

HP ProtectTools

User Guide

© Copyright 2008 Hewlett-Packard
Development Company, L.P.

Microsoft and Windows are U.S. registered
trademarks of Microsoft Corporation.
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. 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: June 2008

Document Part Number: 481201-001

Table of contents

1 Introduction to security

| | |
|--|----|
| HP ProtectTools features | 2 |
| Accessing HP ProtectTools Security | 4 |
| Achieving key security objectives | 6 |
| Protecting against targeted theft | 6 |
| Restricting access to sensitive data | 6 |
| Preventing unauthorized access from internal or external locations | 6 |
| Creating strong password policies | 7 |
| Additional security elements | 8 |
| Assigning security roles | 8 |
| Managing HP ProtectTools passwords | 8 |
| Creating a secure password | 10 |
| Backing up and restoring HP ProtectTools credentials | 10 |
| Backing up credentials and settings | 10 |

2 Credential Manager for HP ProtectTools

| | |
|--|----|
| Setup procedures | 11 |
| Logging on to Credential Manager | 11 |
| Using the Credential Manager Logon Wizard | 12 |
| Registering credentials | 12 |
| Registering fingerprints | 12 |
| Setting up the fingerprint reader | 13 |
| Using your registered fingerprint to log on to Windows | 13 |
| Registering a Smart Card or Token | 13 |
| Registering other credentials | 14 |
| General tasks | 15 |
| Creating a virtual token | 15 |
| Changing the Windows logon password | 15 |
| Changing a token PIN | 15 |
| Locking the computer (workstation) | 16 |
| Using Windows Logon | 16 |
| Logging on to Windows with Credential Manager | 16 |
| Using Single Sign On | 17 |
| Registering a new application | 17 |
| Using automatic registration | 17 |
| Using manual (drag and drop) registration | 18 |
| Managing applications and credentials | 18 |
| Modifying application properties | 18 |
| Removing an application from Single Sign On | 18 |

| | |
|--|----|
| Exporting an application | 18 |
| Importing an application | 19 |
| Modifying credentials | 19 |
| Using Application Protection | 20 |
| Restricting access to an application | 20 |
| Removing protection from an application | 20 |
| Changing restriction settings for a protected application | 21 |
| Advanced tasks (administrator only) | 22 |
| Specifying how users and administrators log on | 22 |
| Configuring custom authentication requirements | 23 |
| Configuring credential properties | 23 |
| Configuring Credential Manager settings | 24 |
| Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager | 24 |
| Example 2—Using the “Advanced Settings” page to require user verification before Single Sign On | 25 |

3 Drive Encryption for HP ProtectTools (select models only)

| | |
|--|----|
| Setup procedures | 26 |
| Opening Drive Encryption | 26 |
| General tasks | 27 |
| Activating Drive Encryption | 27 |
| Deactivating Drive Encryption | 27 |
| Logging in after Drive Encryption is activated | 27 |
| Advanced tasks | 28 |
| Managing Drive Encryption (administrator task) | 28 |
| Activating a TPM-protected password (select models only) | 28 |
| Encrypting or decrypting individual drives | 28 |
| Backup and recovery (administrator task) | 28 |
| Creating backup keys | 28 |
| Registering for online recovery | 29 |
| Managing an existing online recovery account | 30 |
| Performing a recovery | 30 |

4 Privacy Manager for HP ProtectTools (select models only)

| | |
|---|----|
| Opening Privacy Manager | 33 |
| Setup procedures | 34 |
| Managing Privacy Manager Certificates | 34 |
| Requesting and installing a Privacy Manager Certificate | 34 |
| Requesting a Privacy Manager Certificate | 34 |
| Installing a Privacy Manager Certificate | 34 |
| Viewing Privacy Manager Certificate details | 35 |
| Renewing a Privacy Manager Certificate | 35 |
| Setting a default Privacy Manager Certificate | 35 |
| Deleting a Privacy Manager Certificate | 35 |
| Restoring a Privacy Manager Certificate | 36 |
| Revoking your Privacy Manager Certificate | 36 |
| Managing Trusted Contacts | 36 |
| Adding Trusted Contacts | 37 |
| Adding a Trusted Contact | 37 |

| | |
|---|----|
| Adding Trusted Contacts using your Microsoft Outlook address book | 38 |
| Viewing Trusted Contact details | 38 |
| Deleting a Trusted Contact | 38 |
| Checking revocation status for a Trusted Contact | 39 |
| General tasks | 40 |
| Using Privacy Manager in Microsoft Office | 40 |
| Using Privacy Manager in Microsoft Outlook | 43 |
| Using Privacy Manager in Windows Live Messenger | 44 |
| Advanced tasks | 48 |
| Migrating Privacy Manager Certificates and Trusted Contacts to a different computer | 48 |
| Exporting Privacy Manager Certificates and Trusted Contacts | 48 |
| Importing Privacy Manager Certificates and Trusted Contacts | 48 |

5 File Sanitizer for HP ProtectTools

| | |
|--|----|
| Setup procedures | 50 |
| Opening File Sanitizer | 50 |
| Setting a shred schedule | 50 |
| Setting a free space bleaching schedule | 51 |
| Selecting or creating a shred profile | 51 |
| Selecting a predefined shred profile | 51 |
| Customizing a shred profile | 51 |
| Customizing a simple delete profile | 52 |
| Setting a shred schedule | 53 |
| Setting a free space bleaching schedule | 53 |
| Selecting or creating a shred profile | 54 |
| Selecting a predefined shred profile | 54 |
| Customizing a shred profile | 54 |
| Customizing a simple delete profile | 55 |
| General tasks | 56 |
| Using a key sequence to initiate shredding | 56 |
| Using the File Sanitizer icon | 56 |
| Manually shredding one asset | 56 |
| Manually shredding all selected items | 57 |
| Manually activating free space bleaching | 57 |
| Aborting a shred or free space bleaching operation | 57 |
| Viewing the log files | 58 |

6 BIOS Configuration for HP ProtectTools

| | |
|--|----|
| General tasks | 60 |
| Accessing BIOS Configuration | 60 |
| Viewing or changing settings | 61 |
| Viewing system information | 61 |
| Advanced tasks | 62 |
| Setting security options | 62 |
| Setting system configuration options | 63 |

7 Embedded Security for HP ProtectTools (select models only)

| | |
|--|----|
| Setup procedures | 69 |
| Enabling the embedded security chip | 69 |
| Initializing the embedded security chip | 70 |
| Setting up the basic user account | 70 |
| General tasks | 71 |
| Using the Personal Secure Drive | 71 |
| Encrypting files and folders | 71 |
| Sending and receiving encrypted e-mail | 71 |
| Changing the Basic User Key password | 72 |
| Advanced tasks | 72 |
| Backing up and restoring | 72 |
| Creating a backup file | 72 |
| Restoring certification data from the backup file | 72 |
| Changing the owner password | 73 |
| Resetting a user password | 73 |
| Enabling and disabling Embedded Security | 73 |
| Permanently disabling Embedded Security | 73 |
| Enabling Embedded Security after permanent disable | 73 |
| Migrating keys with the Migration Wizard | 74 |

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

| | |
|--|----|
| Starting background service | 75 |
| Simple configuration | 76 |
| Device class configuration (advanced) | 77 |
| Adding a user or a group | 77 |
| Removing a user or a group | 77 |
| Denying access to a user or group | 77 |
| Allowing access to a device class for one user of a group | 77 |
| Allowing access to a specific device for one user of a group | 78 |

9 Troubleshooting

| | |
|--|----|
| Credential Manager for HP ProtectTools | 79 |
| Embedded Security for HP ProtectTools (select models only) | 82 |
| Device Access Manager for HP ProtectTools | 88 |
| Miscellaneous | 89 |

| | |
|-----------------------|-----------|
| Glossary | 92 |
|-----------------------|-----------|

| | |
|--------------------|-----------|
| Index | 96 |
|--------------------|-----------|


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. Enhanced security functionality is provided by the following software modules:

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools (select models only)
- Privacy Manager for HP ProtectTools (select models only)
- File Sanitizer for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools (select models only)
- Device Access Manager for HP ProtectTools (select models only)

The software modules available for your computer may vary depending on your model. For example, Embedded Security for HP ProtectTools is available only for computers on which the Trusted Platform Module (TPM) embedded security chip is installed.

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

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

HP ProtectTools features

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

| Module | Key features |
|---|---|
| Credential Manager for HP ProtectTools | <ul style="list-style-type: none">• Credential Manager acts as a personal password vault, streamlining the logon process with the Single Sign On feature, which automatically remembers and applies user credentials.• Single Sign On also offers additional protection by requiring combinations of different security technologies, such as a Java™ Card and biometrics, for user authentication.• Password storage is protected through software encryption and can be enhanced through the use of a TPM embedded security chip and/or security device authentication, such as Java Cards or biometrics. |
| Drive Encryption for HP ProtectTools (select models only) | <ul style="list-style-type: none">• Drive Encryption provides complete, full-volume hard drive encryption.• Drive Encryption forces pre-boot authentication in order to decrypt and access the data. |
| Privacy Manager for HP ProtectTools (select models only) | <ul style="list-style-type: none">• Privacy Manager utilizes advanced logon techniques to verify the source, integrity, and security of communication when using e-mail, Microsoft® Office documents, or instant messaging (IM). |
| File Sanitizer for HP ProtectTools | <ul style="list-style-type: none">• 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. |
| BIOS Configuration for HP ProtectTools | <ul style="list-style-type: none">• BIOS Configuration provides access to power-on user and administrator password management.• BIOS Configuration provides an alternative to the pre-boot BIOS configuration utility known as Computer Setup.• BIOS Configuration enablement of automatic DriveLock support, which is enhanced with the embedded security chip, helps protect a hard drive from unauthorized access, even if it is removed from a system, without requiring the user to remember any additional passwords beyond the embedded security chip user password. |

| Module | Key features |
|--|---|
| Embedded Security for HP ProtectTools (select models only) | <ul style="list-style-type: none"> • Embedded Security uses a Trusted Platform Module (TPM) embedded security chip to help protect against unauthorized access to sensitive user data or credentials stored locally on a PC. • Embedded Security allows creation of a personal secure drive (PSD), which is useful in protecting user file and folder information. • Embedded Security supports third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations. |
| Device Access Manager for HP ProtectTools (select models only) | <ul style="list-style-type: none"> • Device Access Manager allows IT managers to control access to devices based on user profiles. • Device Access Manager prevents unauthorized users from removing data using external storage media and from introducing viruses into the system from external media. • The administrator can disable access to writeable devices for specific individuals or groups of users. |


Accessing HP ProtectTools Security

To access HP ProtectTools Security Manager from Windows® Control Panel:

1. In Windows Vista®, click **Start**, and then click **HP ProtectTools Security Manager for Administrators**.

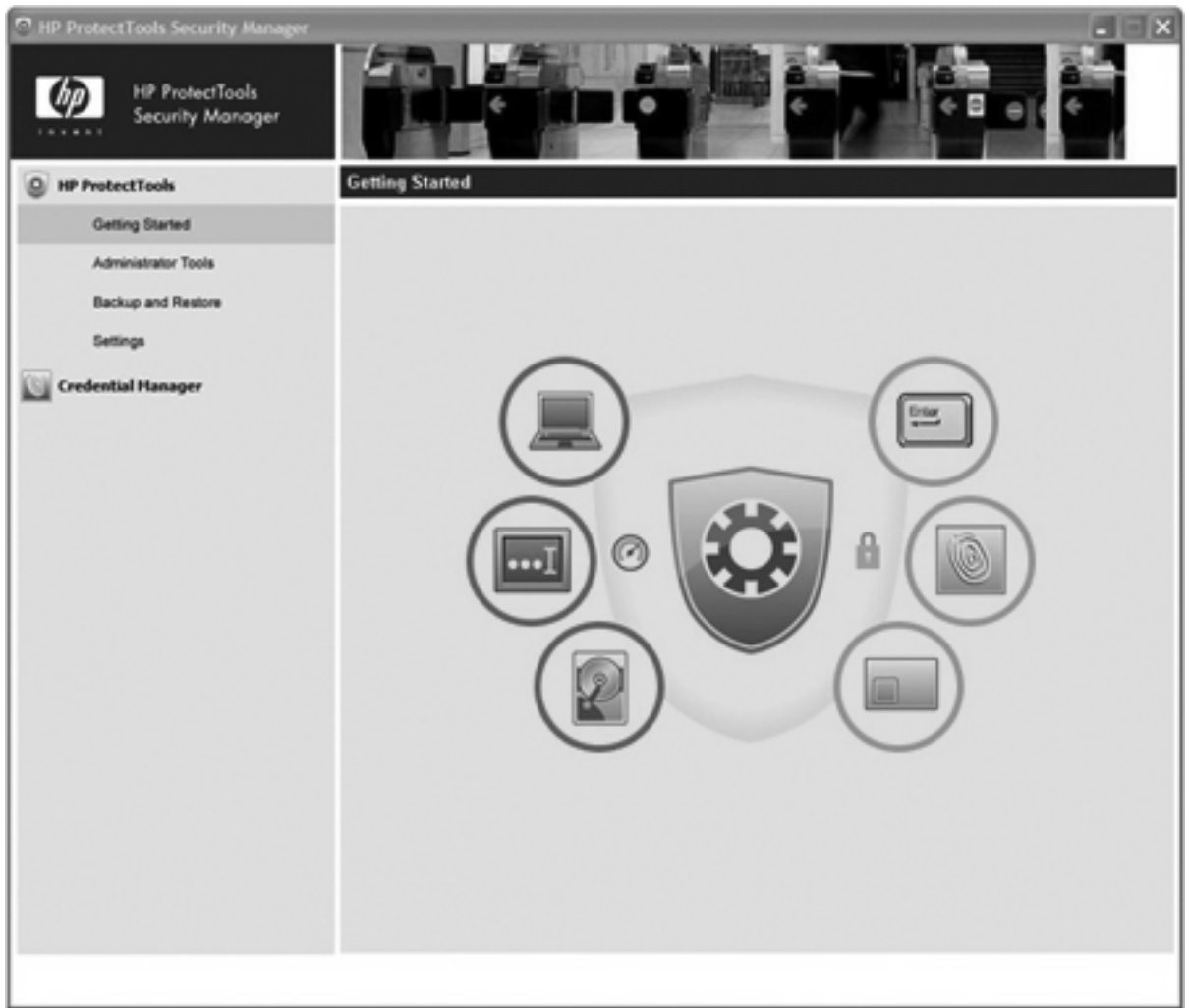
– or –

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


 **NOTE:** If you are not an HP ProtectTools administrator, you can run HP ProtectTools in nonadministrator mode to view information, but you cannot make changes.


