



HP ProtectTools

Getting Started

© Copyright 2012 Hewlett-Packard
Development Company, L.P.

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

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: August 2012

Document Part Number: 702113-001

Table of contents

1 Introduction to security	1
HP ProtectTools features	1
HP ProtectTools security product description and common use examples	2
Password Manager	3
Drive Encryption for HP ProtectTools (select models only)	3
Device Access Manager for HP ProtectTools (select models only)	3
Computrace for HP ProtectTools (formerly LoJack Pro) (purchased separately)	4
Achieving key security objectives	4
Protecting against targeted theft	5
Restricting access to sensitive data	5
Preventing unauthorized access from internal or external locations	5
Creating strong password policies	5
Additional security elements	6
Assigning security roles	6
Managing HP ProtectTools passwords	6
Creating a secure password	7
Backing up credentials and settings	7
2 Getting started	8
HP Client Security Setup Wizard	8
HP ProtectTools Security Manager Setup Wizard	9
HP Client Security Dashboard	9
3 Easy Setup Guide for Small Business	10
Getting started	10
Password Manager	10
Viewing and managing the saved authentications in Password Manager	11
Device Access Manager for HP ProtectTools	11
Drive Encryption for HP ProtectTools	12
4 HP ProtectTools Security Manager Administrative Console	13
Getting started	13
HP Client Security Setup Wizard	13
HP ProtectTools Security Manager Setup Wizard	14
HP Client Security Dashboard	14
Opening HP ProtectTools Administrative Console	15

Using Administrative Console	15
Configuring your system	16
Setting up authentication for your computer	16
Logon Policy	16
Session Policy	17
Settings	17
Managing users	17
Credentials	17
SpareKey	18
Fingerprints	18
Face	19
Smart card	19
Initializing the smart card	19
Registering the smart card	20
Configuring the smart card	20
Contactless card	21
Proximity card	21
Bluetooth	21
PIN	21
Applications	21
General tab	22
Applications tab	22
Data	22
Computer	22
5 HP ProtectTools Security Manager	23
Opening Security Manager	23
Using the Security Manager User Console	23
Your personal ID card	24
My Logons	24
Password Manager	24
For Web pages or programs where a logon has not yet been created	25
For Web pages or programs where a logon has already been created	25
Adding logons	26
Editing logons	27
Using the Password Manager Quick Links menu	27
Organizing logons into categories	27
Managing your logons	28
Assessing your password strength	28
Password Manager icon settings	29
Settings	29

Credential Manager	29
Changing your Windows password	30
Setting up your SpareKey	30
Enrolling your fingerprints	31
Enrolling scenes for face logon	31
Authentication	32
Dark mode	32
Learning	33
Deleting a scene	33
Advanced User Settings	33
Setting up a smart card	33
Initializing the smart card	33
Registering the smart card	34
Changing the smart card PIN	34
Contactless card	34
Proximity card	34
Bluetooth	34
PIN	35
Administration	35
Advanced	35
Setting your preferences	35
Backing up and restoring your data	36
6 Drive Encryption for HP ProtectTools (select models only)	38
Opening Drive Encryption	38
General tasks	39
Activating Drive Encryption for standard hard drives	39
Activating Drive Encryption for self-encrypting drives	39
Deactivating Drive Encryption	41
Logging in after Drive Encryption is activated	41
Protect your data by encrypting your hard drive	42
Advanced tasks	42
Managing Drive Encryption (administrator task)	42
Using Enhanced Security with TPM (select models only)	43
Encrypting or decrypting individual drive partitions (software encryption only)	43
Backup and recovery (administrator task)	43
Backing up encryption keys	43
Recovering access to an activated computer using backup keys	44
Performing an HP SpareKey Recovery	44
Displaying encryption status	45

7 Device Access Manager for HP ProtectTools (select models only)	46
Opening Device Access Manager	46
Setup Procedures	47
Configuring device access	47
Simple Configuration	47
Starting the background service	48
Device Class Configuration	48
Denying access to a user or group	49
Allowing access for a user or a group	50
Allowing access to a class of devices for one user of a group	50
Allowing access to a specific device for one user of a group	50
Removing settings for a user or a group	51
Resetting the configuration	51
JITA Configuration	51
Creating a JITA for a user or group	52
Creating an extendable JITA for a user or group	52
Disabling a JITA for a user or group	53
Advanced Settings	53
Device Administrators group	54
eSATA Device Support	54
Unmanaged Device Classes	54
8 Theft recovery (select models only)	56
9 Localized password exceptions	57
What to do when a password is rejected	57
Windows IMEs not supported at the Preboot Security level or the HP Drive Encryption level	57
Password changes using keyboard layout that is also supported	58
Special key handling	58
Glossary	60
Index	63

1 Introduction to security

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

Application	Features
HP ProtectTools Security Manager Administrative Console (for administrators)	<ul style="list-style-type: none">• Requires Microsoft Windows® administrator rights to access.• Provides access to modules that are configured by an administrator and not available to users.• Allows initial security setup and configures options or requirements for all users.
HP ProtectTools Security Manager User Console (for users)	<ul style="list-style-type: none">• Allows users to configure options provided by an administrator.• Allows administrators to provide users limited control of some HP ProtectTools modules.

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

HP ProtectTools software modules may be preinstalled, preloaded, or available for download from the HP website. For more information, go to <http://www.hp.com>.



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

HP ProtectTools features

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

Module	Key features
HP ProtectTools Security Manager Administrative Console	Administrators can perform the following functions: <ul style="list-style-type: none">• Use the Security Manager Setup Wizard to set up and configure levels of security and security logon methods.• Configure options hidden from users.• Activate Drive Encryption and configure user access.• Configure Device Access Manager policies and user access.• Use administrator tools to add and remove HP ProtectTools users and view user status.
HP ProtectTools Security Manager User Console	General users can perform the following functions: <ul style="list-style-type: none">• View settings for Encryption Status and Device Access Manager.• Activate Computrace for HP ProtectTools.• Configure Preferences and Backup and Restore options.

Module	Key features
Credential Manager	<p>General users can perform the following functions:</p> <ul style="list-style-type: none"> • Change user names and passwords. • Configure and change user credentials such as a Windows password, fingerprint, face images, smart card, proximity card, or contactless card.
Password Manager	<p>General users can perform the following functions:</p> <ul style="list-style-type: none"> • Organize, and set up user names and passwords. • Create stronger passwords for enhanced account security. Password Manager fills in and submits the information automatically. • Streamline the logon process with the Single Sign On feature, which automatically remembers and applies user credentials.
Drive Encryption for HP ProtectTools (select models only)	<ul style="list-style-type: none"> • Provides complete, full-volume hard drive encryption. • Forces pre-boot authentication in order to decrypt and access the data. • Offers the option to activate self-encrypting drives (select models only).
Device Access Manager for HP ProtectTools (select models only)	<ul style="list-style-type: none"> • Allows IT managers to control access to devices based on user profiles. • Prevents unauthorized users from removing data using external storage media, and from introducing viruses into the system from external media. • Allows administrators to disable access to communication devices for specific individuals or groups of users.
Theft Recovery (Computrace for HP ProtectTools, purchased separately)	<ul style="list-style-type: none"> • Requires separate purchase of tracking and tracing subscriptions to activate. • Provides secure asset tracking. • Monitors user activity, as well as hardware and software changes. • Remains active even if the hard drive is reformatted or replaced.

HP ProtectTools security product description and common use examples

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



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

Password Manager

Password Manager stores user names and passwords, and can be used to:

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

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

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

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

Drive Encryption for HP ProtectTools (select models only)

Drive Encryption is used to restrict access to the data on the entire computer hard drive or a secondary drive. Drive Encryption can also manage self-encrypting drives.

Example 1: A doctor wants to make sure only he can access any data on his computer hard drive. The doctor activates Drive Encryption, which requires pre-boot authentication before Windows login. Once set up, the hard drive cannot be accessed without a password before the operating system starts. The doctor could further enhance drive security by choosing to encrypt the data with the self-encrypting drive option.

Drive Encryption for HP ProtectTools does not allow access to the encrypted data even when the drive is removed, because they are both bound to the original system board.

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

Device Access Manager for HP ProtectTools (select models only)

Device Access Manager for HP ProtectTools allows an administrator to restrict and manage access to hardware. Device Access Manager for HP ProtectTools can be used to block unauthorized access to USB flash drives where data could be copied. It can also restrict access to CD/DVD drives, control

of USB devices, network connections, and so on. An example would be a situation where outside vendors need access to company computers but should not be able to copy the data to a USB drive.

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

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

Computrace for HP ProtectTools (formerly LoJack Pro) (purchased separately)

Computrace for HP ProtectTools (purchased separately) is a service that can track the location of a stolen computer whenever the user accesses the Internet. Computrace for HP ProtectTools can also help remotely manage and locate computers, as well as monitor computer usage and applications.

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

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

Achieving key security objectives

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

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

Protecting against targeted theft

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

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system.
 - Security Manager for HP ProtectTools—See [HP ProtectTools Security Manager on page 23](#).
 - Drive Encryption for HP ProtectTools—See [Drive Encryption for HP ProtectTools \(select models only\) on page 38](#).
- Encryption helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system.
- Computrace can track the computer's location after a theft.
 - Computrace for HP ProtectTools—See [Theft recovery \(select models only\) on page 56](#).

Restricting access to sensitive data

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

- Device Access Manager for HP ProtectTools allows IT managers to restrict access to communication devices so that sensitive information cannot be copied from the hard drive. See [Device Class Configuration on page 48](#).

