HP Client Security

Getting Started

First Edition: August 2013

Document Part Number: 735339-001

Table of contents

1 Introduction to HP Client Security Manager

HP Client Security allows you to protect your data, device, and identity, thereby increasing the security of your computer.

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

HP Client Security 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 Client Security software modules.

HP Client Security features

The following table details the key features of HP Client Security modules.

Module	Key features
HP Client Security Manager	Administrators can perform the following functions: • Protect your computer before Windows® starts • Protect your Windows account using strong authentication • Manage your logon and passwords for websites and applications • Easily change your Windows operating system password • Use fingerprints for extra security and convenience • Set up a smart card, contactless card, or proximity card for authentication • Use your Bluetooth phone as a method of identification • Set a PIN to expand your authentication choices • Configure logon and session policies • Back up and restore your program data • Add more applications, such as HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager, and HP Computrace General users can perform the following functions: • View settings for Encryption Status and Device Access Manager. • Activate Computrace. • Configure Preferences and Backup and Restore options.

Module	Key features
Password Manager	General users can perform the following functions: • Organize, and set up user names and passwords. • Create stronger passwords for enhanced account security for email and Web accounts. 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. • Mark an account as compromised, so that you will be alerted for other account(s) with similar credentials. • Import logon data from a supported browser.
HP Drive Encryption (select models only)	• 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).
HP Device Access Manager	• 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.
HP Trust Circles	• Provides file and document security. • Encrypts files placed in user-specified folders and protects them within a trust circle. • Allows files to be used and shared only by members in the trust circle.
Theft Recovery (Computrace, purchased separately)	• 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 Client Security product description and common use examples

Most of the HP Client 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 Client 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.
- Mark an account as compromised, so that you will be alerted for other account(s) with similar credentials.
- Import logon data from a supported browser.

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 employee 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 employee decides to organize all the Web links, company user names, and passwords within Password Manager. Once complete, the employee deploys Password Manager to the employees so they can work on the Web accounts and never know the login credentials that they are using.

HP Drive Encryption (select models only)

HP 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.

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.

HP Device Access Manager (select models only)

HP Device Access Manager allows an administrator to restrict and manage access to hardware. Device Access Manager 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 (purchased separately)

Computrace (purchased separately) is a service that can track the location of a stolen computer whenever the user accesses the Internet. Computrace 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

HP Client Security 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.
  - HP Client Security—See HP Client Security on page 12.
  - HP Drive Encryption—See HP Drive Encryption (select models only) on page 28.
- 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—See Theft recovery (select models only) on page 50.

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:

- HP Device Access Manager allows IT managers to restrict access to communication devices so that sensitive information cannot be copied from the hard drive. See System view on page 41.

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 Research and Development team, and to private information such as patient records or personal financial records. The following features help prevent unauthorized access:

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. (see HP Drive Encryption (select models only) on page 28.
- HP Client Security helps ensure that an unauthorized user cannot get passwords or access to password-protected applications. See HP Client Security on page 12.
- HP Device Access Manager allows IT managers to restrict access to writable devices so sensitive information cannot be copied from the hard drive. See HP Device Access Manager (select models only) on page 40.

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, Password Manager provides a protected repository for passwords and Single Sign On convenience. See Password Manager on page 18.

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 Client Security, 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 Client Security 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 Client Security passwords

Most of the HP Client Security 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 Client Security password	Set in the following module	Function
Windows logon password	Windows Control Panel or HP Client Security	Can be used for manual logon and for authentication to access various HP Client Security features.
HP Client Security Backup and Recovery password	HP Client Security, by individual user	Protects access to the HP Client Security 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 use the Backup and Recovery tool in HP Client Security as a central location from which you can back up and restore security credentials from some of the installed HP Client Security modules.

2 Getting started

To configure HP Client Security for use with your credentials, launch HP Client Security in one of the following ways. Once the wizard has been completed by a user, it cannot be launched again by that user.

1. From the Start or Apps screen, click or tap the **HP Client Security** app (Windows 8).

   – or –

   From the Windows Desktop, click or tap the **HP Client Security Gadget** (Windows 7).

   – or –

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

   – or –

   From the Windows desktop, click or tap the **HP Client Security** icon in the notification area, and then select **Open HP Client Security**.

2. The HP Client Security Setup wizard is launched with the Welcome page displayed.

3. Read the Welcome screen, verify your identity by typing your Windows password, and then click or tap **Next**.

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

4. On the HP SpareKey page, select three security questions. Enter an answer for each question, and then click **Next**. Custom questions are also allowed. For more information, see HP SpareKey—Password Recovery on page 14.