2. In the left pane, click **HP ProtectTools**, and then click **Getting Started**.
3. Click the **Security Manager Setup** button, located directly below the HP ProtectTools shield icon, to launch the Security Manager Wizard.

The following page is displayed:



- The wizard guides Windows operating system administrators through the configuration of levels of security and of the security logon methods that are used in a pre-boot environment, in Credential Manager, and in Drive Encryption.
- Users also use the setup wizard to configure their security logon methods.

 **NOTE:** To access each HP ProtectTools module to set up more powerful features, click the module icon.

 **NOTE:** After you have configured the Credential Manager module, you can also open HP ProtectTools by logging on to Credential Manager directly from the Windows logon screen. For more information, refer to [“Logging on to Windows with Credential Manager on page 16.”](#)

Achieving key security objectives

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

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

Protecting against targeted theft

An example of this type of incident would be the targeted theft of a computer 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:
 - Credential Manager
 - Embedded Security
 - Drive Encryption
- DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system.
- The Personal Secure Drive feature, provided by the Embedded Security for HP ProtectTools module, encrypts sensitive data to help ensure it cannot be accessed without authentication. See the following procedures:
 - Embedded Security “[Setup procedures on page 69](#)”
 - “[Using the Personal Secure Drive on page 71](#)”

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 features help restrict access to data:

- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be printed or copied from the hard drive onto removable media. See “[Device class configuration \(advanced\) on page 77](#).”
- DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system.

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:
 - Credential Manager
 - Embedded Security
 - Drive Encryption
- Embedded Security for HP ProtectTools helps protect sensitive user data or credentials stored locally on a PC using the following procedures:
 - Embedded Security “[Setup procedures on page 69](#)”
 - “[Using the Personal Secure Drive on page 71](#)”
- Using the following procedures, Credential Manager for HP ProtectTools helps ensure that an unauthorized user cannot get passwords or access to password-protected applications:
 - Credential Manager “[Setup procedures on page 11](#)”
 - “[Using Single Sign On on page 17](#)”
- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be copied from the hard drive. See “[Simple configuration on page 76.](#)”
- The Personal Secure Drive feature encrypts sensitive data to help ensure it cannot be accessed without authentication using the following procedures:
 - Embedded Security “[Setup procedures on page 69](#)”
 - “[Using the Personal Secure Drive on page 71](#)”

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, Credential Manager for HP ProtectTools provides a protected repository for passwords and Single Sign On convenience using the following procedures:


- Credential Manager “[Setup procedures on page 11](#)”
- “[Using Single Sign On on page 17](#)”

For stronger security, Embedded Security for HP ProtectTools then protects that repository of user names and passwords. This allows users to maintain multiple strong passwords without having to write them down or try to remember them. See Embedded Security “[Setup procedures on page 69.](#)”

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.

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 |
|--|---|--|
| Credential Manager logon password | Credential Manager | This password offers 2 options: <ul style="list-style-type: none">• It can be used in a separate logon to access Credential Manager after logging on to Windows.• It can be used in place of the Windows logon process, allowing access to Windows and Credential Manager simultaneously. |
| Credential Manager recovery file password | Credential Manager, by IT administrator | Protects access to the Credential Manager recovery file. |
| Basic User Key password NOTE: Also known as: Embedded Security password | Embedded Security | Used to access Embedded Security features, such as secure e-mail, file, and folder encryption. When used for power-on authentication, also protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation. |

| HP ProtectTools password | Set in this HP ProtectTools module | Function |
|--|---|---|
| Emergency Recovery Token password NOTE: Also known as: Emergency Recovery Token Key password | Embedded Security, by IT administrator | Protects access to the Emergency Recovery Token, which is a backup file for the embedded security chip. |
| Owner password | Embedded Security, by IT administrator | Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security. |
| 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 Computer Setup utility and to the computer contents. Authenticates users of Drive Encryption, if the Java Card token is selected. |
| Computer Setup password NOTE: Also known as BIOS administrator, F10 Setup, or Security Setup password | BIOS Configuration, by IT administrator | Protects access to the Computer Setup utility. |
| Power-on password | BIOS Configuration | Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation. |
| Windows Logon password | Windows Control Panel | Can be used for manual logon 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

To back up and restore credentials from all supported HP ProtectTools modules, reference the following:

Backing up credentials and settings

You can back up credentials in the following ways:

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

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



NOTE: You must be connected to the Internet and have a valid e-mail address to register and to recover your password through this service.

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

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools protects against unauthorized access to your computer using the following security features:


- Alternatives to passwords when logging on to Windows, such as using a Java Card or biometric reader to log on to Windows. For additional information, refer to [“Registering credentials on page 12.”](#)
- Single Sign On feature that automatically remembers credentials for Web sites, applications, and protected network resources.
- Support for optional security devices, such as Java Cards and biometric readers.
- Support for additional security settings, such as requiring authentication using an optional security device to unlock the computer.

Setup procedures

Logging on to Credential Manager

Depending on the configuration, you can log on to Credential Manager in any of the following ways:

- HP ProtectTools Security Manager icon in the notification area
- In Windows Vista®, click **Start**, and then click **HP ProtectTools Security Manager for Administrators**.
- In Windows XP, click **Start**, and then click **HP ProtectTools Security Manager**.

 **NOTE:** In Windows Vista, you must launch the HP ProtectTools Security Manager for Administrators to make changes.

After logging on to Credential Manager, you can register additional credentials, such as a fingerprint or a Java Card. For additional information, refer to [“Registering credentials on page 12.”](#)

At the next logon, you can select the logon policy and use any combination of the registered credentials.

Using the Credential Manager Logon Wizard

To log on to Credential Manager using the Credential Manager Logon Wizard, use the following steps:

1. Open the Credential Manager Logon Wizard in any of the following ways:
 - From the Windows logon screen
 - From the notification area, by double-clicking the **HP ProtectTools Security Manager** icon
 - From the “Credential Manager” page of HP ProtectTools Security Manager, by clicking the **Log On** link in the upper-right corner of the window
2. Follow the on-screen instructions to log on to Credential Manager.

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 Credential Manager.

Registering fingerprints

A fingerprint reader allows you to log on to Windows using your fingerprint for authentication instead of using a Windows password.

Setting up the fingerprint reader

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**, and then click **Register Fingerprints**.
3. Follow the on-screen instructions to complete registering your fingerprints and setting up the fingerprint reader.
4. To set up the fingerprint reader for a different Windows user, log on to Windows as that user and then repeat the steps listed above.

Using your registered fingerprint to log on to Windows


1. Immediately after you have registered your fingerprints, restart Windows.
2. At the Windows Welcome screen, swipe any of your registered fingers to log on to Windows.

Registering a Smart Card or Token


A smart card is a plastic card about the size of a credit card with an embedded microchip that can be loaded with information. Smart cards provide protection of information and authentication for individual users. Logging on to a network with a smart card can provide a strong form of authentication when it uses cryptography-based identification and proof of possession when authenticating a user to a domain.

A USB token is simply a smart card in a different form factor. Rather than deploying the smart chip on a plastic credit platform, the smart chip is inserted into a plastic token, also known as a USB key. The major difference between a smart card and a token is in the access interface. A card requires a reader, while a token plugs directly into any USB port. There is no difference in the core functionality of storing and providing credentials.

A USB token is used for strong authentication. It provides enhanced security and ensures safe information access.

 **NOTE:** You must have a card reader configured for this procedure. If you do not have a reader installed, you can register a virtual token as described in [“Creating a virtual token on page 15.”](#)

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**, and then click **Register Smart Card or Token**.
3. On the **Device Type** dialog box, click the desired type of device, and then click **Next**.
4. If a smart card or USB token was selected as the device type, make sure that smart card is inserted or the token is connected to a USB port.

 **NOTE:** If the smart card is not inserted or the USB token is not connected, the Next button is disabled in Select Token dialog box.

5. On the Device Type dialog box, select **Next**.
The Token Properties dialog box is displayed.
6. Type the User PIN, select **Register smart card or token for authentication**, and then click **Finish**.


Registering other credentials

1. In HP ProtectTools Security Manager, click **Credential Manager**.
2. Click **My Identity**, and then click **Register Credentials**.
The Credential Manager Registration Wizard opens.
3. Follow the on-screen instructions.

General tasks

All users have access to the “My Identity” page in Credential Manager. From the “My Identity” page, you can perform the following tasks:

- Change the Windows logon password
- Change a token PIN
- Lock a workstation

 **NOTE:** This option is available only if the Credential Manager classic logon prompt is enabled. See [“Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager on page 24.”](#)

Creating a virtual token

A virtual token works very much like a Java Card or USB Token. 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.

To create a new virtual token:

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**, and then click **Register Smart Card or Token**.
3. On the **Device Type** dialog box, click **Virtual Token**, and then click **Next**.
4. Specify the token name and location, and click **Next**.

A new virtual token can be stored either in a file or in the Windows registry database.


5. On the Token Properties dialog box, specify the Master PIN and User PIN for the newly created virtual token, select **Register smart card or token for authentication**, and then click **Finish**.

Changing the Windows logon password

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**, and then click **Change Windows Password**.
3. Type your old password in the **Old password** box.
4. Type your new password in the **New password** and **Confirm password** boxes.
5. Click **Finish**.


Changing a token PIN

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**, and then click **Change Token PIN**.
3. On the Device Type dialog box, click the desired type of device, and then click **Next**.
4. Select the token for which you want to change the PIN, and then click **Next**.
5. Follow the on-screen instructions to complete the PIN change.

 **NOTE:** If you enter the incorrect PIN for the token several times in sequence, the token gets locked out. You will be unable to use this token until you unlock it.

Locking the computer (workstation)

This feature is available if you log on to Windows using Credential Manager. To secure your computer when you are away from your desk, use the Lock Workstation feature. This prevents unauthorized users from gaining access to your computer. Only you and members of the administrators group on your computer can unlock it.

 **NOTE:** This option is available only if the Credential Manager classic logon prompt is enabled. See [“Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager on page 24.”](#)

For added security, you can configure the Lock Workstation feature to require a Java Card, biometric reader, or token to unlock the computer. For more information, see [“Configuring Credential Manager settings on page 24.”](#)

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **My Identity**.
3. Click **Lock Workstation** to lock your computer immediately.

You must use a Windows password or the Credential Manager Logon Wizard to unlock the computer.

Using Windows Logon

You can use Credential Manager to log on to Windows, either at a local computer or on a network domain. When you log on to Credential Manager for the first time, the system automatically adds your local Windows user account as the account for the Windows Logon service.

Logging on to Windows with Credential Manager

You can use Credential Manager to log on to a Windows network or local account.

1. If you have registered your fingerprint to log on to Windows, swipe your finger to log on.
2. In Windows XP, if you have not registered your fingerprint to log on to Windows, click the keyboard icon in the upper-left corner of the screen next to the fingerprint icon. The Credential Manager Logon Wizard opens.


In Windows Vista, if you have not registered your fingerprint to log on to Windows, click the **Credential Manager** icon at the logon screen. The Credential Manager Logon Wizard opens.

3. Click the **User name** arrow, and then click your name.
4. Type your password in the **Password** box, and then click **Next**.

5. Select **More**, and then click **Wizard Options**.
 - a. If you want this to be the default user name the next time that you log on to the computer, select the **Use last user name on next logon** check box.
 - b. If you want this logon policy to be the default method, select the **Use last policy on next logon** check box.
6. Follow the on-screen instructions. If your authentication information is correct, you will be logged on to your Windows account and to Credential Manager.

Using Single Sign On

Credential Manager has a Single Sign On feature that stores user names and passwords for multiple Internet and Windows programs, and automatically enters logon credentials when you access a registered program.

 **NOTE:** Security and privacy are important features of Single Sign On. All credentials are encrypted and are available only after successful logon to Credential Manager.