Preventing unauthorized access from internal or external locations

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

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system.:
 - Security Manager for HP ProtectTools—See [HP ProtectTools Security Manager on page 23](#).
 - Drive Encryption for HP ProtectTools—See [Drive Encryption for HP ProtectTools \(select models only\) on page 38](#).
- Security Manager helps ensure that an unauthorized user cannot get passwords or access to password-protected applications. See [HP ProtectTools Security Manager on page 23](#).
- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writable devices so sensitive information cannot be copied from the hard drive. See [Device Access Manager for HP ProtectTools \(select models only\) on page 46](#).

Creating strong password policies

If a company policy goes into effect that requires the use of strong password policy for dozens of Web-based applications and databases, Security Manager provides a protected repository for passwords and Single Sign On convenience. See [HP ProtectTools Security Manager on page 23](#).

Additional security elements

Assigning security roles

In managing computer security (particularly for large organizations), one important practice is to divide responsibilities and rights among various types of administrators and users.

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

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

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

 **NOTE:** Many of the features in HP ProtectTools can be customized by the security officer in cooperation with HP. For more information, go to <http://www.hp.com>.

- IT administrator—Applies and manages the security features defined by the security officer. Can also enable and disable some features. For example, if the security officer has decided to deploy smart cards, the IT administrator can enable both password and smart card mode.
- User—Uses the security features. For example, if the security officer and IT administrator have enabled smart cards for the system, the user can set the smart card PIN and use the card for authentication.

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

Unauthorized users should not be granted administrative privileges.

Managing HP ProtectTools passwords

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

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

HP ProtectTools password	Set in the following module	Function
Windows logon password	Windows Control Panel or HP ProtectTools Security Manager	Can be used for manual logon and for authentication to access various Security Manager features.
Security Manager Backup and Recovery password	Security Manager, by individual user	Protects access to the Security Manager Backup and Recovery file.
Smart card PIN	Credential Manager	Can be used as multifactor authentication. Can be used as Windows authentication. Authenticates users of Drive Encryption, if the smart card is selected.

Creating a secure password

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

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

Backing up credentials and settings

You can back up credentials in the following ways:

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

2 Getting started

To configure settings for HP ProtectTools, use the HP Client Security Setup Wizard or the HP ProtectTools Security Manager Setup Wizard.

After you have completed the HP Client Security Setup Wizard, application status is displayed on the HP Client Security Dashboard.

HP Client Security Setup Wizard



NOTE: Administration of HP ProtectTools requires administrative privileges.

The HP Client Security Setup Wizard guides you through setting up the most commonly used features of Security Manager. If you have not completed the HP Client Security Setup Wizard previously, you can launch HP Client Security Setup Wizard in one of the following ways:

- ▲ From the Start screen, click or tap the **HP Client Security** app.

– or –

From the Windows desktop, click or tap the **HP ProtectTools** gadget.

Pages are displayed in the following order:

1. **Windows password**—Enter your Windows password.
This will protect your Windows account using strong authentication.
2. **SpareKey**—To enroll the SpareKey option, select three security questions.
3. **Enroll fingerprints**—If a fingerprint reader and the associated driver are installed, you can enroll fingerprints. You must select and register at least 2 fingerprints.
4. **Drive Encryption**—If Drive Encryption for HP ProtectTools is installed, you can activate encryption on the primary drive:

- Software encryption for a traditional hard drive
- Hardware encryption if a self-encrypting drive is detected.

You must save an encryption key on one or more of the following before encryption is enabled:



NOTE: If you cancel the wizard at this time, you will not be able to activate Windows and Drive Encryption authentication.

- **Removable media**, such as a USB flash drive with FAT 32 format.
 - This option is selected by default if a single removable device is detected before the Drive Encryption page is displayed.
 - If 2 or more removable devices are detected, select one of the drives displayed.
 - **SkyDrive**—This option is available if an Internet connection is detected.
A Windows® Live ID is required. Enter your ID and password, or sign up for one.
5. The Finish page displays a success notification, and you are prompted to reboot for Drive Encryption activation.

HP ProtectTools Security Manager Setup Wizard



NOTE: Administration of HP ProtectTools requires administrative privileges.

The HP ProtectTools Security Manager Setup Wizard guides you through setting up the features of Security Manager. Besides the settings found in the wizard, administrators can configure many additional security features through the Administrative Console. These settings apply to the computer and all users who share the computer.

To launch the HP ProtectTools Security Manager Setup Wizard:

- ▲ Click **Setup Wizard** in the left panel of the Administrative Console, and then follow the on-screen instructions until setup is complete.

Administrators can launch Administrative Console from HP ProtectTools Security Manager User Console. For more information, see [HP ProtectTools Security Manager Administrative Console on page 13](#).

Security Manager and its applications are available to all users who share this computer.

HP Client Security Dashboard

To open HP Client Security if you have previously completed the HP Client Security Setup Wizard:

- ▲ From the Start screen, type `hp` and then select **HP Client Security**.

The dashboard displays a quick overview of features and related status for each application.

- ▲ Click or tap an application row to display more information for the selected application:
 - The **Configure Now** button indicates an application not yet configured. Click or tap the button to open the application page to configure the application.
 - The **Settings** button indicates an application with an OK status. Click or tap the button to access the settings for the application.
 - The **User Console** is launched for a user configuration.
 - The **Administrative Console** is launched for a configuration requiring administrator privilege.
 - The **Status Dashboard** stays open after the User Console or the Administrative Console is launched, and once you have configured settings and closed the Console, the status is refreshed.

3 Easy Setup Guide for Small Business

This chapter is designed to demonstrate the basic steps to activate the most common and useful options within HP ProtectTools for Small Business. There are numerous tools and options available in this software that will allow you to fine-tune your preferences and set your access control. This Easy Setup Guide will focus on getting each module running with the least amount of setup effort and time. For additional information, just select the module you are interested in and click the ? or Help button in the upper right corner. This button will automatically provide information to help you with the currently displayed window.

Getting started

1. From the Windows desktop, open HP ProtectTools Security Manager by double-clicking the **HP ProtectTools** icon in the notification area located at the far right of the taskbar.
2. Enter your Windows password, or create a Windows password.
3. Complete the setup wizard.



NOTE: By default, HP ProtectTools Security Manager is set to Strong Authentication Policy.

This setting is designed to prevent unauthorized access while logged into Windows and should be used when high security is needed or if users are away from their systems frequently throughout the day. If you would like to change this setting, click the **Session Policy** tab, and make your selections.

To have HP ProtectTools Security Manager require authentication only once during the Windows login, follow this procedure.

1. From the Windows desktop, open HP ProtectTools Security Manager by double-clicking the **HP ProtectTools** icon in the notification area located at the far right of the taskbar.
2. In the left pane, click **Administration**, and then click **Administrative Console**.
3. In the left pane under **System**, select **Authentication** from the **Security** group.
4. Click the **Session Policy** tab, and then select the login combination requirements for the session. To reverse these selections, click **Restore Defaults**.
5. Click the **Apply** button when complete.

Password Manager

Passwords! We all have quite a number of them – especially if you regularly access websites or use applications that require you to log on. The normal user either uses the same password for every application and website, or gets really creative and promptly forgets which password goes with which application.

Password Manager can automatically remember your passwords or give you the ability to discern which sites to remember and which to omit. Once you sign on to the computer, Password Manager will provide your passwords or credentials for participating applications or websites.

When you access any application or website requiring credentials, Password Manager will automatically recognize the site, and will ask if you want the software to remember your information. If you want to exclude certain sites, you can decline the request.

To start saving web locations, user names, and passwords:

1. As an example, navigate to a participating website or application, and then click the Password Manager icon in the upper-left corner of the Web page to add the web authentication.
2. Name the link (optional) and enter a user name and password into Password Manager.



NOTE: The areas that Password Manager will use now and for subsequent visits are highlighted.

3. When complete, click the **OK** button.
4. Password Manager can also save your user name and passwords for network shares or mapped network drives.

Viewing and managing the saved authentications in Password Manager

Password Manager allows you to view, manage, back up, and launch your authentications from a central location. Password Manager also supports the launching of saved sites from Windows.

To open Password Manager, use one of the following two methods:

- Use the keyboard combination of **ctrl+Windows logo key+h** to open Password Manager, and then click **Open** to launch and authenticate the saved shortcut.
– or –
- Select the **Manage** tab in Password Manager to open HP ProtectTools Security Manager to edit the credentials.

Password Manager's **Edit** option allows you to view and modify the name, login name, and even reveal the passwords.

HP ProtectTools for Small Business allows all credentials and settings to be backed up and/or copied to another computer.

Device Access Manager for HP ProtectTools

Device Access Manager can be used to restrict the use of various internal and external storage devices so your data will remain secured on the hard drive and not walk out the door of your business. An example would be to allow a user access to your data but block them from copying it to a CD, personal music player, or USB memory device. Below is an easy way to set this up.

1. From the Windows desktop, open HP ProtectTools Security Manager User Console by double-clicking the **HP ProtectTools** icon in the notification area located at the far right of the taskbar.
2. In the left pane of HP ProtectTools Security Manager, click **Administration**, and then click **Administrative Console**.
3. Click **Device Access Manager**, and then click **Device Class Configuration**.
4. The next step is to select who will continue to have access while everyone else is blocked.
5. Select the hardware devices that you want to restrict, and then click the **Apply** button to finish the process.
6. Select **Add**, click **Advanced**, and then click **Find Now**.