5. On the Fingerprints page, enroll at least the minimum number of required fingerprints, and then click or tap **Next**. For more information, see Fingerprints on page 12.

6. On the Drive Encryption page, activate encryption, back up the encryption key, and then click or tap **Next**. For more information, see HP Drive Encryption software Help.

   NOTE: This applies to a scenario where the user is an administrator, and HP Client Security Setup wizard has not been configured by an administrator previously.

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

   This page provides the status of features and credentials.

8. HP Client Security Setup wizard ensures the activation of Just In Time Authentication and File Sanitizer features. For more information, see the HP Device Access Manager software Help and the HP File Sanitizer software Help.

   NOTE: This applies to a scenario where the user is an administrator, and HP Client Security Setup wizard has not been configured by an administrator previously.

Opening HP Client Security

You can open the HP Client Security application in one of the following ways:

NOTE: HP Client Security Setup Wizard must be completed before the HP Client Security application can be launched.

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

  – or –

  From the Windows desktop, click or tap the **HP Client Security** Gadget (Windows 7).

  – or –

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

  – or –

  From the Windows desktop, click or tap the **HP Client Security** icon in the notification area, and then select **Open HP Client Security**.

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 Client Security for Small Business. Numerous tools and options in this software allow you to fine-tune your preferences and set your access control. The focus of this Easy Setup Guide is to get each module running with the least amount of setup effort and time. For additional information, select the module you are interested in, and then click the **?** or Help button in the upper-right corner. This button will automatically display information to help you with the currently displayed window.

Getting started

1. From the Windows desktop, open HP Client Security by double-clicking the **HP Client Security** 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 HP Client Security Setup.

To have HP Client Security require authentication only once during the Windows login, see Security Features on page 25.

Password Manager

Everyone has quite a number of passwords – 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 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.
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 the keyboard combination of Ctrl+Windows key+h to open Password Manager, and then click **Log in** to launch and authenticate the saved shortcut.

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

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

HP Device Access Manager

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.

1. Open **Device Access Manager** (see Opening Device Access Manager on page 40).

   Access for the current user is displayed.

2. To change access for users, groups or devices, click or tap **Change**. For more information, see System view on page 41.

HP Drive Encryption

HP Drive Encryption 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, authentication domains, HP Drive Encryption, Password Manager, and HP Client Security.

To set up HP Drive Encryption during initial setup with the HP Client Security Setup wizard, see Getting started on page 8.

4 HP Client Security

The HP Client Security Home page is the central location for easy access to HP Client Security features, applications, and settings. The Home page is divided into three sections:

- **DATA**—Provides access to applications used for managing data security.
- **DEVICE**—Provides access to applications used for managing device security.
- **IDENTITY**—Provides enrollment and management of authentication credentials.

Move the cursor over an application tile to display a description of the application.

HP Client Security may provide links to user and administrative settings at the bottom of a page. HP Client Security provides access to Advanced Settings and features by tapping or clicking the **Gear** (settings) icon.

Identity features, applications, and settings

The Identity features, applications, and settings provided by HP Client Security assist you in managing various aspects of your digital identity. Click or tap one of the following tiles on the HP Client Security Home page, and then enter your Windows password:

- **Fingerprints**—Enrolls and manages your fingerprint credential.
- **SpareKey**—Sets up and manages your HP SpareKey credential, which can be used to log on to your computer if other credentials have been lost or misplaced. It also allows you to reset your forgotten password.
- **Windows Password**—Provides easy access to change your Windows password.
- **Bluetooth Devices**—Allows you to enroll and manage your Bluetooth devices.
- **Cards**—Allows you to enroll and manage your smart cards, contactless cards, and proximity cards.
- **PIN**—Allows you to enroll and manage your PIN credential.
- **RSA SecurID**—Allows you to enroll and manage your RSA SecurID credential (if appropriate setup is in place).
- **Password Manager**—Allows you to manage passwords for your online accounts and applications.

Fingerprints

The HP Client Security Setup Wizard guides you through the process of setting up, or “enrolling,” your fingerprints.

You can also enroll or delete your fingerprints on the Fingerprints page, which you can access by clicking or tapping the **Fingerprints** icon on the HP Client Security Home page.

1. On the Fingerprints page, swipe a finger until it is successfully enrolled.

   The number of fingers required to be enrolled is indicated on the page. Index or middle fingers are preferable.

2. To delete previously enrolled fingerprints, click or tap **Delete**.
3. To enroll additional fingers, click or tap **Enroll an additional fingerprint**.
4. Click or tap **Save** before leaving the page.

⚠ **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.