NOTE: You can also configure Single Sign On to validate your authentication credentials with a Java Card, a fingerprint reader, or a token before logging on to a secure site or program. This is particularly useful when logging on to programs or Web sites that contain personal information, such as bank account numbers. For more information, refer to "[Configuring Credential Manager settings on page 24.](#)"

Registering a new application

Credential Manager prompts you to register any application that you launch while you are logged on to Credential Manager. You can also register an application manually.

Using automatic registration

1. Open an application that requires you to log on.
2. Click the Credential Manager SSO icon in the program or Web site password dialog box.
3. Type your password for the program or Web site, and then click **OK**. The **Credential Manager Single Sign On** dialog box opens.
4. Click **More** and select from the following options:
 - Do not use SSO for this site or application.
 - Prompt to select account for this application.
 - Fill in credentials but do not submit.
 - Authenticate user before submitting credentials.
 - Show SSO shortcut for this application.
5. Click **Yes** to complete the registration.

Using manual (drag and drop) registration

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications** in the left pane.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. To modify or remove a previously registered web site or application, select the desired record in the list.
4. Follow the on-screen instructions.

Managing applications and credentials

Modifying application properties

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications** from the left pane.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. Click the application entry you want to modify, and then click **Properties**.
4. Click the **General** tab to modify the application name and description. Change the settings by selecting or clearing the check boxes next to the appropriate settings.
5. Click the **Script** tab to view and edit the SSO application script.
6. Click **OK**.

Removing an application from Single Sign On

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications** in the left pane.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. Click the application entry you want to remove, and then click **Remove**.
4. Click **Yes** in the confirmation dialog box.
5. Click **OK**.

Exporting an application

You can export applications to create a backup copy of the Single Sign On application script. This file can then be used to recover the Single Sign On data. This acts as a supplement to the identity backup file, which contains only the credential information.

To export an application:


1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications** in the left pane.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. Click the application entry you want to export, and then click **More**.
4. Follow the on-screen instructions to complete the export.
5. Click **OK**.

Importing an application

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications** in the left pane.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. Click the application entry you want to import, and then click **More**.
4. Follow the on-screen instructions to complete the import.
5. Click **OK**.

Modifying credentials

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Services and Applications**.
2. Click **Manage Services and Applications**.
The Credential Manager Single Sign On dialog box is displayed.
3. Click the application entry you want to modify, and then click **More**.
4. Select any of the following options:
 - Applications
 - Add New
 - Remove
 - Properties
 - Import Script
 - Export Script
 - Credentials
 - Create New
 - View Password

 **NOTE:** You must authenticate your identity before viewing the password.

5. Follow the on-screen instructions.
6. Click **OK**.


Using Application Protection

This feature allows you to configure access to applications. You can restrict access based on the following criteria:

- Category of user
- Time of use
- User inactivity

Restricting access to an application

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane, and then click **Services and Applications**.
2. Click **Application Protection**.
3. Select a category of user whose access you want to manage.


 **NOTE:** If the category is not Everyone, you may need to select **Override default settings** to override the settings for the Everyone category.

4. Click **Add**.
The Add a Program Wizard opens.
5. Follow the on-screen instructions.

Removing protection from an application

To remove restrictions from an application:


1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Services and Applications**.
3. Click **Application Protection**.
4. Select a category of user whose access you want to manage.

 **NOTE:** If the category is not Everyone, you may need to click **Override default settings** to override the settings for the Everyone category.

5. Click the application entry you want to remove, and then click **Remove**.
6. Click **OK**.

Changing restriction settings for a protected application

1. Click **Application Protection**.
2. Select a category of user whose access you want to manage.

 **NOTE:** If the category is not Everyone, you may need to click **Override default settings** to override the settings for the Everyone category.

3. Click the application you want to change, and then click **Properties**. The **Properties** dialog box for that application opens.
4. Click the **General** tab. Select one of the following settings:
 - Disabled (Cannot be used)
 - Enabled (Can be used without restrictions)
 - Restricted (Usage depends on settings)
5. When you select Restricted, the following settings are available:
 - a. If you want to restrict usage based on time, day, or date, click the **Schedule** tab and configure the settings.
 - b. If you want to restrict usage based on inactivity, click the **Advanced** tab and select the period of inactivity.
6. Click **OK** to close the application **Properties** dialog box.
7. Click **OK**.

Advanced tasks (administrator only)

The “Authentication and Credentials” page and the “Advanced Settings” page of Credential Manager are available only to those users with administrator rights. From these pages, you can perform the following tasks:

- Specifying how users and administrators log on
- Configuring custom authentication requirements
- Configuring credential properties
- Configuring Credential Manager settings

Specifying how users and administrators log on

On the “Authentication and Credentials” page, you can specify which type or combination of credentials are required of either users or administrators.

To specify how users or administrators log on:

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Multifactor Authentication**
3. In the right pane, click the **Authentication** tab.
4. Click the category (**Users** or **Administrators**) from the category list.
5. Click the type or combination of authentication methods from the list.
6. Click **Apply**, and then click **OK**.

Configuring custom authentication requirements

If the set of authentication credentials you want is not listed on the Authentication tab of the “Authentication and Credentials” page, you can create custom requirements.

To configure custom requirements:

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Multifactor Authentication**.
3. In the right pane, click the **Authentication** tab.
4. Click the category (**Users** or **Administrators**) from the category list.
5. Click **Custom** in the list of authentication methods.
6. Click **Configure**.
7. Select the authentication methods you want to use.
8. Choose the combination of methods by clicking one of the following selections:
 - Use AND to combine the authentication methods
(Users will have to authenticate with all of the methods you checked each time they log on.)
 - Use OR to require one of two or more authentication methods
(Users will be able to choose any of the selected methods each time they log on.)
9. Click **OK**.
10. Click **Apply**, and then click **OK**.

Configuring credential properties

On the Credentials tab of the “Authentication and Credentials” page, you can view the list of available authentication methods, and modify the settings.

To configure the credentials:

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Multifactor Authentication**.
3. Click the **Credentials** tab.
4. Click the credential type you want to modify. You can modify the credential using one of the following choices:
 - To register the credential, click **Register**, and then follow the on-screen instructions.
 - To delete the credential, click **Clear**, and then click **Yes** in the confirmation dialog box.
 - To modify the credential properties, click **Properties**, and then follow the on-screen instructions.
5. Click **Apply**, and then click **OK**.

Configuring Credential Manager settings

From the “Advanced Settings” page, you can access and modify various settings using the following tabs:


- **General**—Allows you to modify the settings for basic configuration.
- **Single Sign On**—Allows you to modify the settings for how Single Sign On works for the current user, such as how it handles detection of logon screens, automatic logon to registered logon dialogs, and password display.
- **Services and Applications**—Allows you to view the available services and modify the settings for those services.
- **Security**—Allows you to select the fingerprint reader software and adjust the security level of the fingerprint reader.
- **Smart Cards and Tokens**—Allows you to view and modify properties for all available Java Cards and tokens.

To modify Credential Manager settings:

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Settings**.
3. Click the appropriate tab for the settings you want to modify.
4. Follow the on-screen instructions to modify the settings.
5. Click **Apply**, and then click **OK**.

Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager

1. In HP ProtectTools Security Manager, click **Credential Manager** in the left pane.
2. Click **Settings**.
3. Click the **General** tab.
4. Under **Select the way users log on to Windows (requires restart)**, select the **Use Credential Manager with classic logon prompt** check box.
5. Click **Apply**, and then click **OK**.
6. Restart the computer.

 **NOTE:** Selecting the **Use Credential Manager with classic logon prompt** check box allows you to lock your computer. See “[Locking the computer \(workstation\) on page 16.](#)”

Example 2—Using the “Advanced Settings” page to require user verification before Single Sign On

1. In HP ProtectTools Security Manager, click **Credential Manager**, and then click **Settings**.
2. Click the **Single Sign On** tab.
3. Under **When registered logon dialog or Web page is visited**, select the **Authenticate user before submitting credentials** check box.
4. Click **Apply**, and then click **OK**.
5. Restart the computer.

3 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.

Setup procedures

Opening Drive Encryption

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

General tasks

Activating Drive Encryption


Use the HP ProtectTools Security Manager setup wizard to activate Drive Encryption.

Deactivating Drive Encryption


Use the HP ProtectTools Security Manager setup wizard to deactivate Drive Encryption.

Logging in after Drive Encryption is activated

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

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

1. Select your user name, and then type your Windows password or 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 logon screen, you will also be prompted to select your Windows user name and type your password at the Windows logon screen.


Advanced tasks

Managing Drive Encryption (administrator task)

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

Activating a TPM-protected password (select models only)


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

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

1. Use the Embedded Security tool in HP ProtectTools to activate the TPM.
2. Open Drive Encryption, and click **Encryption Management**.
3. Select the **TPM-protected password** check box.

Encrypting or decrypting individual drives


1. Open Drive Encryption, and 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 Windows administrators to back up and recover encryption keys.

Creating backup keys

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


1. Open Drive Encryption, and then click **Recovery**.
2. Click **Backup Keys**.
3. On the “Select Backup Disk” page, click the name of the device where you want to back up your encryption key, and then click **Next**.
4. Read the information on the next page that is displayed, and then click **Next**.

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


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

Registering for online recovery


The Online Drive Encryption Key Recovery Service stores a backup copy of your encryption key, which will enable you to access your computer if you forget your password and do not have access to your local backup.

 **NOTE:** You must be connected to the Internet and have a valid e-mail address to register and to recover your password through this service.

1. Open Drive Encryption, and then click **Recovery**.
2. Click **Register**.
3. Click one of the following options:
 - I want to create a new recovery account for this PC. If you choose this option, type your e-mail address and other information, and then click **Next**.
 - I want to add this PC to my existing web recovery account.
4. Create and confirm a password, select security questions and type the answers, and then click **Next**.

 **NOTE:** An account activation code will be sent to the e-mail address you provided.

5. Enter the activation code, and then click **Next**.
6. Enter the computer serial number, and then click **Next**.

 **NOTE:** To locate the computer serial number, click **Start**, and then click **Help and Support**.

7. If you do not have a subscription coupon, click the **Click here to purchase coupons** link.
Clicking the link directs you to the SafeBoot Recovery Service Web site. Do not exit the wizard.
8. Click **Purchase Coupon Codes**.
9. Select your country, the type of computer, and then click **Start**.
10. Click **Buy** next to the 1-year subscription option or the 3-year subscription option.
11. Click **Checkout**.
12. Read the terms and conditions, and then click **Accept**.
13. Enter your billing information, and then click **Continue**.
14. Enter your credit card information, and then click **Make Payment**.
15. Write down your coupon code, and then return to the “Account Activation” page in the wizard.
16. Enter your account activation code, and then click **Next**.
17. When the confirmation dialog box opens, click **OK**.

Managing an existing online recovery account

After you create an online recovery account, you can access the SafeBoot Recovery Service Web site to recover access to your computer if you lose your password, modify your personal settings, reset the password you use for the online recovery account, and view or renew your account.

1. Open Drive Encryption, and then click **Recovery**.
2. Click **Manage**.
3. When the “SafeBoot Recovery Service” Web page opens, click **Recovery Service Account** or **Recovery Process**.
4. On the recovery service logon page, enter your e-mail address, password, and the numbers and letters you see in the box.
5. Click **Logon**.
6. Click **Profile** to update your personal information, such as your telephone or billing address.

– or –

Click **Reset Password** to reset or change your password.

– or –

Click **My Subscriptions** to view your current subscription information.



NOTE: The “My Subscriptions” page also allows you to renew your subscription. Click **Renew Subscription** to perform this action.

Performing a recovery

Performing a local recovery


1. Turn on the computer.
2. Insert the removable storage device that stores your backup key.
3. When the Drive Encryption for HP ProtectTools logon dialog box opens, click **Cancel**.
4. Click **Options** in the lower-left corner of the screen, and then click **Recovery**.
5. Click **Local recovery**, and then click **Next**.
6. Select the file that contains your backup key or click **Browse** to search for it, and then click **Next**.
7. When the confirmation dialog box opens, click **OK**.

The recovery process is completed and your computer starts.




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


Performing an online recovery

 **NOTE:** This section describes how to perform an online recovery when you have access to a different computer with an Internet connection. If you do not have access to such a computer, contact HP technical support.

1. Turn on the computer.
2. When the Drive Encryption for HP ProtectTools logon dialog box opens, click **Cancel**.
3. Click **Options** in the lower-left corner of the screen, and then click **Recovery**.
4. Click **Web recovery**, and then click **Next**.
5. Record the client code, and then click **Next**.
6. On a different computer with an Internet connection, access the SafeBoot Recovery Service Web site at <http://www.safeboot-hp.com>.
7. Click **Recovery Process**.
8. On the recovery service logon page, enter your e-mail address, password, and the numbers and letters you see in the box.
9. Click **Logon**.
10. Click **Recovery Process**.
11. Enter the client code you recorded from the computer you are recovering, and enter the numbers and letters you see in the box.
12. Click **Submit**.
13. Record each line of the response key.
14. On the computer you are recovering, enter line 1 of the response key that you recorded from the SafeBoot Recovery Service Web site, and then click **Enter**.
15. Enter line 2 of the response key, and then click **Enter**.
16. Enter line 3 of the response key, and then click **Enter**.
17. Enter line 4 of the response key, and then click **Enter**.