7. Select the desired user, and then click **OK > OK > Apply**.
Your choice is displayed in the **Users/Groups** box.
8. Select the **Device Class** that the user will be using, select **Allow** or **Deny**, and then click **Apply**.

Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools is used to protect your data by encrypting the entire hard drive. The data on your hard drive will stay protected if your PC is ever stolen and/or if the hard drive is removed from the original computer and placed in a different computer.

An additional security benefit is that Drive Encryption requires you to properly authenticate using your user name and password before the operating system starts. This process is called pre-boot authentication.

To make it easy for you, multiple software modules synchronize passwords automatically, including Windows user accounts, domains, Drive Encryption for HP ProtectTools, Password Manager, and HP ProtectTools Security Manager.

Use the following simple steps to activate Drive Encryption for HP ProtectTools:

1. From the Windows desktop, open HP ProtectTools Security Manager by double-clicking the **HP ProtectTools** icon in the notification area located at the far right of the taskbar.
2. In the left pane, click **Administration**, and then click **Administrative Console**.
3. In the left pane, click **Setup Wizard**.
4. Select **Next** in the Welcome screen.
5. Enter your Windows password to start the activation wizard, and then click **Next**.
6. Skip SpareKey if it is not desired.
7. Check the **Drive Encryption** box, and then click **Next**.
8. Check the drive to encrypt, and then click **Next**.
9. The Drive Encryption configuration window requires a USB flash drive or other external device to store the encryption recovery key. Keep this recovery key safe and secure because it is used to recover data or access the drive if the pre-boot password is lost or fails.
10. Click **Next**, complete the process, and then click **Finish**. Remove the USB flash drive, and then reboot the computer when ready.
11. When the system starts, Drive Encryption will request your Windows password. Enter the password, and then click **OK**.

 **NOTE:** The computer may appear to run slowly while the drive is encrypting. Once totally encrypted, the performance will return to normal. As data on the drive is accessed, it is encrypted or decrypted as required by the administrator.

Drive Encryption authentication will “chain” through Windows login directly to the Windows desktop so that you will not need to enter your password twice.

4 HP ProtectTools Security Manager Administrative Console

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

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

Using the Administrative Console, the local administrator can perform the following tasks:

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

Getting started

To configure settings for HP ProtectTools, use the HP Client Security Setup Wizard or the HP ProtectTools Security Manager Setup Wizard.

After you have completed the HP Client Security Setup Wizard, application status is displayed on the HP Client Security Dashboard.

HP Client Security Setup Wizard

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

The HP Client Security Setup Wizard guides you through setting up the most commonly used features of Security Manager. If you have not completed the HP Client Security Setup Wizard previously, you can launch HP Client Security Setup Wizard in one of the following ways:

- ▲ From the Start screen, click or tap the **HP Client Security** app.

– or –

From the Windows desktop, click or tap the **HP ProtectTools** gadget.

Pages are displayed in the following order:

1. **Windows password**—Enter your Windows password.
This will protect your Windows account using strong authentication.
2. **SpareKey**—To enroll the SpareKey option, select three security questions.
3. **Enroll fingerprints**—If a fingerprint reader and the associated driver are installed, you can enroll fingerprints. You must select and register at least 2 fingerprints.

4. **Drive Encryption**—If Drive Encryption for HP ProtectTools is installed, you can activate encryption on the primary drive:

- Software encryption for a traditional hard drive
- Hardware encryption if a self-encrypting drive is detected.

You must save an encryption key on one or more of the following before encryption is enabled:

 **NOTE:** If you cancel the wizard at this time, you will not be able to activate Windows and Drive Encryption authentication.

- **Removable media**, such as a USB flash drive with FAT 32 format.
 - This option is selected by default if a single removable device is detected before the Drive Encryption page is displayed.
 - If 2 or more removable devices are detected, select one of the drives displayed.
 - **SkyDrive**—This option is available if an Internet connection is detected.
A Windows® Live ID is required. Enter your ID and password, or sign up for one.
5. The Finish page displays a success notification, and you are prompted to reboot for Drive Encryption activation.

HP ProtectTools Security Manager Setup Wizard

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

The HP ProtectTools Security Manager Setup Wizard guides you through setting up the features of Security Manager. Besides the settings found in the wizard, administrators can configure many additional security features through the Administrative Console. These settings apply to the computer and all users who share the computer.

To launch the HP ProtectTools Security Manager Setup Wizard:

- ▲ Click **Setup Wizard** in the left panel of the Administrative Console, and then follow the on-screen instructions until setup is complete.

Administrators can launch Administrative Console from HP ProtectTools Security Manager User Console. For more information, see [HP ProtectTools Security Manager Administrative Console on page 13](#).

Security Manager and its applications are available to all users who share this computer.

HP Client Security Dashboard

To open HP Client Security if you have previously completed the HP Client Security Setup Wizard:

- ▲ From the Start screen, type `hp` and then select **HP Client Security**.

The dashboard displays a quick overview of features and related status for each application.

- ▲ Click or tap an application row to display more information for the selected application:
 - The **Configure Now** button indicates an application not yet configured. Click or tap the button to open the application page to configure the application.
 - The **Settings** button indicates an application with an OK status. Click or tap the button to access the settings for the application.
 - The **User Console** is launched for a user configuration.

- The **Administrative Console** is launched for a configuration requiring administrator privilege.
- The **Status Dashboard** stays open after the User Console or the Administrative Console is launched, and once you have configured settings and closed the Console, the status is refreshed.

Opening HP ProtectTools Administrative Console

Use the HP ProtectTools Administrative Console for administrative tasks, such as setting system policies or configuring software. Access the Administrative Console by opening HP ProtectTools Security Manager:

1. From the Windows desktop, double-click the **HP ProtectTools** icon in the notification area, located at the far right of the taskbar.
 – or –
 From **Control Panel**, select **System and Security**, and then select **HP ProtectTools Security Manager**.
2. In the left panel of Security Manager User Console, click **Administration**, and then click **Administrative Console**.

Using Administrative Console

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

1. From the Windows desktop, double-click the **HP ProtectTools** icon in the notification area, located at the far right of the taskbar.
 – or –
 From **Control Panel**, select **System and Security**, and then select **HP ProtectTools Security Manager**.
2. In the left panel of Security Manager User Console, click **Administration**, and then click **Administrative Console**.

The Administrative console displays the following selections under Home in the left panel:

- **System**—Allows you to configure the following security features and authentication for users and devices.
 - **Security**
 - **Users**
 - **Credentials**
- **Applications**—Allows you to configure settings for HP ProtectTools Security Manager and for Security Manager applications.
- **Data**—allows you to configure settings for Drive Encryption (select models only).
- **Computer**—allows you to configure settings for Device Access Manager
- **Setup Wizard**—Guides you through setting up HP ProtectTools Security Manager.

- **About**—Displays information about HP ProtectTools Security Manager, such as the version number and copyright notice.
 - **Main area**—Displays application-specific screens.
- ?—Displays the Administrative Console Help. This icon is located at the top right of the window frame, next to the minimize and maximize icons.

Configuring your system

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

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

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

Setting up authentication for your computer

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

To set up authentication on your computer:

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

Logon Policy

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

1. In the left panel of Administrative Console, click **Security**, and then click **Authentication**.
2. On the **Logon Policy** tab, select a user category, such as Administrators or Standard users.
3. Click an authentication credential to display the edit dialog.
4. To require a combination of two authentication credentials, click the down arrow to select each credential, and then click **OK**.
5. To remove a credential, click the **X**, or right-click the credential, and then click **Delete**.
6. Click **Yes** on the configuration dialog.
7. To confirm whether users can log on, click **Check that HP ProtectTools can log on**.

8. To return to the original settings, click **Restore Defaults**.
9. Click **Apply**.

Session Policy

To define policies governing the credentials required to perform authentication during a Windows session:

1. In the left panel of Administrative Console, click **Security**, and then click **Authentication**.
2. On the **Session Policy** tab, select a user category, such as Administrators or Standard users.
3. Click an authentication credential to display the edit dialog.
4. To require a combination of two authentication credentials, click the down arrow to select each credential, and then click **OK**.
5. To remove a credential, click the **X**, or right-click the credential, and then click **Delete**.
6. Click **Yes** on the configuration dialog.
7. To confirm whether users can log on, click **Check that HP ProtectTools can log on**.
8. To return to the original settings, click **Restore Defaults**.
9. Click **Apply**.

Settings

To allow users of this computer to skip Windows logon if authentication was already performed at the BIOS level or at the Drive Encryption level:

1. In the left panel of Administrative Console, click **Security**, and then click **Settings**.
2. **Allow One Step logon**—Select the check box to enable One Step logon, or clear the check box to disable it.
3. Click **Apply**.

Managing users

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

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

To manage users, select from the following settings:

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

Credentials

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

SpareKey

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

1. Select the security questions that will be presented to users during their SpareKey enrollment.

You can specify up to three custom questions, or you can allow users to type their own passphrase.

2. To allow SpareKey recovery for Windows logon, select the check box.
3. Click **Apply**.

Fingerprints

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

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

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

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

- **Sensitivity**—Move the slider to adjust the sensitivity used by the fingerprint reader when you swipe your finger(s).

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

- **Advanced**—Select one of the following options to configure the fingerprint reader to conserve power and to enhance visual feedback:
 - **Optimized**—The fingerprint reader activates when needed. You may observe a slight delay when the reader is used for the first time.
 - **Conserve power**—The fingerprint reader is slower to respond, but the setting requires less power.
 - **Full power**—The fingerprint reader is always ready to be used, but this setting uses the most power.

