trusted Contacts 59
- restricting
  - access to sensitive data 3
  - device access 70

## S

- sealing 50
- security
  - key objectives 3
  - roles 5
  - summary 34
- Security Applications Status 34
- security features, enabling 10
- Security Manager
  - logon password 5
  - Setup Wizard 24
- security roles 5
- selecting
  - assets for shredding 65
  - shred profile 65
- setting
  - free space bleaching schedule 64
  - shred schedule 64
- settings
  - adding 21, 25, 34
  - applications 21, 25, 34

- General tab 20
- icon 30
- Setup Wizard 8, 24
- shred cycle 65
- signing
  - e-mail message 49
  - Microsoft Office document 51
- Simple Configuration 71
- simple delete 66
- smart card
  - setting up 12
  - settings 18
- specifying security settings 16
- starting Privacy Manager Chat session 54
- suggested signer
  - adding 51
  - adding a signature line 52
- system requirements 41

## T

- theft, protecting against 3, 80
- tools, adding 22
- troubleshooting
  - Device Access Manager 83
  - miscellaneous 85
  - Security Manager 81
- Trusted Contacts
  - adding 46
  - checking revocation status 48
  - deleting 48
  - viewing details 47

## U

- unauthorized access, preventing 3
- user
  - allowing access 75
  - denying access 74
  - removing 75

## V

- viewing
  - chat history 56
  - encrypted Microsoft Office document 54
  - log files 69
  - sealed e-mail message 50
  - signed Microsoft Office document 53

## W

- Windows Live Messenger, chatting 55
- Windows Logon password Wizard
  - HP ProtectTools Setup 8
- Word, adding a signature line 51