 **NOTE:** Line 4 of the response key is shorter than the first 3 lines.

18. Click **Finish**.

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

4 Privacy Manager for HP ProtectTools (select models only)

Privacy Manager for HP ProtectTools enables you to use advanced security logon (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 logon methods:

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

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

Opening Privacy Manager

To open Privacy Manager:

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

– or –

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

– or –

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

– or –

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

Setup procedures

Managing Privacy Manager Certificates

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

Requesting and installing a Privacy Manager Certificate

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

Requesting a Privacy Manager Certificate

1. Open Privacy Manager, and click **Certificate Manager**.
2. Click Request a **Privacy Manager Certificate**.
3. On the “Welcome” page, read the text, and then click **Next**.
4. On the “License Agreement” page, read the license agreement.
5. Be sure that the check box next to **Check here to accept the terms of this license agreement** is selected, and then click **Next**.
6. On the “Your Certificate Details” page, enter the required information, and then click **Next**.
7. On the “Certificate Request Accepted” page, click **Finish**.

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

Installing a Privacy Manager Certificate

1. When you receive the e-mail with your Privacy Manager Certificate attached, open the e-mail and click the **Setup** button, in the lower-right corner of the message.
2. Authenticate using your chosen security logon method.
3. On the “Certificate Installed” page, click **Next**.
4. On the “Certificate Backup” page, enter a location and name for the backup file, or click **Browse** to search for a location.

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

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

6. Authenticate using your chosen security logon method.
7. If you choose to begin the Trusted Contact invitation process, follow the on-screen instructions.
– or –

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


Viewing Privacy Manager Certificate details

1. Open Privacy Manager, and click **Certificate Manager**.
2. Click a Privacy Manager Certificate.
3. Click **Certificate details**.
4. When you have finished viewing the details, click **OK**.

Renewing a Privacy Manager Certificate

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

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


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

Setting a default Privacy Manager Certificate

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

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

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

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

Deleting a Privacy Manager Certificate

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


To delete a Privacy Manager Certificate:

1. Open Privacy Manager, and click **Certificate Manager**.
2. Click the Privacy Manager Certificate you want to delete, and then click **Advanced**.
3. Click **Delete**.
4. When the confirmation dialog box opens, click **Yes**.
5. Click **Close**, and then click **Apply**.

Restoring a Privacy Manager Certificate


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

1. Open Privacy Manager, and click **Migration**.
2. Click **Import migration file**.
3. Click On the “Migration File” page, click **Browse** to search for the .dppsm file that you created when you installed or exported the Privacy Manager Certificate, and then click **Next**.
4. On the “Migration File Import” page, click **Finish**.
5. Click **Close**, and then click **Apply**.

 **NOTE:** Refer to [Installing a Privacy Manager Certificate or Exporting Privacy Manager Certificates and Trusted Contacts](#) for more information.

Revoking your Privacy Manager Certificate

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

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

1. Open Privacy Manager, and click **Certificate Manager**.
2. Click **Advanced**.
3. Click the Privacy Manager Certificate you want to revoke, and then click **Revoke**.
4. When the confirmation dialog box opens, click **Yes**.
5. Authenticate using your chosen security logon method.
6. Follow the on-screen instructions.


Managing Trusted Contacts

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

Adding Trusted Contacts

1. You send an e-mail invitation to a Trusted Contact recipient.
2. The Trusted Contact recipient responds to the e-mail.
3. You receive the e-mail response from the Trusted Contact recipient, and click **Accept**.

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

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

7. Authenticate using your chosen security logon method.
8. When you receive an e-mail response from a recipient accepting the invitation to become a Trusted Contact, click **Accept** in the lower-right corner of the e-mail.

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

9. Click **OK**.

Adding Trusted Contacts using your Microsoft Outlook address book

1. 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.

6. Authenticate using your chosen security logon 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 Manager**.
2. Click a Trusted Contact.
3. Click **Contact details**.
4. When you have finished viewing the details, click **OK**.

Deleting a Trusted Contact

1. Open Privacy Manager, and click **Trusted Contacts Manager**.
2. Click the Trusted Contact you want to delete.
3. Click **Delete contact**.
4. When the confirmation dialog box opens, click **Yes**.

Checking revocation status for a Trusted Contact

1. Open Privacy Manager, and click **Trusted Contacts Manager**.
2. Click a Trusted Contact.
3. Click the **Advanced** button.
The Advanced Trusted Contact Management dialog box opens.
4. Click **Check Revocation**.
5. Click **Close**.

General tasks

Using Privacy Manager in Microsoft Office

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

Configuring Privacy Manager in a Microsoft Office document

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

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

1. Click the **Office** button in the upper-left corner of the screen.
2. Click **Prepare**, and then click **Mark as Final**.
3. When the confirmation dialog box opens, click **Yes**, and continue working.
4. When you have completed your editing, sign the document again.

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

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

1. In Microsoft Word or Microsoft Excel create and save a document.
2. Click the **Home** menu.
3. Click the down arrow next to **Sign and Encrypt**, and then click **Add Signature Line Before Signing**.



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

4. Click the down arrow next to **Sign and Encrypt**, and then click **Sign Document**.
5. Authenticate using your chosen security logon method.

Adding suggested signers to a Microsoft Word or Microsoft Excel document


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

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


1. In Microsoft Word or Microsoft Excel, create and save a document.
2. Click the **Insert** menu.
3. In the **Text** group on the toolbar, click the arrow next to **Signature Line**, and then click **Privacy Manager Signature Provider**.

The Signature Setup dialog box opens.

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

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

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

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

8. Click **OK**.

Adding a suggested signer's signature line

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

To sign the document:

1. Double-click the appropriate signature line.
2. Authenticate using your chosen security logon method.

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

Encrypting a Microsoft Office document

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


To encrypt a Microsoft Office document:

1. In Microsoft Word, Microsoft Excel, or Microsoft PowerPoint, create and save a document.
2. Click the **Home** menu.

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

The Select Trusted Contacts dialog box opens.

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

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

5. Click **OK**.

6. Authenticate using your chosen security logon method.

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

Removing the encryption from a Microsoft Office document

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

To remove encryption from a Microsoft Office document:

1. Open an encrypted Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document.
2. Authenticate using your chosen security logon method.
3. Click the **Home** menu.
4. Click the down arrow next to **Sign and Encrypt**, and then click **Remove Encryption**.

Sending an encrypted Microsoft Office document


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

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

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

1. In Microsoft Outlook, click **New** or **Reply**.
2. Type your e-mail message.
3. Attach the Microsoft Office document.
4. Refer to Sealing and sending an e-mail message for further instructions.

Viewing a signed Microsoft Office document

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

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

Viewing an encrypted Microsoft Office document

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

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

Using Privacy Manager in Microsoft Outlook

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

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 **Privacy**, and then click **Settings**.

– or –

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

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

Signing and sending an e-mail message

- ▲ In Microsoft Outlook, click **New** or **Reply**.
- ▲ Type your e-mail message.
- ▲ Click the down arrow next to **Send Securely**, and then click **Sign and Send**.
- ▲ Authenticate using your chosen security logon method.

Sealing and sending an e-mail message

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

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

1. In Microsoft Outlook, click **New** or **Reply**.
2. Type your e-mail message.
3. Click the down arrow next to **Send Securely**, and then click **Seal for Trusted Contacts and Send**.
4. Authenticate using your chosen security logon method.

Viewing a sealed e-mail message

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

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


Using Privacy Manager in Windows Live Messenger

Adding Privacy Manager Chat activity

To add the Privacy Manager Chat feature to Windows Live Messenger, follow these steps:

1. Log in to Windows Live Home.
2. Click the **Windows Live** icon, and then click **Windows Live Services**.
3. Click **Gallery**, and then click **Messenger**.
4. Click **Activities**, and then click **Safety and Security**.
5. Click **Privacy Manager Chat**, and then follow the on-screen instructions.

Starting Privacy Manager Chat

 **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 5.

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

– or –

- a. Double-click an online contact in Live Messenger, and then click the **Conversation** menu.
- b. Click **Action**, and then click **Start Privacy Manager Chat**.

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 Chat 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 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 logon 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 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.

Starting the Chat History viewer

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. Click **Privacy Manager: Sign and Chat**, and then click **Chat History Viewer**.

– or –

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

– or –

- ▲ On the “Chat Configuration” page, click **Start Live Messenger History Viewer**.

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.

1. In the Chat History Viewer, right-click any session, and then select **Reveal All Sessions**.
2. Authenticate using your chosen security logon 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.

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

The Contact Screen Names are 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

- ▲ In the Chat History View, 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.

1. In the Chat History Viewer, right-click any revealed session, and select **View**.
2. If prompted, authenticate using your chosen security logon 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.

1. In the Chat 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 Chat 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 Chat History Viewer.

Displaying sessions for a specific account

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

Displaying sessions for a range of dates

1. In the Chat History View, 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 Chat History View, 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 a different computer. To do this, export them as a password-protected file to a network location or any removable storage device, and then import the file to the new computer.

Exporting Privacy Manager Certificates and Trusted Contacts

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

1. Open Privacy Manager, and click **Migration**.
2. Click **Export migration file**.
3. On the “Select Data” page, select the data categories to be included in the migration file, and then click **Next**.
4. On the “Migration File” page, enter a file name or click **Browse** to search for a location, and then click **Next**.
5. Enter and confirm a password, and then click **Next**.



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

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


Importing Privacy Manager Certificates and Trusted Contacts

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

1. Open Privacy Manager, and click **Migration**.
2. Click **Import migration file**.
3. On the “Select Data” page, select the data categories to be included in the migration file, and then click **Next**.
4. On the “Migration File” page, enter a file name or click **Browse** to search for a location, and then click **Next**.
5. On the “Migration File Import” page, click **Finish**.

5 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 periodically bleach your hard drive.

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

About shredding

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


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

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

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

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

About free space bleaching

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

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

Setup procedures


Opening File Sanitizer

To open File Sanitizer:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. Click **File Sanitizer**.
– or –
 - Double-click the **File Sanitizer** icon.
– or –
 - Right-click the HP ProtectTools icon in the notification area, at the far right of the taskbar, click File Sanitizer, and then click Open File Sanitizer.


Setting a shred schedule

1. Open File Sanitizer, and click **Shred**.
2. Select a shred option:
 - **Windows startup** — Choose this option to shred all selected assets when Windows starts up.
 - **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.
 - **Scheduler** — Select the Activate Scheduler check box, enter your Windows password, and then enter a day and time to shred selected assets.
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 then 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 **Cancel**, 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 different times. If you choose the higher security shred cycles, shredding may take a significant length of time; however, the higher the number of shred cycles you specify, the more secure the computer is.


3. Select the assets you want to shred:
 - a. Under **Available shred options**, click an asset, and then click **Add**.
 - b. To add a custom asset, click **Add Custom Option**, enter a file name or folder name, and then click **OK**. Click the custom asset, and then click **Add**.

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

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

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

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


 **NOTE:** Only file extensions can be excluded from shredding. For example, if you add the .BMP file extension, all files with the .BMP extension will be excluded from shredding.


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:** It is highly recommended that you run free space bleaching regularly if you use the simple delete option.
-
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 shred the following**, click **Add** to select the specific assets that you want to exclude from shredding.


 **NOTE:** Only file extensions can be excluded from deleting. For example, if you add the .BMP file extension, all files with the .BMP extension will be excluded from deletion.

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**.


Setting a shred schedule

1. Open File Sanitizer, and click **Shred**.
2. Select a shred option:
 - **Windows startup** — Choose this option to shred all selected assets when Windows starts up.
 - **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.
 - **Scheduler** — Select the Activate Scheduler check box, enter your Windows password, and then enter a day and time to shred selected assets.
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

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 then 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 **Cancel**, 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 different times. If you choose the higher security shred cycles, shredding may take a significant length of time; however, the higher the number of shred cycles you specify, the more secure the computer is.


3. Select the assets you want to shred:
 - a. Under **Available shred options**, click an asset, and then click **Add**.
 - b. To add a custom asset, click Add Custom Option, enter a file name or folder name, and then click **OK**. Click the custom asset, and then click **Add**.

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

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

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

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


 **NOTE:** Only file extensions can be excluded from shredding. For example, if you add the .BMP file extension, all files with the .BMP extension will be excluded from shredding.

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


1. Open **File Sanitizer**, click **Settings**, click **Simple Delete Setting**, and then click **View Details**.
2. Select the assets you want to delete:
 - Under **Available delete options**, click an asset, and then click **Add**.
 - 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:** Only file extensions can be excluded from deleting. For example, if you add the .BMP file extension, all files with the .BMP extension will be excluded from deletion.

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

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, and then select the **CTRL**, **ALT**, or **SHIFT** box, or select all three.

For example, to initiate automatic shredding using the **s** key and **ctrl+shift**, enter **s** in the box, and then select the **CTRL** and **SHIFT** options.

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

To initiate shredding using a key sequence:

1. Hold down the **ctrl**, **alt**, or **shift** key (or whichever combination you specified) while pressing your chosen character.
2. If a confirmation dialog box opens, click **Yes**.

Using the File Sanitizer icon


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

1. Navigate to the document or folder you want to shred.
2. Drag the asset to the File Sanitizer icon on the desktop.
3. When the confirmation dialog box opens, click **Yes**.

Manually shredding one asset

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

1. Right-click the **HP ProtectTools** icon in the notification area, at the far right of the taskbar, 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**.