Face

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

1. Click **Credentials**, and then click **Face**.
2. For more convenience, click the slider to move it to the left, or for more accuracy, click the slider to move it to the right.
 - **Convenience**—To make it easier for enrolled users to gain access in marginal situations, click the slider bar to move it to the **Convenience** position.
 - **Balance**—To provide a good compromise between security and usability, or if you have sensitive information or your computer is located in an area where unauthorized logon attempts can occur, click the slider bar to move it to the **Balance** position.
 - **Accuracy**—To make it more difficult for a user to gain access if enrolled scenes or current lighting conditions are below normal and less likely that a false acceptance can occur, click the slider bar to move it to the **Accuracy** position.
3. To return the settings to the original values, click **Restore Defaults**.
4. Click **Apply**.

Smart card

Administrators must initialize the smart card before it can be used for authentication. Most CSP and PKCS11 standard smart cards are supported in Windows.

Initializing the smart card

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

 **NOTE:** Smart card middleware must be installed.

1. Obtain and install middleware for the smart card being used (such as ActivClient 6.x for an ActivIdentity smart card).
2. Insert the smart card into the reader.
3. Initialize (format) the smart card.
 - a. Launch the smart card initialization tool, or it may be displayed when you insert the smart card into the reader.
 - b. Follow the on-screen instructions to set up a PIN.
 - c. Note the unlock code for future reference.
4. Create a key pair and certificate.
 - a. Launch **HP ProtectTools Administrative Console**.
 - b. Click **Credentials**, click **Smart Card**, and then click the **Administration** tab.

- c. Be sure that **Initialize the smart card** is selected.
- d. Enter your PIN, click **Apply**, and then follow the on-screen instructions.

After the smart card has been successfully initialized, you need to register the smart card.

Registering the smart card

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

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

Users can also register a smart card in Security Manager User Console. For more information, see the HP ProtectTools Security Manager software Help clicking the blue ? icon at the top right of the Smart card page.

Configuring the smart card

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

- **Settings**—Select the **Lock the computer upon smart card removal** check box to configure the computer to automatically lock when a smart card is removed, and then click **Apply**.



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

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



NOTE: Features that are not supported by your smart card or the associated middleware are not available.

- ▲ Click **Apply**.

Contactless card

A contactless card is a small plastic card containing a computer chip. If a contactless card reader is connected to the computer, if the associated driver from the manufacturer has been installed, and if a contactless card has been selected as an authentication credential, you can use your contactless card for authentication. The following types of contactless cards are supported by HP ProtectTools:

- Contactless HID iCLASS memory cards
- Contactless MiFare Classic 1k, 4k, and mini memory cards
- ▲ To set up your contactless card, place it very close to the reader, follow the on-screen instructions, and then click **Apply**.

Proximity card

A proximity card is a small plastic card containing a computer chip. If a proximity card reader is connected to the computer, if the associated driver from the manufacturer has been installed, and if a proximity card has been selected as an authentication credential, you can use a proximity card in conjunction with other credentials for additional security.

- ▲ To set up your proximity card, place it very close to the reader, and then click **Apply**.

Bluetooth

If the computer is equipped with Bluetooth® functionality, if Bluetooth has been selected as an authentication credential, and if a Bluetooth phone is paired with the computer, you can use your Bluetooth phone in conjunction with other credentials for additional security. Specify the Bluetooth settings:

- ▲ To allow silent authentication, select the check box, and then click **Apply**.

PIN

If PIN has been selected as an authentication credential, you can use a PIN in conjunction with other credentials for additional security. Specify the PIN settings:

1. Click the up or down arrow to select the minimal PIN length.
The maximum number of digits allowed is 8.
2. Click **Apply**.

Applications

The Settings page under Applications in the left panel of Administrative Console contains two tabs that allow you to customize the behavior of currently installed HP ProtectTools Security Manager applications.

- ▲ In the left panel of Administrative Console, under **Applications**, click **Settings**.

General tab

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

- **Do not automatically launch the Setup Wizard for administrators**—Select this option to prevent the wizard from automatically opening upon logon.
 - **Do not automatically launch the Getting Started Wizard for users**—Select this option to prevent user setup from automatically opening upon logon.
1. Select the check box next to a specific setting to enable it, or clear the check box to disable the setting.
 2. Click **Apply**.

Applications tab

Administrators can enable or disable the following applications:

- **Status**—Select the check box to enable all applications, or clear the check box to disable all applications.
 - **Password Manager**—Enables Password Manager for all users of the computer.
1. Select the check box next to a specific setting to enable it, or clear the check box to disable the setting.
 2. Click **Apply**.

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

Data

The Data section of the left panel of Administrative Console allows you to configure settings for the following application:

- **Drive Encryption**—Configure settings and display drive status. For more information, see the Drive Encryption software Help by clicking the blue ? icon at the top right of the Drive Encryption page.

Computer

The Computer section of the left panel of Administrative Console allows you to configure settings for the Device Access Manager application:

- Simple Configuration
- Device Class Configuration
- Just-in-Time-Authentication (JITA) Configuration
- Advanced settings

For more information, see the Device Access Manager software Help by clicking the blue ? icon at the top right of the Device Access Manager page.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager allows you to significantly increase the security of your computer. You can use preloaded Security Manager applications, as well as additional applications available for immediate download from the Web:

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

Opening Security Manager

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

- ▲ From the Windows desktop, double-click the **HP ProtectTools** icon in the notification area, located at the far right of the taskbar.

– or –

From **Control Panel**, select **System and Security**, and then select **HP ProtectTools Security Manager**.

Using the Security Manager User Console

The Security Manager User Console is the central location for easy access to Security Manager features, applications, and settings. The User Console displays the following components:

- **ID Card**—Displays the Windows user name and icon identifying the logged on user account.
- **Security Applications**—Displays an expanding menu of links for configuring the following categories of security:
 - **Home**—Manage passwords, set up your authentication credentials, or check the status of the security applications.
 - **Theft Recovery**—Computrace for HP ProtectTools (purchased separately)
- **My Logons**—Manage your authentication credentials with Password Manager and Credential Manager.
- **My Data**—Manage the security of your data with Drive Encryption.



NOTE: This item is not displayed if the application is not installed.

- **My Computer**—Manage the security of your computer with Device Access Manager.



NOTE: This item is not displayed if the application is not installed.

- **Administration**—Allows administrators to access the **Administrative Console** to manage security and users.
- **Advanced**—Displays commands for accessing additional features, including:
 - **Preferences**—Allows you to personalize Security Manager settings.
 - **Backup and Restore**—Allows you to back up or restore data.
 - **About**—Displays information about HP ProtectTools Security Manager, such as the version number and copyright notice.
- **Main area**—Displays application-specific screens.
- **?**—Displays the Security Manager User Console Help. This icon is located at the top right of the window frame, next to the minimize and maximize icons.

Your personal ID card

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

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

To change the displayed name:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. Click the ID card in the upper-left corner of the User Console.
3. Click the box displaying your Windows user name for this account, type the new name, and then click **Save**.

My Logons

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

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

Administrators can access information about available additional security applications by clicking **Administration**, and then clicking **Central Management** in the lower-left corner of the dashboard.

Password Manager

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

Password Manager offers the following options:

Manage tab

- Add, edit, or delete logons.
- Use Quick Links to launch your default browser and log on to any website or program, after it has been set up.
- Drag and drop to organize your Quick Links into categories.
- See at a glance whether any of your passwords are a security risk.

Password Strength tab

- Check the strength of individual passwords used for websites and applications, as well as the overall password strength.
- Password strength is illustrated by red, yellow, or green status indicators.

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

- ▲ Click the **Password Manager** icon to display a context menu where you can choose from the following options:
 - Add [somedomain.com] to Password Manager
 - Open Password Manager
 - Icon settings
 - Help

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

The following options are displayed on the context menu:

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

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

The following options are displayed on the context menu:

- **Fill in logon data**—Displays a Verify your identity page. If successfully authenticated, your logon data is entered in the logon fields automatically, and then the page is submitted (if submission was specified when the logon was created or last edited).
- **Edit Logon**—Allows you to edit your logon data for this website.
- **Add Logon**—Allows you to add an account to Password Manager.
- **Open Password Manager**—Launches Password Manager.
- **Help**—Displays the Security Manager Help.



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

Adding logons

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

To add a logon:

1. Open the logon screen for a website or program.
2. Click the arrow on the **Password Manager** icon, and then click one of the following, depending on whether the logon screen is for a website or a program:
 - For a website, click **Add [domain name] to Password Manager**.
 - For a program, click **Add this logon screen to Password Manager**.
3. Enter your logon data. Logon fields on the screen, and their corresponding fields on the dialog box, are identified with a bold orange border. You can also display this dialog box by clicking **Add Logon** from the **Password Manager Manage** tab, using the **ctrl+Windows logo key+h** hotkey, or swiping your finger(s).
 - a. To populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
 - b. To view the password for this logon, click **Show password**.
 - c. To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.
 - d. Click **OK** to select the authentication method that you wish to use (fingerprints, face, smart card, proximity card, contactless card, Bluetooth phone, PIN, or password), and then log on with the selected authentication method.

The plus sign is removed from the **Password Manager** icon to notify you that the logon has been created.
 - e. If Password Manager does not detect the logon fields, click **More fields**.
 - Select the check box for each field that is required for logon, or clear the check box for any fields that are not required for logon.
 - Click **Close**.

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

Editing logons

To edit a logon, follow these steps:

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

You can also display this dialog box by clicking **Edit for the desired logon** on the **Password Manager Manage** tab.
3. Edit your logon information.
 - To select a **Username** logon field with one of the preformatted choices, click the down arrow to the right of the field.
 - To select a **Password** logon field with one of the preformatted choices, click the down arrow to the right of the field.
 - To add additional fields from the screen to your logon, click **More fields**.
 - To view the password for this logon, click **Show password**.
 - To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.
4. Click **OK**.

Using the Password Manager Quick Links menu

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

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

To display the **Quick Links** menu:

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

Organizing logons into categories

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

To add a category:

1. From the Security Manager User Console, click **Password Manager**.
2. Click the **Manage** tab, and then click **Add Category**.
3. Enter a name for the category.
4. Click **OK**.

To add a logon to a category:

1. Place your mouse pointer over the desired logon.
2. Press and hold the left mouse button.
3. Drag the logon into the list of categories. Categories are highlighted as you move your mouse pointer over them.
4. Release the mouse button when the desired category is highlighted.

Your logons are not moved to the category, but only copied to the selected category. You can add the same logon to more than one category, and you can display all of your logons by clicking **All**.

Managing your logons

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

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

To manage your logons:

- ▲ From the Security Manager User Console, click **Password Manager**, and then click the **Manage** tab.
 - **Add a logon**—Click **Add Logon** and follow the on-screen instructions.
 - **Your logons**—Click an existing logon, select one of the following options, and then follow the on-screen instructions:
 - **Open**—Open a website or program for which you have an existing logon.
 - **Add**—Add a logon. For more information, see [Adding logons on page 26](#).
 - **Edit**—Edit a logon. For more information, see [Editing logons on page 27](#).
 - **Delete**—Delete a website or program for which you have an existing logon.
 - **Add Category**—Click **Add Category**, and then follow the on-screen instructions. For more information, see [Organizing logons into categories on page 27](#).

To add an additional logon for a website or program:

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

Assessing your password strength

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

Password Manager makes monitoring and improving your security easy with instant and automated analysis of the strength of each of the passwords used to log on to your websites and programs.

On the **Password Strength** tab, red, yellow, or green status indicators illustrate the strength of individual passwords used for websites and applications, as well as the overall password strength.

Password Manager icon settings

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

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

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

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

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

The Add Logon to Password Manager screen is displayed.
- Follow the on-screen instructions. For more information, see [Adding logons on page 26](#).
- The **Password Manager** icon is displayed whenever this website logon or program screen is opened.

Do not prompt to add logons for logon screens—Select the radio button.

2. To access additional Password Manager settings, double-click **Password Manager**, and then click **Settings** on the Security Manager User Console.

Settings

You can specify settings for personalizing Password Manager:

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

Credential Manager

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

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

- Password
- SpareKey
- Fingerprints
- Face
- Smart card
- Contactless Card
- Proximity Card
- Bluetooth
- PIN

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

Changing your Windows password

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

To change your Windows password, follow these steps:

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

Setting up your SpareKey

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

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

To set up your SpareKey:

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

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

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

Enrolling your fingerprints

If the administrator selected Fingerprints on the **Choose your credentials** screen and if your computer has a fingerprint reader built in or connected, the HP ProtectTools Security Manager Setup Wizard guides you through the process of setting up, or "enrolling," your fingerprints: You can also enroll your fingerprints on the Fingerprint page under **Credential Manager** in the Security Manager User Console.

1. On the Fingerprints page of the wizard, an outline of two hands is displayed. Fingers that are already enrolled are highlighted. Click a finger on the outline.



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

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



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

Enrolling scenes for face logon

If you choose face logon, and if a webcam is built in or connected to your computer, HP ProtectTools Security Manager Setup Wizard prompts you to enroll scenes. You can also enroll scenes on the Face logon page under **Credential Manager** in the Security Manager User Console.

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

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



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

To enroll a scene from the HP ProtectTools Security Manager Setup Wizard:

1. On the Face logon page of the wizard, click **Advanced**, and then configure additional options. For more information, see [Advanced User Settings on page 33](#).
2. Click **OK**.
3. Click **Start**, or if you have enrolled scenes previously, click **Enroll a new scene**.
4. During scene enrollment you can watch a demonstration by clicking **Play Video**.

If this is the initial enrollment, a dialog will appear asking if you want to see a demonstration video. Click **Yes** or **No**.

5. In low light, the software can brighten the screen automatically, or change the background lighting, click the **Light bulb** icon.

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

 **NOTE:** Be sure to look at your image, turning your head accordingly, while the scenes are being captured.

7. Click **Next**.

You can also enroll scenes from the Security Manager User Console:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. Under **My Logons**, click **Credential Manager**, and then click **Face**.
3. Click **Advanced** to configure additional options. For more information, see [Advanced User Settings on page 33](#).
4. Click **OK**.
5. Click **Start**, or if you have enrolled scenes previously, click **Enroll a new scene**.
6. If you are prompted to enter your Windows password, enter it, and then click **Next**.
7. During scene enrollment you can watch a demonstration by clicking **Play Video**.
If this is the initial enrollment, a dialog will appear asking if you want to see a demonstration video. Click **Yes** or **No**.
8. In low light, the software can brighten the screen automatically, or change the background lighting, click the **Light bulb** icon.
9. Click the **Camera** icon, and then follow the on-screen instructions to enroll your scene.

 **NOTE:** Be sure to look at your image, turning your head accordingly, while the scenes are being captured.

For more information, see the Face Recognition software Help by clicking the blue ? icon at the top right of the Face enrollment page.

Authentication

After you have enrolled one or more scenes, you can use your face for authentication when you log on to the computer or when you begin a new Windows session.

1. When the authentication screen is launched and the camera detects your face, you have 5 seconds to start the logon process. If your face is authenticated successfully, you can access the computer.
2. If face logon times out, Face Recognition pauses. Click the **Camera** icon to resume the authentication process.

 **NOTE:** If lighting is insufficient, and you are not able to log on using Face Recognition, you can enter your Windows password to log on to the computer.

3. Once you log on to the computer, if Face Recognition asks you to add additional scenes to enhance your ability to log on during future login sessions, click **Yes**.

Dark mode

If the lighting is too dark during the face logon process, the face logon screen background color switches automatically to a white screen to provide better illumination of the face.

To switch the face logon screen background color manually, click the **Light bulb** icon.

Learning

If face logon is unsuccessful but you enter your password successfully, you may be prompted to save a series of images to increase the chances of successful face logon in the future.

Deleting a scene

To delete a currently enrolled scene:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. Under **My Logons**, click **Credential Manager**, and then click **Face**.
3. Click the scene to be deleted, and then click the **Trash can** icon.
4. Click **OK** on the confirmation dialog.

Advanced User Settings

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. Under **My Logons**, click **Credential Manager**, and then click **Face**.
3. Click **Advanced** to configure the following options:
 - Other Settings** tab—Select the check box to enable one or more of the following options, or clear the check box to disable an option. These settings apply only to the current user.
 - **Play sound on face recognition events**—Plays a sound when face logon succeeds or fails.
 - **Prompt to update scenes when logon fails**—If face logon is unsuccessful but you enter your password successfully, you may be prompted to save a series of captured images to increase the chances of successful face logon in the future.
 - **Prompt to enroll a new scene when logon fails**—If face logon is unsuccessful but you enter your password successfully, you may be prompted to enroll a new scene to increase the chances of successful face logon in the future.
4. To return the settings to the original values, click **Restore Defaults**.
5. Click **OK**.

Setting up a smart card

If a smart card reader is built in or connected to your computer and if the administrator has enabled a smart card as an authentication credential and performed the steps described in the HP ProtectTools Administrative Console software Help, the HP ProtectTools Security Manager Setup Wizard prompts you to insert and set up a smart card. You can also set up your smart card on the Smart Card page under **Credential Manager** in the Security Manager User Console.



NOTE: An administrator must initialize the smart card before it can be used.

Initializing the smart card

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

Administrators can initialize the smart card using the manufacturer's software and HP ProtectTools Administrative Console. For more information, see the HP ProtectTools Administrative Console software Help.

Registering the smart card

After the smart card is initialized, users can register it in Security Manager:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. Click **Credential Manager**, and then click **Smart card**.
3. Be sure that **Set up** is selected.
4. Enter your Windows password and your PIN, and then click **Save**.

Administrators can also register the smart card in HP ProtectTools Administrative Console. For more information, see the HP ProtectTools Administrative Console software Help.

Changing the smart card PIN

To change your smart card PIN:

1. Insert a smart card that has been previously formatted and initialized.
2. Select **Change smart card PIN**.
3. Enter your old PIN, and then enter and confirm a new PIN.

Contactless card

A contactless card is a small plastic card containing a computer chip. If a contactless card reader is connected to the computer, if the administrator has installed the associated driver from the manufacturer, and if the administrator has enabled a contactless card as an authentication credential, you can use a contactless card as an authentication credential. The following types of contactless cards are supported by HP ProtectTools:

- Contactless HID iCLASS memory cards
- Contactless MiFare Classic 1k, 4k, and mini memory cards
- ▲ To set up your contactless card, place it very close to the reader, follow the on-screen instructions, and then click **Apply**.

Proximity card

A proximity card is a small plastic card containing a computer chip. If a proximity card reader is connected to the computer, if the administrator has installed the associated driver from the manufacturer, and if the administrator has enabled a proximity card as an authentication credential, you can use a proximity card in conjunction with other credentials for additional security.