– or –

1. Open File Sanitizer, and click **Shred**.
2. Click the **Shred Now** button.
3. 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**.

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

6 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools provides access to the Computer Setup utility security and configuration settings. This gives users Windows access to system security features that are managed by Computer Setup.

With BIOS Configuration, you can accomplish the following objectives:

- Manage administrator passwords.
- Configure other power-on authentication features, such as embedded security authentication.
- Enable and disable hardware features, such as CD-ROM boot or hardware ports.
- Configure boot options, which includes enabling MultiBoot and changing the boot order.

 **NOTE:** Many of the features in BIOS Configuration for HP ProtectTools are also available in Computer Setup.

General tasks


BIOS Configuration allows you to manage various computer settings that would otherwise be accessible only by pressing **f10** at startup to enter Computer Setup.

Accessing BIOS Configuration


To access BIOS Configuration:

1. Click **Start**, click **Settings**, and then click **Control Panel**.
2. Click **HP ProtectTools Security Manager**, and then click **BIOS Configuration**.

You can also access BIOS Configuration from an icon in the notification area, at the far right of the taskbar.

 **NOTE:** To display the HP ProtectTools Security Manager icon, you may need to click the **Show Hidden Icons** icon (< or <<) in the notification area.

- Right-click the **HP ProtectTools Security Manager** icon in the notification area.
 - Click **BIOS Configuration**.
3. If you are an HP ProtectTools user, enter your Windows password.
 - If you enter the Windows password correctly, but you are not a BIOS administrator, your ability to make changes varies according to the security level settings. Refer to [Setting system configuration options on page 63](#)

 **NOTE:** An HP ProtectTools user may or may not be a BIOS administrator.

- If you enter the Windows password incorrectly, you can only view BIOS configuration settings but not change them.
4. If you are not an HP ProtectTools user, the BIOS Configuration software checks to see whether a BIOS administrator password has been set up.
 - If a BIOS administrator password has been set up, you must enter it.
 - If you enter the BIOS administrator password correctly, you can both view and make changes to the BIOS configuration settings.
 - If a BIOS administrator password has been set up, but if you fail to enter it or enter it incorrectly, you can view BIOS configuration settings but you cannot change them.
 - If a BIOS administrator password has not been set, you can both view and make changes to BIOS configuration settings.

Viewing or changing settings

To view or change configuration settings:


1. Click one of the BIOS Configuration pages:
 - File
 - Security
 - System Configuration
2. Make your changes, and then click **Apply** to save your changes and leave the window open.

– or –

Make your changes, and then click **OK** to save your changes and close the window.

3. Exit and restart the computer.


Your changes go into effect when the computer restarts.

 **NOTE:** Password changes take effect immediately with no need to restart the computer.

Viewing system information

Use the “File” page to view the following types of information:

- Identification information about the computer (including the serial number) and about batteries in the system
- Specification information about the processor; cache and memory size; video version; keyboard controller version; and system ROM

 **NOTE:** The “File” page is for information purposes only. None of the displayed information can be modified.


To view system information:

- ▲ Access BIOS Configuration, and click **File**.

Advanced tasks

Setting security options

Use the “Security” page of BIOS Configuration to enhance the security of your computer.

 **NOTE:** Not all options are available on all computers, and additional options may also be included.

To set security options:

1. Access BIOS Configuration, and click **Security**.
2. Select any of the options listed in the table below.
3. Change the settings as needed.
4. Click **Apply** to apply the new settings and leave the window open.

– or –

Click **OK** to apply the new settings and close the window.


Security

| Option | Action |
|--|---|
| BIOS Administrator Password | Click the Set button to set a BIOS administrator password. |
| NOTE: This option may be called “Setup Password”. | |

System IDs

| Option | Action |
|-----------------------|------------------------|
| Ownership Tag | Enter, view or change. |
| Asset Tracking Number | Enter, view or change. |

TPM Embedded Security

 **NOTE:** This feature is supported only on computers equipped with the HP ProtectTools Embedded Security Chip (TPM).

| Option | Action |
|---------------------------------------|-----------------------------|
| Reset of TPM from OS | Enable or disable. |
| OS Management of TPM | Enable or disable. |
| Embedded Security Device Availability | Select available or hidden. |

| Option | Action |
|---------------------------------|---|
| Power-On Authentication Support | Enable or disable support for smart card power-on authentication. NOTE: This feature is supported only on computers with optional smart card readers. |
| Automatic Drivelock Support | Enable or disable. |

Administrator Tools

| Option | Action |
|--|--------------------|
| HP SpareKey | Enable or disable. |
| Fingerprint Reset on Reboot (if present) | Enable or disable. |

Password Policy


| Option | Action |
|--|--------------------|
| At least one symbol required | Enable or disable. |
| At least one number required | Enable or disable. |
| At least one upper case character required | Enable or disable. |
| At least one lower case character required | Enable or disable. |
| Are spaces allowed in password | Enable or disable. |

Hard Disk Sanitization Report

| Option | Action |
|------------------------|---|
| Hard Disk Sanitization | If hard disk sanitization has been run at least once, you can view information about the most recent hard disk sanitization procedures that have been completed on the computer. NOTE: This option erases sensitive data from a computer hard drive. If a hard drive has been sanitized and then removed from the computer, the information about that sanitization process is still available. |

Setting system configuration options

Use the “System Configuration” page to view and modify system configuration settings.

 **NOTE:** Not all options are available on all computers, and additional options may also be included.

To set system configuration options:

1. Access **BIOS Configuration**, and then click **System Configuration**.
2. Select one of the following options, as described in the table below:
 - **Port options**
 - **Boot options**
 - **Device configuration options**
 - **Built-in device options**
 - **AMT options (select models only)**
 - **Security level options**
3. Change the settings as needed.
4. Click **Apply** to apply the new settings to the system and leave the window open.

– or –

Click **OK** in the HP ProtectTools Security Manager window to apply the new settings to the system and close the window.

Port options

| Option | Action |
|--------------------|--------------------|
| Flash Media Reader | Enable or disable. |
| USB Ports | Enable or disable. |
| 1394 port | Enable or disable. |
| Express Card slot | Enable or disable. |

Boot options

| Option | Action |
|--------------------------------|---|
| Startup Check Delay (Sec) | Set the Startup Check Delay, in seconds. |
| Custom Logo | Enable or disable. |
| Express Boot Popup Delay (Sec) | Set the Express Boot Popup Delay, in seconds. |
| CD-ROM Boot | Enable or disable. |
| SD Card Boot | Enable or disable. |
| Boot from EFI File | Enable or disable. |
| Floppy boot | Enable or disable. |
| PXE Internal NIC boot | Enable or disable. |
| Boot Order | Set the order in which system devices boot. |

Device configuration options

| Option | Action |
|---------------------------------|--|
| USB Legacy Support | Enable or disable. |
| Parallel port mode | Select a parallel port mode: standard, bidirectional, EPP (Enhanced Parallel Port), or ECP (Enhanced Capabilities Port). |
| Fan always on while on AC power | Enable or disable the system fan when connected to an AC outlet. |
| Data execution prevention | Enable/disable the option to monitor memory use and shut down suspicious programs. |
| SATA device mode | Select IDE, AHCI, or RAID. |
| Dual core CPU | Enable or disable. |
| Secondary battery fast charge | Enable or disable. |
| HP QuickLook 2 | Enable or disable. |
| TXT technology | Enable or disable. |
| Display Diagnostic URL | Enable or disable. |
| HDD Translation Mode | Select Bit-shift or LBA-assisted. |
| Virtualization technology | Enable or disable the option to allow multiple virtual machines to run side by side on the same computer. |

Built-in device options

| Option | Action |
|------------------------------------|--|
| Wireless Button State | Enable or disable. |
| Embedded WWAN Device Radio | Enable or disable. |
| Fingerprint Device | Enable or disable. |
| Notebook MultiBay | Enable or disable. |
| Network Interface Controller (LAN) | Enable or disable. |
| Ambient light sensor | Enable or disable. |
| Embedded Bluetooth® Device Radio | Enable or disable. |
| Wake on LAN | Enable or disable the option to turn on the computer remotely from another computer connected to the same network. |

AMT options (select models only)

| Option | Action |
|-------------------------|-----------------------|
| Terminal Emulation Mode | Select ANSI or VT100. |
| Firmware Verbosity | Enable or disable. |

| Option | Action |
|---------------------------------|--------------------|
| Firmware Progress Event Support | Enable or disable. |
| Unconfigure AMT on next boot | Enable or disable. |

Security Level options




NOTE: These settings control the access level of HP ProtectTools users.

| Option | Action |
|--|------------------------|
| CD-ROM Boot Security Level | Change, view, or hide. |
| Floppy Boot Security Level | Change, view, or hide. |
| Internal Network Adapter Boot Security Level | Change, view, or hide. |
| USB Legacy Support Security Level | Change, view, or hide. |
| Fan Always on while on AC Power Security Level | Change, view, or hide. |
| Flash Media Reader Security Level | Change, view, or hide. |
| Startup Check Delay (Sec) Security Level | Change, view, or hide. |
| Parallel Port Mode Security Level | Change, view, or hide. |
| Express Boot Popup Delay (Sec) Security Level | Change, view, or hide. |
| LAN/WLAN Switching Security Level | Change, view, or hide. |
| Embedded Bluetooth Device Radio Security Level | Change, view, or hide. |
| Embedded WWAN Device Radio Security Level | Change, view, or hide. |
| Power-On Authentication Support Security Level | Change, view, or hide. |
| Automatic Drivelock Support Security Level | Change, view, or hide. |
| Data Execution Prevention Security Level | Change, view, or hide. |
| SATA Device Mode Security Level | Change, view, or hide. |
| USB Ports Security Level | Change, view, or hide. |
| 1394 Port Security Level | Change, view, or hide. |
| Express Card Slot Security Level | Change, view, or hide. |
| Dual Core CPU Security Level | Change, view, or hide. |
| Wake on LAN Security Level | Change, view, or hide. |
| Ambient Light Sensor Security Level | Change, view, or hide. |
| Secondary Battery Fast Charge Security Level | Change, view, or hide. |
| Embedded Security Device Availability Security Level | Change, view, or hide. |
| HDD Translation Mode Security Level | Change, view, or hide. |
| Fingerprint Device Security Level | Change, view, or hide. |
| Optical Disk Drive Security Level | Change, view, or hide. |

| | |
|---|------------------------|
| Network Interface Controller (LAN) Security Level | Change, view, or hide. |
| OS Management of TPM Security Level | Change, view, or hide. |
| Reset of TPM from OS Security Level | Change, view, or hide. |
| Virtualization Technology Security Level | Change, view, or hide. |
| Terminal Emulation Mode Security Level | Change, view, or hide. |
| Firmware Verbosity Security Level | Change, view, or hide. |
| Firmware Progress Event Support Security Level | Change, view, or hide. |
| Unconfigure AMT Security Level | Change, view, or hide. |
| Asset Tracking Number Security Level | Change, view, or hide. |
| Ownership Tag Security Level | Change, view, or hide. |
| Boot Order Security Level | Change, view, or hide. |
| Custom Logo Policy | Change, view, or hide. |
| Unconfigure AMT on next boot Security Level | Change, view, or hide. |
| SD Card Boot Security Level | Change, view, or hide. |
| Boot From EFI File Security Level | Change, view, or hide. |
| HP QuickLook 2 Security Level | Change, view, or hide. |
| Wireless Button State Security Level | Change, view, or hide. |
| Modem Device Security Level | Change, view, or hide. |
| Finger Print reset Security Level | Change, view, or hide. |
| HP SpareKey Security Level | Change, view, or hide. |
| TXT Technology Security Level | Change, view, or hide. |
| Diagnostic URL Security Level | Change, view, or hide. |

7 Embedded Security for HP ProtectTools (select models only)

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

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

- Enhanced Microsoft® Encryption File System (EFS) file and folder encryption
- Creation of a personal secure drive (PSD) for protecting user data
- Data management functions, such as backing up and restoring the key hierarchy
- Support for third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations when using the Embedded Security software

The TPM embedded security chip enhances and enables other HP ProtectTools Security Manager security features. For example, Credential Manager for HP ProtectTools can use the embedded chip as an authentication factor when the user logs on to Windows. On select models, the TPM embedded security chip also enables enhanced BIOS security features accessed through BIOS Configuration for HP ProtectTools.

Setup procedures

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

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

Enabling the embedded security chip

The embedded security chip must be enabled in the Computer Setup utility. This procedure cannot be performed in BIOS Configuration for HP ProtectTools.

To enable the embedded security chip:

1. Open Computer Setup by turning on or restarting the computer, and then pressing **f10** while the “f10 = ROM Based Setup” message is displayed in the lower-left corner of the screen.
2. If you have not set an administrator password, use the arrow keys to select **Security**, select **Setup password**, and then press **enter**.
3. Type your password in the **New password** and **Verify new password** boxes, and then press **f10**.
4. In the **Security** menu, use the arrow keys to select **TPM Embedded Security**, and then press **enter**.
5. Under **Embedded Security**, if the device is hidden, select **Available**.
6. Select **Embedded security device state** and change to **Enable**.
7. Press **f10** to accept the changes to the Embedded Security configuration.
8. To save your preferences and exit Computer Setup, use the arrow keys to select **File**, and click **Save Changes and Exit**. Then follow the on-screen instructions.

Initializing the embedded security chip

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

- Set an owner password for the embedded security chip that protects access to all owner functions on the embedded security chip.
- Set up the emergency recovery archive, which is a protected storage area that allows reencryption of the Basic User Keys for all users.

To initialize the embedded security chip:

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

The HP ProtectTools Embedded Security Initialization Wizard opens.

2. Follow the on-screen instructions.

Setting up the basic user account

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

- Produces a Basic User Key that protects encrypted information, and sets a Basic User Key password to protect the Basic User Key.
- Sets up a personal secure drive (PSD) for storing encrypted files and folders.


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

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

1. If the Embedded Security User Initialization Wizard is not open, click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **User Settings**.
3. In the right pane, under **Embedded Security Features**, click **Configure**.

The Embedded Security User Initialization Wizard opens.

4. Follow the on-screen instructions.

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

General tasks

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

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

Using the Personal Secure Drive

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

Encrypting files and folders

When working with encrypted files, consider the following rules:

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

To encrypt files and folders:

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

Sending and receiving encrypted e-mail

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

Changing the Basic User Key password

To change the Basic User Key password:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **User Settings**.
3. In the right pane, under **Basic User Key password**, click **Change**.
4. Type the old password, and then set and confirm the new password.
5. Click **OK**.

Advanced tasks

Backing up and restoring

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

Creating a backup file

To create a backup file:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Backup**.
3. In the right pane, click **Backup**. The HP Embedded Security for ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.

Restoring certification data from the backup file

To restore data from the backup file:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Backup**.
3. In the right pane, click **Restore**. The HP Embedded Security for ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.

Changing the owner password

To change the owner password:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Advanced**.
3. In the right pane, under **Owner Password**, click **Change**.
4. Type the old owner password, and then set and confirm the new owner password.
5. Click **OK**.

Resetting a user password

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

Enabling and disabling Embedded Security

It is possible to disable the Embedded Security features if you want to work without the security function.

The Embedded Security features can be enabled or disabled at 2 different levels:

- Temporary disabling—With this option, embedded security is automatically reenabled on Windows restart. This option is available to all users by default.
- Permanent disabling—With this option, the owner password is required to reenable Embedded Security. This option is available only to administrators.

Permanently disabling Embedded Security

To permanently disable Embedded Security:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Advanced**.
3. In the right pane, under **Embedded Security**, click **Disable**.
4. Type your owner password at the prompt, and then click **OK**.

Enabling Embedded Security after permanent disable

To enable Embedded Security after permanently disabling it:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Advanced**.
3. In the right pane, under **Embedded Security**, click **Enable**.
4. Type your owner password at the prompt, and then click **OK**.

Migrating keys with the Migration Wizard

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

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

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

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

- Device profiles that are created for each user to define device access
- Device access that can be granted or denied on the basis of group membership

Starting background service

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


Simple configuration

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

- USB devices for all non-administrators
- All removable media (floppy disks, pen drives, etc.) for all non-administrators
- All DVD/CD-ROM drives for all non-administrators
- All serial and parallel ports for all non-administrators

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

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Simple Configuration**.
3. In the right pane, select the check box of a device to deny access.
4. Click **Apply**.

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

5. Click **OK**.

Device class configuration (advanced)

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

Adding a user or a group

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. In the device list, click the device class that you want to configure.
4. Click **Add**. The **Select Users or Groups** dialog box opens.
5. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
6. Click a user or a group to be added to the list of available users and groups, and then click **OK**.
7. Click **OK**.

Removing a user or a group

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. In the device list, click the device class that you want to configure.
4. Click the user or group you want to remove, and then click **Remove**.
5. Click **Apply**, then click **OK**.

Denying access to a user or group

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. In the device list, click the device class that you want to configure.
4. Under **User/Groups**, click the user or group to be denied access.
5. Click **Deny** next to the user or group to be denied access.
6. Click **Apply**, and then click **OK**.

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

You can allow one user access to a device class while denying access to all other members of that user's group.

To allow access to one user but not the group:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. Click the device class that you want to configure in the device list.

4. Under **User/Groups**, add the group to be denied access.
5. Click **Deny** next to the group to be denied access.
6. Navigate to the folder below that of the required class and add the specific user. Click **Allow** to grant this user access.
7. Click **Apply**, and then click **OK**.

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

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

To allow access to a specific device for one user but not the group:

1. Click **Start**, click **All Programs**, and then click **HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. In the device list, click the device class that you want to configure, and then navigate to the folder below that.
4. Under **User/Groups**, add the group to be denied access.
5. Click **Deny** next to the group to be denied access.
6. Navigate to the specific device to be allowed for the user in the device list.
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 a user to be allowed access, and then click **OK**.
10. Click **Allow** to grant this user access.
11. Click **Apply**, and then click **OK**.

9 Troubleshooting

Credential Manager for HP ProtectTools

| Short description | Details | Solution |
|---|---|---|
| Using the Credential Manager Network Accounts option, a user can select which domain account to log on to. When TPM authentication is used, this option is not available. All other authentication methods work properly. | Using TPM authentication, the user is only logged on to the local computer. | Using Credential Manager Single Sign On tools allows the user to authenticate other accounts. |
| Smart cards and USB tokens are not available in Credential Manager if installed after the Credential Manager installation. | <p>In order to use smart cards or USB tokens in Credential Manager, the supporting software (drivers, PKCS#11 providers, etc.) must be installed prior to Credential Manager installation.</p> <p>If you already have the Credential Manager installed do the following steps after installing smart card or token supporting software:</p> | <p>Log on to Credential Manager.</p> <p>In HP ProtectTools Security Manager, click Credential Manager, click Advanced Settings, and then click the Smart Cards and Tokens tab. A list of available tokens is displayed under Local Tokens.</p> <p>Access a popup menu by right-clicking the Local Tokens node, and then select Scan for New Smart Cards and Tokens.</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>Credential 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 Credential 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 Browse for Virtual Token is not displayed during the logon process. | The user cannot move the location of a registered virtual token in Credential 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 Credential Manager using an account with Administrator's rights on the domain and the local PC. When the domain administrator attempts to change the | Credential Manager cannot change a domain user's account password through Change Windows password . Credential Manager can only change the local PC account passwords. The domain user can change his/her password through the Change password option of Windows security , but since the domain user does not have a physical account on the |

| Short description | Details | Solution |
|--|---|--|
| | Windows password from Credential Manager, the administrator gets an error logon failure: User account restriction . | local PC, Credential Manager can only change the password used to log on. |
| Credential Manager has incompatibility issues with Corel WordPerfect 12 password GINA. | If the user logs on to Credential Manager, creates a document in WordPerfect, and saves with password protection, Credential Manager cannot detect or recognize, either manually or automatically, the password GINA. | HP is researching a workaround for future product enhancements. |
| Credential Manager does not recognize the Connect button on screen. | If the Single Sign On credentials for Remote Desktop Connection (RDP) are set to Connect , when Single Sign On is relaunched, it always enters Save As instead of Connect . | HP is researching a workaround for future product enhancements. |
| Users can lose all Credential Manager credentials protected by the TPM. | If the TPM module is removed or damaged, users lose all credentials protected by the TPM. | This is as designed. The TPM Module is designed to protect the Credential Manager credentials. HP recommends that the user back up their identity from Credential Manager prior to removing the TPM module. |
| The user is unable to log on to Credential 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 Credential Manager and the Windows logon screen remains displayed no matter which logon credential (password, fingerprint, or Java Card) is selected. | Update Windows to Service Pack 2 via Windows Update. Refer to Microsoft knowledge base article 813301 at http://www.microsoft.com for more information on the cause of the issue. In order to log on, the user must select Credential Manager and log on. After logging on to Credential 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. If the user logs on to Windows first, then the user must manually log on to Credential Manager. |
| Restoring Embedded Security causes Credential Manager to fail. | Credential Manager fails to register any credentials after the ROM is restored to factory settings. | Credential Manager fails to access the TPM if the ROM is reset to factory settings after installing Credential Manager. The TPM embedded security chip can be enabled using the f10 Computer Setup utility, BIOS Configuration, or HP Client Manager. To enable the TPM embedded security chip using Computer Setup, follow these steps: <ol style="list-style-type: none"> 1. Open Computer Setup by turning on or restarting the computer, and then pressing f10 while the f10 = ROM Based Setup message is displayed in the lower-left corner of the screen. 2. Use the arrow keys to click Security, and then click Setup Password. Set a password. 3. Select Embedded Security Device. 4. Use the arrow keys to select Embedded Security Device—Disable. Use the arrow keys to change it to Embedded Security Device—Enable. 5. Click Enable, and then click Save changes and exit. |

| Short description | Details | Solution |
|--|--|---|
| The security Restore Identity process loses association with virtual token. | When user restores identity, Credential Manager can lose the association with the location of the virtual token at logon screen. Even though Credential Manager has the virtual token registered, the user must reregister the token to restore the association. | HP is investigating resolution options for future customer software releases. This is currently by design. When uninstalling Credential 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. HP is investigating long-term options for resolution. |

Embedded Security for HP ProtectTools (select models only)

| Short description | Details | Solution |
|--|---|--|
| Encrypting folders, subfolders, and files on PSD causes an error message. | If the user copies files and folders to the PSD and tries to encrypt folders/files or folders/subfolders, the Error Applying Attributes message is displayed. The user can encrypt the same files on the C:\ drive or an extra installed hard drive. | This is as designed. Moving files/folders to the PSD automatically encrypts them. There is no need to "double-encrypt" the files/folders. Attempting to double-encrypt them on the PSD using EFS produces this error message. |
| Cannot Take Ownership With Another OS In MultiBoot Platform. | If a drive is set up for multiple OS boot, ownership can only be taken with the platform initialization wizard in one operating system. | This is as designed, for security reasons. |
| An unauthorized administrator can view, delete, rename, or move the contents of encrypted EFS folders. | Encrypting a folder does not stop an unauthorized user with administrative rights to view, delete, or move contents of the folder. | This is as designed. It is a feature of EFS, not the Embedded Security TPM. Embedded Security uses Microsoft EFS software, and EFS preserves file/folder access rights for all administrators. |
| The user has no encrypt options when attempting to restore the hard drive using FAT32. | If the user attempts to restore the hard drive using FAT32, there will be no encrypt options for any files/folders using EFS. | This is as designed. Software should not be installed on a restore with a FAT32 partition. Microsoft EFS is supported only on NTFS and does not function on FAT32. This is a feature of Microsoft EFS and is not related to HP ProtectTools software. |
| The user is able to encrypt or delete the recovery archive XML file. | By design, the ACLs for this folder are not set; therefore, a user can inadvertently or purposely encrypt or delete the file, thus making it inaccessible. After this file has been encrypted or deleted, no one can use the TPM software. | This is as designed. Users have access rights to an emergency archive so that they can save/update their Basic User Key backup copy. Users should be instructed never to encrypt or delete the recovery archive files. |
| Embedded Security EFS interaction with Symantec Antivirus or McAfee Total Protection produces longer encryption/decryption and scan times. | Encrypted files interfere with Symantec Antivirus or McAfee Total Protection virus scan. Encrypting files using Embedded Security EFS takes longer when Symantec Antivirus or McAfee Total Protection is running. | To reduce the time required to scan Embedded Security EFS files, the user can either type the encryption password before scanning or decrypt before scanning. To reduce the time required to encrypt/decrypt data using Embedded Security EFS, the user should disable Auto-Protect on Symantec Antivirus or McAfee Total Protection. |
| The emergency recovery archive cannot be saved to removable media. | If the user inserts a MultiMediaCard or Secure Digital (SD) Memory Card when creating the emergency recovery archive path during Embedded Security initialization, an error message is displayed. | This is as designed. Storage of the recovery archive on removable media is not supported. The recovery archive can be stored on a network drive or on another local drive other than the C drive. |

| Short description | Details | Solution |
|--|---|--|
| Errors occur after a power loss interrupts Embedded Security initialization. | <p>If there is a power loss during the initialization of the Embedded Security chip, the following issues occur:</p> <ul style="list-style-type: none"> When attempting to launch the Embedded Security Initialization Wizard, the following error message is displayed: The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner. When attempting to launch the User Initialization Wizard, the following error message is displayed: The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first. | <p>Perform the following procedure to recover from the power loss:</p> <p>NOTE: Use the arrow keys to select various menus, menu items, and to change values (unless otherwise specified).</p> <ol style="list-style-type: none"> Start or restart the computer. Press f10 when the f10=Setup message appears on the screen. Select the appropriate language option. Press enter. Select Security, and then click Embedded Security. Set the Embedded Security Device option to Enable. Press f10 to accept the change. Select File, and then click Save Changes and Exit. Press enter. Press f10 to save the changes and exit the utility. |
| The Computer Setup (f10) Utility password can be removed after enabling the TPM Module. | Enabling the TPM module requires a Computer Setup (f10) Utility password. When the module has been enabled, the user can remove the password. This allows anyone with direct access to the system to reset the TPM module and cause possible loss of data. | <p>This is as designed.</p> <p>The Computer Setup (f10) Utility password can only be removed by a user who knows the password. However, HP strongly recommends having the Computer Setup (f10) Utility password protected at all times.</p> |
| The PSD password box is no longer displayed when the system becomes active after standby status | When a user logs on to the system after creating a PSD, the TPM asks for the Basic User password. If the user does not type the password and the system initiates Standby, the password dialog box is no longer available when the user resumes. | <p>This is by design.</p> <p>The user has to log off and back on to view the PSD password box again.</p> |
| No password is required to change the Security Platform Policies. | Access to Security Platform Policies (both Machine and User) does not require a TPM password for users who have administrative rights on the system. | <p>This is by design.</p> <p>Any administrator can modify the Security Platform Policies with or without TPM user initialization.</p> |
| When a certificate is viewed, it shows as non-trusted. | After setting up HP ProtectTools and running the User Initialization Wizard, the user has the ability to view the certificate issued; however, when the certificate is viewed, it shows as non-trusted. While the certificate can be installed at this point by clicking the install button, installing it does not make it trusted. | Self-signed certificates are not trusted. In a properly configured enterprise environment, EFS certificates are issued by online Certification Authorities and are trusted. |