- ▲ To set up your proximity card, place it very close to the reader, follow the on-screen instructions, and then click **Apply**.

Bluetooth

If the administrator has enabled Bluetooth as an authentication credential, you can set up a Bluetooth phone in conjunction with other credentials for additional security.



NOTE: Only Bluetooth phone devices are supported.

1. Be sure that Bluetooth functionality is enabled on the computer, and that the Bluetooth phone is set in discovery mode. To connect the phone, you may be required to type an automatically generated code on the Bluetooth device. Depending on the Bluetooth device configuration settings, a comparison of pairing codes between the computer and the phone may be required.
2. To enroll the phone, select it, and then click **Enroll**.
3. Click **OK** on the confirmation dialog.

PIN

If the administrator has enabled a PIN as an authentication credential, you can set up a PIN in conjunction with other credentials for additional security.

- ▲ To set up a new PIN, enter the PIN, and then enter it again to confirm it.

Administration

Administrators can access the Administrative Console and Central Management by clicking **Administration** and then selecting **Administrative Console** in the lower-left panel of the HP ProtectTools Security Manager User Console.

For more information, see the HP ProtectTools Administrative Console software Help.

Advanced

You can access the following options by clicking **Advanced** in the lower-left panel of the User Console:

- **Preferences**—Allows you to personalize settings for Security Manager.
- **Backup and Restore**—Allows you to back up and restore your Security Manager data.
- **About**—Displays version information about Security Manager

Setting your preferences

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

General tab

Appearance—Show icon in taskbar notification area

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

Fingerprint tab



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

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

To assign a Quick Action to one of the listed keys, click a **(Key) + Fingerprint** option, and then select one of the available tasks from the menu.
- **Fingerprint Scan Feedback**—Displayed only when a fingerprint reader is available. Use this setting to adjust the feedback that occurs when you swipe your fingerprint.
 - **Enable sound feedback**—Security Manager gives you audio feedback when a fingerprint has been swiped, playing different sounds for specific program events. You may assign new sounds to these events through the **Sounds** tab in the Sound setting in Windows Control Panel, or disable sound feedback by clearing this option.
 - **Show scan quality feedback**

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

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

Backing up and restoring your data

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

Backups can also be used to migrate from one computer to another, also called importing and exporting.



NOTE: Only Password Manager and Face Recognition information is backed up by this feature. Drive Encryption has an independent backup method. Device Access Manager and fingerprint authentication information is not backed up.

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

To back up your data:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. On the left panel of the User Console, click **Advanced**, and then click **Backup and Restore**.
3. Click **Back up data**.
4. Select the modules that you want to include in the backup. In most cases, you will select all of the modules.
5. Verify your identity.
6. Enter a name for the storage file. By default, the file is saved to your Documents folder. Click **Browse** to specify a different location.
7. Enter a password to protect the file.
8. Click **Finish**.

To restore your data:

1. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
2. On the left panel of the User Console, click **Advanced**, and then click **Backup and Restore**.
3. Click **Restore data**.
4. Select the previously created storage file. Enter the path in the field provided, or click **Browse**.
5. Enter the password used to protect the file.
6. Select the modules for which you want to restore data. In most cases, you will select all of the modules listed.
7. Verify your Windows password.
8. Click **Finish**.

6 Drive Encryption for HP ProtectTools (select models only)

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

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

The following tasks can be performed with Drive Encryption:

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



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

- Creating backup keys
- Recovering access to an encrypted computer using backup keys and HP SpareKey
- Enabling Drive Encryption pre-boot authentication using a password, registered fingerprint, or PIN for select smart cards

Opening Drive Encryption

Administrators can access Drive Encryption by opening HP ProtectTools Security Manager User Console.

1. From the Windows desktop, double-click the **HP ProtectTools** icon in the notification area, located at the far right of the taskbar.

– or –

From **Control Panel**, select **System and Security**, and then select **HP ProtectTools Security Manager**.

2. In the left panel of HP ProtectTools Security Manager User Console, select **Administration**, and then select **Administrative Console**.
3. In the left panel of HP ProtectTools Administrative Console, select **Drive Encryption**.

General tasks

Activating Drive Encryption for standard hard drives

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

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click **Setup Wizard**.
3. Select the **Drive Encryption** check box, and then click **Next**.
4. To back up the encryption key, connect an external device for recording this key. This key must be used to access the data if other methods fail.
5. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
6. Click **Next**.

 **NOTE:** You are prompted to restart the computer. After restart, the Drive Encryption pre-boot screen is displayed, requiring authentication before Windows will start.

Drive Encryption has been activated. Encryption of the selected drive partition(s) might take a number of hours, depending on the number and size of the partition(s).

See the HP ProtectTools Security Manager software Help for more information.

Activating Drive Encryption for self-encrypting drives

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

 **NOTE:** Hardware encryption is available only if ALL drives in your computer are self-encrypting drives meeting Trusted Computing Group's OPAL specification for self-encrypting drive management. In this case, the **Use hardware drive encryption** option is available, and either hardware or software encryption can be used.

If there is a mix of self-encrypting drives and standard hard drives, then the **Use hardware drive encryption** option is not available, and only software encryption can be used. For more information, see [Activating Drive Encryption for standard hard drives on page 39](#).

▲ Use the HP ProtectTools Security Manager Setup Wizard to activate Drive Encryption.

– or –

Software encryption

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click **Setup Wizard**.
3. Select the **Drive Encryption** check box, and then click **Next**.

 **NOTE:** If the **Use hardware drive encryption** option is available at the bottom of the screen, clear the check box.

4. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt, and then click **Next**.
5. To back up the encryption key, insert the storage device into the appropriate slot.
6. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
7. Click **Apply**.

 **NOTE:** The computer will restart.

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

Hardware encryption

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click **Setup Wizard**.
3. Select the **Drive Encryption** check box, and then click **Next**.
4. If the **Use hardware drive encryption** check box is available at the bottom of the screen, be sure that it is selected.

If the check box is cleared or if it is not available, software encryption is applied. For more information, see [Activating Drive Encryption for standard hard drives on page 39](#).

5. Under **Drives to be encrypted**, select the check box for the hard drive that you want to encrypt, and then click **Next**.

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

If more than one drive is shown, disk 0 will also be automatically selected and grayed out but the option to select further hard drives for hardware encryption is made available.

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

6. To back up the encryption key, insert the storage device into the appropriate slot.
7. Under **Back up Drive Encryption keys**, select the check box for the storage device where the encryption key will be saved.
8. Click **Apply**.

 **NOTE:** You are prompted to restart the computer. Drive Encryption pre-boot will be displayed, requiring authentication before Windows will start.

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

See the HP ProtectTools Security Manager software Help for more information.

Deactivating Drive Encryption

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

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click **Setup Wizard**.
3. Clear the **Drive Encryption** check box, and then click **Next**.

Drive Encryption deactivation begins.

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

If hardware encryption was used, the drive is instantly decrypted, and after a few minutes, Drive Encryption is deactivated.

Once Drive Encryption is deactivated, you will be prompted to shut down the computer, if hardware encrypted, or restart the computer, if software encrypted.

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 on at the Drive Encryption login screen:

 **NOTE:** When waking from Sleep or Standby, Drive Encryption pre-boot authentication is not displayed for software encryption or hardware encryption. Hardware encryption provides the **Disable Sleep Mode for Added Security** option, which prevents Sleep or Standby from occurring when enabled.

When waking from Hibernation, Drive Encryption pre-boot authentication is displayed for both software or hardware encryption.

 **NOTE:** If the Windows administrator has enabled BIOS Pre-boot Security in HP ProtectTools Security Manager and if One-Step Logon is enabled (by default), you can log on to the computer immediately after authenticating at BIOS Pre-boot, without needing to reauthenticate at the Drive Encryption login screen.

Single user logon:

- ▲ On the **Logon** page, enter your Windows password, smart card PIN, SpareKey, Face, or swipe a registered finger.

Multiple user logon:

1. On the **Select user to log on** page, select the user to log on from the drop-down list, and then click **Next**.
2. On the **Logon** page, enter your Windows password or smart card PIN, or swipe a registered finger.

 **NOTE:** The following smart cards are supported:

Supported smart cards

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)



NOTE: If the recovery key is used to log on at the Drive Encryption login screen, additional credentials are required at Windows logon to access user accounts.

Protect your data by encrypting your hard drive

It is highly recommended that you use the HP ProtectTools Security Manager Setup Wizard to protect your data by encrypting your hard drive. After activation any added hard drives or partitions created can be encrypted by following these steps:

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



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

– or –

- ▲ For hardware-encrypted drives, select additional drive(s) to be encrypted.

Advanced tasks

Managing Drive Encryption (administrator task)

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



NOTE: Only additional hard drives can be selected or deselected for hardware encryption on the Drive Encryption Settings page.

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

Software encryption

- Not encrypted
- Encrypted
- Encrypting
- Decrypting

Hardware encryption

- Encrypted
- Not encrypted (for additional drives)

Using Enhanced Security with TPM (select models only)

If the Trusted Platform Module (TPM) is activated and the Drive Encryption Enhanced Security with TPM functionality is selected, the Drive Encryption password is protected by the TPM security chip. If the hard drive is removed and installed in another computer, access to the drive is denied.

 **CAUTION:** TPM ownership cannot be shared with Windows TPM.msc.

 **NOTE:** Because the password is protected by the 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.

 **NOTE:** The TPM option must be enabled in BIOS Setup.

Encrypting or decrypting individual drive partitions (software encryption only)

Administrators can use the Drive Encryption Settings page to encrypt one or more hard drive partition(s) on the computer or decrypt any drive partition(s) that have already been encrypted.

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click the **+** icon to the left of **Drive Encryption** to display the available options.
3. Click **Settings**.
4. Under **Drive Status**, select or clear the check box next to each hard drive you want to encrypt or decrypt, and then click **Apply**.

 **NOTE:** When a partition is being encrypted or decrypted, a progress bar displays the percentage of partition encrypted and the time remaining to complete the process.

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

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

Backup and recovery (administrator task)

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

Backing up encryption keys

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

 **CAUTION:** Be sure to keep the storage device containing the backup key in a safe place, because if you forget your password, lose your smart card, or do not have a finger registered, this device provides your only access to the computer. The storage place should also be secure, because the storage device allows access to Windows.

 **NOTE:** To save the encryption key, you must use a USB storage device with the FAT32 or FAT16 format. A USB memory stick, Secure Digital (SD) Memory Card, or MultiMedia Card (MMC) may be used for backup.

1. Launch **HP ProtectTools Administrative Console**. For more information, see [Opening HP ProtectTools Administrative Console on page 15](#).
2. In the left panel, click the **+** icon to the left of **Drive Encryption** to display the available options.
3. Click **Backing up Encryption Keys**.
4. Insert the storage device being used to back up the encryption key.

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

5. Under **Drive**, select the check box for the device where you want to back up your encryption key.
6. Click **Backup Keys**.
7. Read the information on the page that is displayed, and then click **OK**. The encryption key is saved on the storage device you selected.

Recovering access to an activated computer using backup keys

Administrators can perform a recovery using the Drive Encryption key backed up to a removable storage device at activation or by selecting the **Backing up Drive Encryption Keys** option in Security Manager.

1. Insert the removable storage device that contains your backup key.
2. Turn on the computer.
3. When the Drive Encryption for HP ProtectTools login dialog box opens, click **Options**.
4. Click **Recovery**.
5. Enter the file path or name that contains your backup key, and then click **Recover**.

– or –

Click **Browse** to search for the required backup file, click **OK**, and then click **Recover**.

6. When the confirmation dialog box opens, click **OK**.

The Windows logon screen is displayed.

 **NOTE:** If the recovery key is used to log on at the Drive Encryption login screen, additional credentials are required at Windows logon to access user accounts. It is highly recommended that you reset your password after performing a recovery.

Performing an HP SpareKey Recovery

SpareKey recovery within Drive Encryption pre-boot requires you to answer security questions correctly before you can access the computer. For more information on setting up SpareKey Recovery, see the Security Manager software Help.

To perform an HP SpareKey Recovery if you forget your password:

1. Turn on the computer.
2. When the Drive Encryption for HP ProtectTools page is displayed, navigate to the user logon page.
3. Click **SpareKey**.

 **NOTE:** If your SpareKey has not been initialized in Security Manager, the **SpareKey** button is not available.

4. Type correct answers to the displayed questions, and then click **Logon**.
The Windows logon screen is displayed.

 **NOTE:** If SpareKey is used to log on at the Drive Encryption logon screen, additional credentials are required at Windows logon to access user accounts. It is highly recommended that you reset your password after performing a recovery.

Displaying encryption status

Users can display encryption status from HP ProtectTools Security Manager.

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

1. Launch **HP ProtectTools User Console**. For more information, see [Opening Security Manager on page 23](#).
2. Under **My Data**, click **Drive Encryption**.

In a software or hardware encryption scenario, the drive encryption status is displayed as one of the following:

- Enabled
- Disabled

In a software encryption scenario, the drive encryption status is displayed as one of the following for each hard drive or hard drive partition:

- Not encrypted
- Encrypted
- Encrypting
- Decrypting

In a hardware encryption scenario, the drive encryption status is displayed as one of the following

- Not encrypted
- Encrypted

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

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

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



NOTE: Some human interface/input devices, such as a mouse, keyboard, TouchPad, and fingerprint reader, are not controlled by Device Access Manager. For more information, see [Unmanaged Device Classes on page 54](#).

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

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

Opening Device Access Manager

1. Log on as an Administrator.
2. Launch **HP ProtectTools Security Manager** from **HP Client Security Dashboard**.

– or –

From the Windows desktop, double-click the **HP ProtectTools** icon in the notification area, located at the far right of the taskbar.

– or –

From **Control Panel**, select **System and Security**, and then select **HP ProtectTools Security Manager**.

3. In the left panel of HP ProtectTools Security Manager User Console, click **Administration**, and then select **Administrative Console**.
4. In the left panel of Administrative Console, click **Device Access Manager**.

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

Setup Procedures

Configuring device access

HP ProtectTools Device Access Manager offers four views:

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

Simple Configuration

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

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



NOTE: If Bluetooth devices are used as authentication credentials, Bluetooth device access should not be restricted in the Device Access Manager policy.

- All modem devices
- All PCMCIA/ExpressCard devices
- All 1394 devices

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

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

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

3. Click **Apply**.



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

4. Click **OK**.

Starting the background service

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

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

Administrators can also start or stop this service.

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

- Device Locking/Auditing service
- DAMDrv.sys driver

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

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

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

Device Class Configuration

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Denying access to a user or group

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

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



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

Allowing access for a user or a group

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

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click one of the following:
 - **Device class**
 - **All devices**
 - **Individual device**
3. Click **Add**.
The **Select Users or Groups** dialog box opens.
4. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
5. Click a user or a group to be added to the list of available users and groups, and then click **OK**.
6. Click **OK** again.
7. Click **Allow** to grant this user access.
8. Click **Apply**.

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

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

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

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

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

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **Device Class Configuration**.
2. In the device list, click the device class that you want to configure, and then navigate to the folder below that.
3. Under **User/Groups**, click **Allow** next to the group to be granted access.

4. Click **Deny** next to the group to be denied access.
5. Navigate to the specific device to which access is to be allowed for the user in the device list.
6. Click **Add**.
The **Select Users or Groups** dialog box opens.
7. Click **Advanced**, and then click **Find Now** to search for users or groups to add.
8. Click a user to be allowed access, and then click **OK**.
9. Click **Allow** to grant this user access.
10. Click **Apply**.

Removing settings for a user or a group

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

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

Resetting the configuration

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

 **NOTE:** The Advanced Settings page is not reset.

To reset the configuration settings to the factory values:

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

JITA Configuration

JITA Configuration allows the administrator to view and modify lists of users and groups that are allowed to access devices using just-in-time authentication (JITA).

JITA-enabled users will be able to access some devices for which policies created in the **Device Class Configuration** or **Simple Configuration** view have been restricted.

- **Scenario**—A Simple Configuration policy is configured to deny all non-Device Administrators access to the DVD/CD-ROM drive.
- **Result**—A JITA-enabled user who attempts to access the DVD/CD-ROM drive receives the same “access denied” message as a non-JITA-enabled user. Then a balloon message is displayed, asking if the user would like JITA access. If the balloon is clicked, the authenticate user dialog is displayed. When the user enters credentials successfully, access is granted to the DVD/CD-ROM drive.

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

The JITA period can also be extended, if configured to do so. In this scenario, 1 minute before the JITA period is about to expire, users can click the prompt to extend their access without having to re-authenticate.

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

JITA is available for the following device classes:

- DVD/CD-ROM drives
- Removable media

Creating a JITA for a user or group

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

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

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

Creating an extendable JITA for a user or group

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

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

6. Select the **Extendable** check box.
7. Click **Apply**.

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

Disabling a JITA for a user or group

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

1. In the left pane of HP ProtectTools Administrative Console, click **Device Access Manager**, and then click **JITA Configuration**.
2. From the device's drop-down menu, select either **removable media** or **DVD/CD-ROM drives**.
3. Select the user or group whose JITA you wish to disable.
4. Clear the **Enabled** check box.
5. Click **Apply**.

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

Advanced Settings

Advanced Settings provides the following functions:

- Management of the Device Administrators group
- Management of drive letters to which Device Access Manager never denies access.

The Device Administrators group is used to exclude trusted users (trusted in terms of device access) from the restrictions imposed by a Device Access Manager policy. Trusted users usually include System Administrators. See [Device Administrators group on page 54](#) for more information.

The **Advanced Settings** view also enables the administrator to configure a list of drive letters to which Device Access Manager will not restrict access for any user.

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

To start these services:

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

– or –

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

```
sc start fldlock
```

Press **enter**.

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

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

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

Device Administrators group

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

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

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

To add users to the Device Administrators group:

1. In the **Advanced Settings** view, click **+**.
2. Enter the user name of the trusted user.
3. Click **OK**.
4. Click **Apply**.

eSATA Device Support

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

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

Unmanaged Device Classes

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

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

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

8 Theft recovery (select models only)

Computrace for HP ProtectTools (purchased separately) allows you to remotely monitor, manage, and track your computer.

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

To activate Computrace for HP ProtectTools:

1. Connect to the Internet.
2. Open the Security Manager User Console. For more information, see [Opening Security Manager on page 23](#).
3. In the left pane of Security Manager, click **Theft Recovery**.
4. To launch the Computrace Activation Wizard, click **Get Started**.
5. Enter your contact information and your credit card payment information, or enter a prepurchased Product Key.

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

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

To log on to the Customer Center:

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

Using the Customer Center, you can:

- Monitor your computers.
- Protect your remote data.
- Report the theft of any computer protected by Computrace.
- ▲ Click **Learn More** for more information about Computrace for HP ProtectTools.