| Short description | Details | Solution |
|---|---|--|
| An intermittent encrypt and decrypt error occurs: The process cannot access the file because it is being used by another process. | This is an extremely intermittent error during file encryption or decryption which occurs because the file is being used by another process, even though that file or folder is not being processed by the operating system or other applications. | To resolve the failure: <ol style="list-style-type: none"> 1. Restart the system. 2. Log off. 3. Log back on. |
| Data loss in removable storage occurs if the storage media is removed prior to completing the new data generation or transfer. | Removing storage media such as a MultiBay hard drive still shows PSD availability and does not generate errors while adding/modifying data to the PSD. After the system is restarted, the PSD does not reflect file changes that occurred while the removable storage was unavailable. | Do not remove a PSD before data generation or transfer is complete. This issue is only experienced if the user accesses the PSD, then removes the hard drive before completing new data generation or transfer. If the user attempts to access the PSD when the removable hard drive is not present, an error message is displayed stating that the device is not ready . |
| During uninstall, if the user has not initialized the Basic User and opens the Administration tool, the Disable option is not available and Uninstaller will not continue until the Administration tool is closed. | <p>The user has the option of uninstalling either without disabling the TPM or by first disabling the TPM (through the Administration tool), and then uninstalling. Accessing the Administration tool requires Basic User Key initialization. If basic initialization has not occurred, all options are inaccessible to the user.</p> <p>Since the user has explicitly chosen to open the Administration tool (by clicking Yes in the dialog box prompting Click Yes to open Embedded Security Administration tool), uninstall waits until the Administration tool is closed. If the user clicks No in that dialog box, the Administration tool does not open at all and uninstall proceeds.</p> | The Administration tool is used for disabling the TPM chip, but that option is not available unless the Basic User Key has already been initialized. If it has not been initialized, select OK or Cancel to continue with the uninstallation. |
| Intermittent system lockup occurs after creating PSD on 2-user accounts and using fast-user-switching in 128-MB system configurations. | The system may lock up with a black screen and nonresponding keyboard and mouse instead of showing welcome (logon) screen when using fast-switching with minimal RAM. | <p>The root cause is suspected to be a timing issue in low memory configurations.</p> <p>Integrated graphics uses UMA architecture taking 8 MB of memory, which leaves only 120 MB available to the user. The error is generated when this 120 MB is shared by both users who are logged on and are fast-user-switching.</p> <p>The workaround is to reboot the system and increase memory configuration (HP does not ship 128-MB configurations with security modules).</p> |
| EFS User Authentication (password request) times out with access denied . | The EFS User Authentication password reopens after the user clicks OK or the system exits Standby. | This is by design—to avoid issues with Microsoft EFS, a 30-second watchdog timer was created to generate the error message). |
| Minor truncation during setup of Japanese is observed in functional descriptions. | Functional descriptions during custom setup option during installation wizard are truncated. | HP will correct this in a future release. |
| EFS Encryption works without a password being typed in the prompt. | By allowing the prompt for User password to time out, encryption is still available on a file or folder. | The ability to encrypt does not require password authentication, since this is a feature of the Microsoft EFS encryption. Decryption will require the user password to be supplied. |

| Short description | Details | Solution |
|--|---|---|
| Secure e-mail is supported, even when secure e-mail is not specified in the User Initialization Wizard or when secure e-mail configuration is disabled in user policies. | Embedded security software and the wizard do not control settings of an e-mail client (Outlook, Outlook Express, or Netscape). | This behavior is as designed. Configuration of TPM e-mail settings does not prohibit editing encryption settings directly in an e-mail client. Usage of secure e-mail is set and controlled by 3rd-party applications. The HP wizard allows linkage to the three reference applications for immediate customization. |
| Running Large Scale Deployment a second time on the same PC or on a previously initialized PC overwrites Emergency Recovery and Emergency Token files. The new files are useless for recovery. | Running Large Scale Deployment on any previously initialized HP ProtectTools Embedded Security system renders existing Recovery Archives and Recovery Tokens useless by overwriting those XML files. | HP is working to resolve the XML-file-overwrite issue and will provide a solution in a future SoftPaq. |
| Automated logon scripts do not function during user restore in Embedded Security. | <p>The error occurs after the user performs the following actions:</p> <ul style="list-style-type: none"> • Initializes owner and user in Embedded Security (using the default locations—My Documents). • Resets the chip to factory settings in the BIOS. • Reboots the computer. • Begins to restore Embedded Security. During the restore process, Credential Manager asks if the system can automate the logon to Infineon TPM User Authentication. If the user selects Yes, the location of SPEmRecToken is automatically displayed in the text box. <p>Even though this location is correct, the following error message is displayed: No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.</p> | Click the Browse button on the screen to select the location, and the restore process proceeds. |
| Multiple-User PSDs do not function in a fast-user-switching environment. | This error occurs when multiple users have been created and given a PSD with the same drive letter. If an attempt is made to fast-user-switch between users when the PSD is loaded, the second user's PSD is unavailable. | The second user's PSD will be available only if it is reconfigured to use another drive letter or if the first user is logged off. |
| The PSD is disabled and cannot be deleted after formatting the hard drive on which the PSD was generated. | <p>The PSD icon is still visible, but the error message drive is not accessible is displayed when the user attempts to access the PSD.</p> <p>The user is not able to delete the PSD and the following message is displayed: your PSD is still in use, please be sure that your PSD contains no open files</p> | <p>As designed: If a customer force-deletes or disconnects from the storage location of the PSD data, the Embedded Security PSD drive emulation continues to function and will produce errors based on lack of communication with the missing data.</p> <p>Resolution: After the next reboot, the emulations fail to load and user can delete the old PSD emulation and create a new PSD.</p> |

| Short description | Details | Solution |
|--|--|--|
| | <p>and is not accessed by another process. The user must reboot the system in order to delete the PSD and it is not loaded after reboot.</p> | |
| <p>An internal error is detected when the user is restoring from the Automatic Backup Archive.</p> | <p>In Embedded Security, if the user clicks the Restore under Backup option to restore from the automatic backup Archive and then selects SPSystemBackup.xml, the Restore Wizard fails and the following error message is displayed: The selected Backup Archive does not match the restore reason. Please select another archive and continue.</p> | <p>If the user selects SpSystemBackup.xml when the SpBackupArchive.xml is required, the Embedded Security Wizard fails and displays the following message: An internal Embedded Security error has been detected.</p> <p>The user must select the correct XML file to match the required reason.</p> <p>The processes are working as designed and function properly; however, the internal Embedded Security error message is not clear and should state a more appropriate message. HP is working to enhance this in future products.</p> |
| <p>The security system exhibits a restore error with multiple users.</p> | <p>During the restore process, if the administrator selects users to restore, the users not selected are not able to restore the keys when trying to restore at a later time. A decryption process failed error message is displayed.</p> | <p>The non-selected users can be restored by resetting the TPM, running the restore process, and selecting all users before the next default daily backup runs. If the automated backup runs, it overwrites the non-restored users and their data is lost. If a new system backup is stored, the previous unselected users cannot be restored.</p> <p>Also, the user must restore the entire system backup. An Archive Backup can be restored individually.</p> |
| <p>Resetting System ROM to default hides the TPM.</p> | <p>Resetting the system ROM to default hides the TPM to Windows. This does not allow the security software to operate properly and makes TPM-encrypted data inaccessible.</p> | <p>Unhide the TPM in BIOS:</p> <p>Open the Computer Setup (f10) Utility, navigate to Security > Device security, and then modify the field from Hidden to Available.</p> |

| Short description | Details | Solution |
|--|--|--|
| Automatic backup does not work with the mapped drive. | <p>When an administrator sets up Automatic Backup in Embedded Security, it creates an entry in Windows > Tasks > Scheduled Task. This Windows Scheduled Task is set to use NT AUTHORITY\SYSTEM for rights to execute the backup. This works properly to any local drive.</p> <p>When the administrator instead configures the Automatic Backup to save to a mapped drive, the process fails because the NT AUTHORITY\SYSTEM does not have the rights to use the mapped drive.</p> <p>If the Automatic Backup is scheduled to occur upon logon, Embedded Security TNA Icon displays the following message: The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again. If the Automatic Backup is scheduled for a specific time, however, the backup fails without displaying notice of the failure.</p> | <p>The workaround is to change the NT AUTHORITY \SYSTEM to (computer name)\(admin name). This is the default setting if the Scheduled Task is created manually.</p> <p>HP is working to provide future product releases with default settings that include computer name\admin name.</p> |
| Embedded Security cannot be temporarily disabled in the Embedded Security GUI. | <p>The current 4.0 software was designed for HP Notebook 1.1B implementations, as well as supporting HP Desktop 1.2 implementations.</p> <p>This option to disable is still supported in the software interface for TPM 1.1 platforms.</p> | HP will address this issue in future releases. |

Device Access Manager for HP ProtectTools

| Short description | Details | Solution |
|--|---|---|
| Users have been denied access to devices within Device Access Manager, but the devices are still accessible. | 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. | <p>Verify that the HP ProtectTools Device Locking service has started.</p> <p>As an administrative user, browse to Control Panel > Administrative Tools > Services. In the Services window, search for the HP ProtectTools Device Locking/Auditing service. Be sure that the service is started and that the startup type is Automatic.</p> |
| A user has unexpected access to a device or a user is unexpectedly denied access to a device. | 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. | <p>The Device Class Configuration within Device Access Manager should be used to investigate the Users device settings.</p> <p>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 the 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.</p> |
| Allow or deny—which takes precedence? | <p>Within Device Class Configuration, the following configuration has been set:</p> <ul style="list-style-type: none"> 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). <p>If a user is a member of both those groups (e.g., Administrator), which takes precedence?</p> | <p>The user is denied access to the device. Deny takes precedence over Allow.</p> <p>Access is denied due to 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.</p> <p>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.</p> <p>A further workaround would be to have 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.</p> |

Miscellaneous

| Software Impacted— Short description | Details | Solution |
|--|---|--|
| Security Manager— Warning received: The security application can not be installed until the HP Protect Tools Security Manager is installed. | All security applications such as Embedded Security, 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. |
| TPM Firmware Update Utility for models containing Broadcom-enabled TPMs—The tool provided through HP support Web site reports ownership required. | <p>This is the expected behavior of the TPM firmware utility for models containing Broadcom-enabled TPMs.</p> <p>The firmware upgrade tool allows the user to upgrade the firmware, with or without an endorsement key (EK). When there is no EK, no authorization is required to complete the firmware upgrade.</p> <p>When there is an EK, a TPM owner must exist, since the upgrade requires owner authorization. After the successful upgrade, the platform must be restarted for the new firmware to take effect.</p> <p>If the BIOS TPM is factory-reset, ownership is removed and firmware update capability is prevented until the Embedded Security Software platform and User Initialization Wizard have been configured.</p> <p>NOTE: A reboot is always recommended after performing a firmware update. The firmware version is not identified correctly until after the reboot.</p> | <ol style="list-style-type: none"> 1. Reinstall Embedded Security Software. 2. Run the Platform and User Configuration Wizard. 3. Be sure that the system contains Microsoft .NET framework 1.1 installation: <ol style="list-style-type: none"> a. Click Start. b. Click Control Panel. c. Click Add or remove programs. d. Be sure that Microsoft .NET Framework 1.1 is listed. 4. Check the hardware and software configuration: <ol style="list-style-type: none"> a. Click Start. b. Click All Programs. c. Click HP ProtectTools Security Manager. d. Select Embedded Security from the tree menu. e. Click More Details. The system should have the following configuration: <ul style="list-style-type: none"> • Product version = V4.0.1 • Embedded Security State: Chip State = Enabled, Owner State = Initialized, User State = Initialized • Component Info: TCG Spec. Version = 1.2 • Vendor = Broadcom Corporation • FW Version = 2.18 (or greater) • TPM Device driver library version 2.0.0.9 (or greater) 5. If the FW version does not match 2.18, download and update the TPM firmware. The TPM Firmware SoftPak is a support download available on the HP Web site at http://www.hp.com. |
| HP ProtectTools Security Manager—Intermittently, | Intermittently (1 in 12 instances), an error is created by using the close button in the | This is related to a timing dependency on plug-in services load time when closing and restarting Security |

| Software Impacted— Short description | Details | Solution |
|---|---|--|
| an error is returned when closing the Security Manager interface. | upper right of the screen to close Security Manager before all plug-in applications have finished loading. | <p>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"> • Deletion of PSD • Malicious modification of user settings • Disabling of security policies and functions | <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> |
| The BIOS and OS Embedded Security passwords are out of synch. | If a user does not validate a new password as the BIOS Embedded Security password, the BIOS Embedded Security password reverts back to the original embedded security password through f10 BIOS. | This is functioning as designed; these passwords can be re-synchronized by changing the OS Basic User password and authenticating it at the BIOS Embedded Security password prompt. |
| Only one user can log on to the system after TPM preboot authentication is enabled in BIOS. | The TPM BIOS PIN is associated with the first user who initializes the user setting. If a computer has multiple users, the first user is, in essence, the administrator. The first user will have to give his TPM user PIN to other users to use to log on. | This is functioning as designed; HP recommends that the customer’s IT department follow good security policies for rolling out their security solution and ensuring that the BIOS administrator password is configured by IT administrators for system level protection. |
| The user has to change their PIN to make TPM preboot work after a TPM factory reset. | The user has to change their PIN or create another user to initialize their user setting to make TPM BIOS authentication work after reset. There is no option to make TPM BIOS authentication work. | This is as designed; the factory reset clears the Basic User Key. The user must change his user PIN or create a new user to re-initialize the Basic User Key. |
| Power-on authentication support is not set to default using Embedded Security Reset to Factory Settings | In Computer Setup, the Power-on authentication support option is not being reset to factory settings when using the Embedded Security Device option Reset to Factory Settings . By default, Power-on authentication support is set to Disable . | <p>The Reset to Factory Settings option disables Embedded Security Device, which hides the other Embedded Security options (including Power-on authentication support). However, after reenabling Embedded Security Device, Power-on authentication support remains enabled.</p> <p>HP is working on a resolution, which will be provided in future Web-based ROM SoftPaq offerings.</p> |

| Software Impacted— Short description | Details | Solution |
|--|---|---|
| Security Power-On Authentication overlaps the BIOS Password during boot sequence. | Power-On Authentication prompts the user to log on to the system using the TPM password, but, if the user presses f10 to access the BIOS, the user is granted Read rights access only. | To be able to write to BIOS, the user must type the BIOS password instead of the TPM password at the Power-on Authentication window. |
| The BIOS asks for both the old and new passwords through Computer Setup after the Owner password is changed. | The BIOS asks for both the old and new passwords through Computer Setup after the Owner password is changed in Embedded Security Windows software. | This is as designed. This is due to the inability of the BIOS to communicate with the TPM, after the operating system is up and running, and to verify the TPM pass phrase. |

Glossary

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

administrator. See Windows administrator.

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

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

automatic DriveLock. Security feature that causes the DriveLock passwords to be generated and protected by the TPM Embedded Security chip. When the user is authenticated by the TPM embedded security chip during startup by entering the correct TPM Basic User Key password, the BIOS unlocks the hard drive for the user.

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

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

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

BIOS administrator password. Computer Setup *setup* password.

BIOS profile. Group of BIOS configuration settings that can be saved and applied to other accounts.

BIOS security mode. Setting in Java Card Security that, when enabled, requires the use of a Java Card and a valid PIN for user authentication.

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

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

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

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

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

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

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

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

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

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

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

Drive Encryption logon screen. A logon screen that is displayed before Windows starts up. Users must enter their Windows user name and the password or 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 File System (EFS). System that encrypts all files and subfolders within the selected folder.

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

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

HP SpareKey. Backup copy of drive encryption key.

identity. In the HP ProtectTools Credential 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](#).

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

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

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

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

power-on authentication. Security feature that requires 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.

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

reboot. Process of restarting the computer.

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

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

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

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

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

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

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

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

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

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

Single Sign On. Feature that stores authentication information and allows you to use the Credential 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.

stringent security. Security feature in BIOS Configuration that provides enhanced protection for the power-on and administrator passwords and other forms of power-on authentication.

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

Trusted Contact list. A listing of Trusted Contacts.

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

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

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

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

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

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

TXT. Trusted Execution Technology.

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

Index

- A**
- access
 - controlling 75
 - preventing unauthorized 6
- accessing 60
- accessing HP ProtectTools Security 4
- account
 - basic user 70
- administrator tasks
 - Credential Manager 22
- advanced tasks
 - BIOS Configuration 62
 - Credential Manager 22
 - Device Access Manager 77
 - Embedded Security 72
- AMT options 65
- B**
- background service, Device Access Manager 75
- backing up and restoring
 - certification information 72
 - Embedded Security 72
 - HP ProtectTools
 - credentials 10
 - Single Sign On data 18
- basic user account 70
- Basic User Key password
 - changing 72
 - setting 70
- biometric readers 13
- BIOS administrator password 9
- BIOS Configuration
 - accessing 60
 - changing settings 61
 - setting security options 62
 - setting system configuration options 63
 - viewing settings 61
 - viewing system information 61
- BIOS Configuration for HP ProtectTools 59
- boot options 63, 64
- built-in device options 63, 65
- C**
- changing settings 61
- Computer Setup
 - administrator password 9
- controlling device access 75
- Credential Manager for HP ProtectTools
 - administrator tasks 22
 - application protection 20
 - application protection, removing 20
 - changing application restriction setting 21
 - credential properties, configuring 23
 - credentials, registering 12
 - custom authentication requirements 23
 - fingerprint log on 13
 - fingerprint reader 13
 - lock workstation 16
 - locking computer 16
 - logging on 11
 - logon password 8
 - logon specifications 22
 - logon wizard 12
 - recovery file password 8
 - registering fingerprints 12
 - registering other credentials 14
 - registering Smart Card 13
 - registering token 13
 - registering virtual token 13
 - restriction application
 - access 20
 - settings, configuring 24
 - setup procedures 11
 - Single Sign On (SSO) 17
 - SSO application, exporting 18
 - SSO application, importing 19
 - SSO application, modifying properties 18
 - SSO application, removing 18
 - SSO applications and credentials 18
 - SSO automatic registration 17
 - SSO credentials, modifying 19
 - SSO manual registration 18
 - SSO new application 17
 - token PIN, changing 15
 - troubleshooting 79
 - user verification 25
 - virtual token, creating 15
 - Windows Logon 16
 - Windows logon password, changing 15
 - Windows logon, allow 24
- D**
- data, restricting access to 6
- decrypting a drive 26
- Device Access Manager for HP ProtectTools
 - background service 75
 - device class configuration 77
 - device class, allowing access to one 77
 - device, allowing access to one 78
 - simple configuration 76
 - troubleshooting 88
 - user or group, adding 77

- user or group, denying access to 77
 - user or group, removing 77
- device configuration options 63, 65
- disabling
 - Embedded Security 73
 - Embedded Security, permanently 73
- Drive Encryption for HP ProtectTools
 - activating 27
 - activating a TPM-protected password 28
 - backup and recovery 28
 - creating backup keys 28
 - deactivating 27
 - decrypting individual drives 28
 - encrypting individual drives 28
 - logging in after Drive Encryption is activated 27
 - managing an existing online recovery account 30
 - managing Drive Encryption 28
 - opening 26
 - performing a local recovery 30
 - performing a recovery 30
 - performing an online recovery 30
 - registering for online recovery 29
- E**
- Embedded Security for HP ProtectTools
 - backup file, creating 72
 - basic user account 70
 - Basic User Key 70
 - Basic User Key password, changing 72
 - certification data, restoring 72
 - enabling after permanent disable 73
 - enabling and disabling 73
 - enabling TPM chip 69
 - encrypted e-mail 71
 - encrypting files and folders 71
 - initializing chip 70
 - migrating keys 74
 - owner password, changing 73
 - password 8
 - permanently disabling 73
 - Personal Secure Drive 71
 - resetting user password 73
 - setup procedures 69
 - troubleshooting 82
- emergency recovery 70
- emergency recovery token password
 - definition 9
 - setting 70
- enabling
 - Embedded Security 73
 - Embedded Security after permanent disable 73
 - TPM chip 69
- encrypting a drive 26
- encrypting files and folders 71
- F**
- f10 Setup password 9
- features, HP ProtectTools 2
- File Sanitizer
 - setting a shred schedule 50, 53
- File Sanitizer for HP ProtectTools
 - aborting a shred or free space bleaching operation 57
 - free space bleaching 49
 - manually activating free space bleaching 57
 - manually shredding all selected items 57
 - manually shredding one asset 56
 - opening 50
 - predefined shred profile 51, 54
 - setting a free space bleaching schedule 51, 53
 - setup procedures 50
 - shred profile 51, 54
 - shred profile, selecting or creating 51, 54
 - shredding 49
 - simple delete profile 52, 55
 - using key sequence to initiate shredding 56
- using the File Sanitizer icon 56
- viewing log files 58
- fingerprints, Credential Manager 12
- H**
- HP ProtectTools features 2
- HP ProtectTools Security, accessing 4
- I**
- initializing embedded security chip 70
- J**
- Java Card Security for HP ProtectTools
 - Credential Manager 13
 - PIN 9
- K**
- key security objectives 6
- L**
- lock workstation 16
- locking computer 16
- O**
- objectives, security 6
- owner password
 - changing 73
 - definition 9
 - setting 70
- P**
- password
 - Basic User Key 72
 - BIOS administrator 60
 - changing owner 73
 - emergency recovery token 70
 - guidelines 10
 - HP ProtectTools 8
 - managing 8
 - owner 70
 - policies, creating 7
 - resetting user 73
 - secure, creating 10
 - Windows 60
 - Windows logon 15
- personal secure drive (PSD) 71

- port options 63, 64
- power-on password
 - definition 9
- Privacy Manager 40
- Privacy Manager for HP
 - ProtectTools
 - add or remove columns 47
 - adding a signature line when signing a Microsoft Word or Microsoft Excel document 40
 - adding a suggested signer's signature line 41
 - adding a trusted contact 37
 - adding Privacy Manager chat activity 44
 - Adding suggested signers to a Microsoft Word or Microsoft Excel document 40
 - adding trusted contacts 37
 - adding trusted contacts using Microsoft Outlook address book 38
 - chatting in the Privacy Manager Chat window 45
 - checking revocation status for a trusted contact 39
 - configuring Privacy Manager Chat for Windows Live Messenger 45
 - configuring Privacy Manager for Microsoft Outlook 43
 - configuring Privacy Manager in a Microsoft Office document 40
 - delete a session 47
 - deleting a Privacy Manager certificate 35
 - deleting a trusted contact 38
 - displaying sessions for a range of dates 47
 - displaying sessions for a specific account 47
 - displaying sessions that are saved in a folder other than the default folder 47
 - encrypting a Microsoft Office document 41
 - exporting Privacy Manager Certificates and Trusted Contacts 48
 - filter displayed sessions 47
 - importing Privacy Manager Certificates and Trusted Contacts 48
 - installing a Privacy Manager certificate 34
 - managing Privacy Manager certificates 34
 - managing trusted contacts 36
 - migrating Privacy Manager Certificates and Trusted Contacts to a different computer 48
 - opening 33
 - removing the encryption from a Microsoft Office document 42
 - renewing a Privacy Manager certificate 35
 - requesting a Privacy Manager certificate 34
 - restoring a Privacy Manager certificate 36
 - reveal all sessions 46
 - reveal sessions for a specific account 46
 - revoking a Privacy Manager certificate 36
 - sealing and sending an e-mail message 43
 - search sessions for specific text 46
 - sending an encrypted Microsoft Office document 42
 - setting a default Privacy Manager certificate 35
 - setup procedures 34
 - signing a Microsoft Office document 40
 - signing and sending an e-mail message 43
 - starting Privacy Manager Chat 44
 - starting the Chat History viewer 46
 - using Privacy Manager in Microsoft Office 40
 - using Privacy Manager in Microsoft Outlook 43
 - using Privacy Manager in Windows Live Messenger 44
 - view a session 46
 - view a session ID 46
 - viewing a sealed e-mail message 43
 - viewing a signed Microsoft Office document 42
 - viewing an encrypted Microsoft Office document 43
 - viewing chat history 45
 - viewing Privacy Manager certificate details 35
 - viewing trusted contact details 38
 - properties
 - application 18
 - authentication 22
 - credential 23
- R**
 - registering
 - application 17
 - credentials 12
 - restricting
 - access to sensitive data 6
 - device access 75
- S**
 - security
 - key objectives 6
 - roles 8
 - Security Level options 66
 - security roles 8
 - security setup password 9
 - setting
 - boot options 63
 - built-in device options 63
 - device configuration options 63
 - port options 63
 - security options 62
 - system configuration options 63
 - shred profile
 - customizing 51, 54

- predefined 51, 54
- selecting or creating 51, 54
- simple delete profile
 - customizing 52, 55
- Single Sign On
 - automatic registration 17
 - exporting applications 18
 - manual registration 18
 - modifying application
 - properties 18
 - removing applications 18
- system configuration options
 - boot options 63
 - built-in device options 63
 - device configuration
 - options 63
 - port options 63
 - system configuration
 - options 63

T

- targeted theft, protecting
 - against 6
- token, Credential Manager 13
- TPM chip
 - enabling 69
 - initializing 70
- troubleshooting
 - Credential Manager 79
 - Device Access Manager 88
 - Embedded Security 82
 - miscellaneous 89

U

- unauthorized access,
 - preventing 6

V

- viewing
 - file options 61
- viewing settings 61
- virtual token 15
- virtual token, Credential Manager 13, 15

W

- Windows Logon
 - Credential Manager 16
 - password 9