9 Localized password exceptions

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

What to do when a password is rejected

Passwords can be rejected for the following reasons:

- A user is using an IME that is not supported. This is a common issue with double-byte languages (Korean, Japanese, Chinese). To resolve this issue:
 1. Using **Control Panel**, add a supported keyboard layout (add US/English keyboards under Chinese Input Language).
 2. Set the supported keyboard for default input.
 3. Restart HP ProtectTools, and then enter the password again.
- A user is using a character that is not supported. To resolve this issue:
 1. Change the Windows password so that it uses only supported characters. For more information about unsupported characters, see the HP ProtectTools Administrative Console software help.
 2. Run the HP ProtectTools Security Manager Setup Wizard again, and then enter the new Windows password.

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

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

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

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

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

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

Password changes using keyboard layout that is also supported

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



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

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

Special key handling

- Chinese, Slovakian, Canadian French and Czech

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

- Korean

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

- Unsupported characters are listed in the following table:

Language	Windows	BIOS	Drive Encryption
Arabic	The ٠, ١, and ٢ keys generate two characters.	The ٠, ١, and ٢ keys generate one character.	The ٠, ١, and ٢ keys generate one character.
Canadian French	ç, è, à, and é with caps lock are Ç, È, À, and É in Windows.	ç, è, à, and é with caps lock are ç, è, à, and é in the BIOS Preboot Security.	ç, è, à, and é with caps lock are ç, è, à, and é in HP Drive Encryption.

Language	Windows	BIOS	Drive Encryption
Spanish	40a is not supported. It nevertheless works because the software converts it to c0a. However, because of subtle differences between the keyboard layouts, it is recommended that Spanish-speaking users change their Windows keyboard layout to 1040a (Spanish Variation) or 080a (Latin American).	n/a	n/a
US international	<ul style="list-style-type: none"> ◦ The j, ñ, ' , ¥, and × keys on the top row are rejected. ◦ The â, ®, and Þ keys on the second row are rejected. ◦ The á, ð, and ø keys on the third row are rejected. ◦ The æ key on the bottom row is rejected. 	n/a	n/a
Czech	<ul style="list-style-type: none"> ◦ The ě key is rejected. ◦ The ě key is rejected. ◦ The ů key is rejected. ◦ The é, í, and ž keys are rejected. ◦ The ě, ě, ě, and ě keys are rejected. 	n/a	n/a
Slovakian	The ž key is rejected.	<ul style="list-style-type: none"> ◦ The š, ś, and ș keys are rejected when typed, but they are accepted when entered with the soft keyboard. ◦ The † dead key generates two characters. 	n/a
Hungarian	The ž key is rejected.	The † key generates two characters.	n/a
Slovenian	The žž key is rejected in Windows, and the alt key generates a dead key in the BIOS.	ú, Ú, ů, Ů, š, Š, ś, Ś, š, and Š keys are rejected in the BIOS.	n/a
Japanese	When available, Microsoft Office 2007 IME is a better choice. Despite the IME name, it is actually keyboard layout 411, which is supported.	n/a	n/a

Glossary

activation

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

Administrative Console

A central location where administrators can access and manage the features and settings in HP ProtectTools.

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

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

background service

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

backup

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

biometric

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

certification authority (CA)

A service that issues the certificates required to run a public key infrastructure.

credentials

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

cryptographic service provider (CSP)

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

cryptography

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

decryption

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

device access control policy

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

device class

All devices of a particular type, such as drives.

domain

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

Drive Encryption

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

Drive Encryption logon screen

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

DriveLock

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

emergency recovery archive

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

encryption

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

Encryption File System (EFS)

A system that encrypts all files and subfolders within the selected folder.

fingerprint

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

group

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

HP SpareKey Recovery

The ability to access your computer by answering security questions correctly.

ID card

A Windows desktop gadget that serves to visually identify your desktop with your user name and chosen picture.

identity

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

JITA

Just-in-time authentication.

logon

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

network account

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

PIN

Personal identification number.

PKI

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

power-on authentication

A security feature that requires some form of authentication, such as a smart card, security chip, or password, when the computer is turned on.

reboot

The process of restarting the computer.

restore

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

revocation password

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

SATA device mode

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

scene

An image of an enrolled user to be used for authentication.

security logon method

The method used to log on to the computer.

Single Sign On

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

smart card

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

Trusted Platform Module (TPM) embedded security chip

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

TXT

Trusted Execution Technology.

user

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

Windows administrator

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

Windows Logon Security

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

Windows user account

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

Index

A

- access
 - controlling 46
 - preventing unauthorized 5
- activating
 - Drive Encryption for self-encrypting drives 39
 - Drive Encryption for standard hard drives 39
- Administrative Console
 - configuring 16
 - using 15
- Advanced Settings 53
- allowing access 50
- Applications 21
- Applications tab, settings 22
- authentication 16, 32

B

- background service 48
- backing up
 - data 36
 - encryption key 43
 - HP ProtectTools credentials 7
- Bluetooth 21, 34

C

- Computrace 56
- configuration
 - device class 48
 - resetting 51
 - simple 47
- configuring
 - Administrative Console 16
 - device access 47
- contactless card 21, 34
- controlling device access 46
- Credential Manager 29
- credentials 24
 - specifying 17

D

- dark mode 32
- data
 - backing up 36

- restoring 36
- restricting access to 5
- deactivating Drive Encryption 41
- decrypting
 - drives 38
 - hard drive partitions 43
- denying 49
- Device Access Manager for HP ProtectTools 46
 - easy setup 11
 - opening 46
- device class
 - allowing access for a user 50
 - unmanaged 54
- device class configuration
 - configuration 48
- device settings
 - face 19
 - fingerprint 18
 - smart card 20
 - SpareKey 18
- device, allowing access for a user 50
- Drive Encryption for HP ProtectTools 38, 42
 - activating 39
 - backup and recovery 43
 - deactivating 39
 - decrypting individual drives 42
 - easy setup 12
 - encrypting individual drives 42
 - logging in after Drive Encryption is activated 39
 - managing Drive Encryption 42

E

- Easy Setup Guide for Small Business 10
- encrypting
 - drives 38
 - hard drive 42
 - hard drive partitions 43
- encryption
 - hardware 39, 41, 45
 - software 39, 41, 43, 45

- encryption key
 - backing up 43
- encryption status, displaying 45
- enrolling
 - fingerprints 31
 - scenes 31
- eSATA 54

F

- face, settings 19
- features, HP ProtectTools 1
- fingerprints
 - enrolling 31
 - settings 18

G

- General tab, settings 22
- getting started 10, 47
- group
 - allowing access 50
 - denying access 49
 - removing 51

H

- hardware encryption 39, 40, 41, 45
- HP Client Security Dashboard 9, 14
- HP ProtectTools Administrative Console 9, 13, 14
 - opening 15
- HP ProtectTools features 1
- HP ProtectTools Security Manager 23
 - Backup and Recovery password 6
- HP ProtectTools Security Manager Setup Wizard 9, 14
- HP SpareKey Recovery 44

I

- ID card 24

- J**
- JITA
 - configuration 51
 - creating extendable for user or group 52
 - creating for user or group 52
 - disabling for user or group 53
- Just-in-time Authentication Configuration 51
- K**
- key security objectives 4
- L**
- learning 33
- Light bulb icon 32
- logging in to the computer 41
- logons
 - adding 26
 - categories 27
 - editing 27
 - managing 28
- M**
- managing
 - credentials 29
 - encrypting or decrypting drive partitions 43
 - passwords 22, 24, 25
 - users 17
- O**
- objectives, security 4
- opening
 - Device Access Manager for HP ProtectTools 46
 - HP ProtectTools Administrative Console 15
 - Security Manager 23
- opening Drive Encryption 38
- P**
- password
 - changes using different keyboard layouts 58
 - changing 30
 - exceptions 57
 - guidelines 7
 - HP ProtectTools 6
 - managing 6
 - policies 5
 - rejected 57
 - secure 7
 - strength 28
- Password Manager 22, 24, 25
 - easy setup 10
 - viewing and managing saved authentications 11
- PIN 35
- preferences, setting 35
- proximity card 21, 34
- Q**
- Quick Links
 - menu 27
- R**
- recovering
 - access using backup keys 44
- removing
 - access 51
- resetting 51
- restoring
 - data 36
 - HP ProtectTools credentials 7
- restricting
 - access to sensitive data 5
 - device access 46
- S**
- scenes
 - deleting 33
 - enrolling 31
- screen color 32
- security 6
 - key objectives 4
 - roles 6
- Security Manager, opening 23
- settings 17, 35
 - adding 22, 23
 - advanced user 33
 - applications 22, 23
 - General tab 22
 - icon 29
- Setup Wizard 9, 14
- Simple Configuration 47
- smart card 33
 - changing the PIN 34
 - configuring 20
 - initializing 19, 33
 - PIN 6
 - registering 20, 34
- software encryption 39, 41, 43, 45
- SpareKey
 - setting up 30
 - settings 18
- special key handling 58
- specify security settings 17
- T**
- theft recovery 56
- theft, protecting against 5
- TPM 43
- U**
- unauthorized access, preventing 5
- unmanaged device classes 54
- user
 - allowing access 50
 - denying access 49
 - removing 51
- User Console settings 23
- W**
- Windows Logon password 6
- wizard
 - HP ProtectTools Client Security Setup 8
 - HP ProtectTools Security Manager Setup 8
- wizard, HP ProtectTools Security Manager Setup 9, 14