- ▲ To access Fingerprints Administrative Settings, where administrators can specify the enrollment, accuracy, and other settings, click or tap **Administrative Settings** (requires administrative privileges).
- ▲ To access Fingerprints User Settings, where you can specify settings that govern the fingerprint recognition appearance and behavior, click or tap **User Settings**.

Fingerprints Administrative Settings

Administrators can specify the enrollment, accuracy, and other settings for a fingerprint reader. Administrative privileges are required.

- ▲ To access Administrative Settings for the fingerprint credential, click or tap **Administrative Settings** on the Fingerprints page.
- **User enrollment**—Choose the minimum and maximum number of fingerprints that a user is allowed to enroll.
- **Recognition**—Move the slider to adjust the sensitivity used by the fingerprint reader when you swipe your finger.

  If your fingerprint is not recognized consistently, you may need to select a lower recognition 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.

Fingerprints User Settings

On the Fingerprint User Settings page, you can specify settings that govern the fingerprint recognition appearance and behavior.

- ▲ To access User Settings for the fingerprint credential, click or tap **User Settings** on the Fingerprints page.
- **Enable sound feedback**—By default, HP Client Security gives you audio feedback when a fingerprint has been swiped, playing different sounds for specific program events. You can assign new sounds to these events through the Sounds tab in the Sound setting in Windows Control Panel, or to disable sound feedback, clear the check box.
- **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.

HP SpareKey—Password Recovery

The HP SpareKey allows you to gain access to your computer (on supported platforms) by answering three security questions.

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

To set up your HP SpareKey:

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

   You can select a question from a predefined list or write your own question.

2. Click or tap **Enroll**.

To delete your HP SpareKey:

▲ Click or tap **Delete your SpareKey**.

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

You can select different questions or change your answers on the SpareKey page, which is accessed from the Password Recovery tile on the HP Client Security Home page.

To access HP SpareKey Settings, where an administrator can specify settings relating to the HP SpareKey credential, click **Settings** (requires administrative privileges).

HP SpareKey Settings

On the HP SpareKey Settings page, you can specify settings that govern the behavior and use of the HP SpareKey credential.

▲ To launch the HP SpareKey Settings page, click or tap **Settings** on the HP SpareKey page (requires administrative privileges).

Administrators can select the following settings:

- Specify the questions that are presented to each user during HP SpareKey setup.
- Add up to three custom security questions to add to the list presented to users.
- Choose whether or not to allow users to write their own security questions.
- Specify which authentication environments (Windows or Power-on authentication) allow use of HP SpareKey for password recovery.

Windows password

HP Client Security makes changing your Windows password simpler and quicker than changing it through Windows Control Panel.

To change your Windows password:

1. From the HP Client Security Home page, click or tap **Windows 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 or tap **Change** to immediately change your current password to the new one that you entered.

Bluetooth Devices

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 or tap **Enroll**.

To access the Bluetooth Devices Settings on page 15 page where an administrator can specify settings for Bluetooth devices, click **Settings** (requires administrative privileges).

Bluetooth Devices Settings

Administrators can specify the following settings that govern the behavior and use of Bluetooth Device credentials:

Silent Authentication

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity**—Select the check box to allow users to use the Bluetooth credential for authentication without requiring user action, or clear the check box to disable this option.

Bluetooth Proximity

- **Lock computer when your enrolled Bluetooth device moves out of range of your computer**—Select the check box to lock the computer when a Bluetooth Device which was connected during login moves out of range, or clear the check box to disable this option.

NOTE: The Bluetooth module on your computer must support this capability to take advantage of this feature.

Cards

HP Client Security can support a number of different types of identification cards, which are small plastic cards containing a computer chip. These include smart cards, contactless cards, and proximity cards. If one of these cards, and the appropriate card reader, is connected to the computer, if the administrator has installed the associated driver from the manufacturer, and if the administrator has enabled the card as an authentication credential, you can use the card as an authentication credential.

For smart cards, the manufacturer should provide tools to install a security certificate and PIN management that HP Client Security uses in its security algorithm. The number and type of characters used as PIN may vary. An administrator must initialize the smart card before it can be used.

The following smart card formats are supported by HP Client Security:

- CSP
- PKCS11

The following types of contactless cards are supported by HP Client Security:

- Contactless HID iCLASS memory cards
- Contactless MiFare Classic 1k, 4k, and mini memory cards

The following proximity cards are supported by HP Client Security:

- HID Proximity Cards

To enroll a smart card:

1. Insert the card in an attached smart card reader.
2. When the card is recognized, enter the card's PIN, and then click or tap **Enroll**.

To change a smart card PIN:

1. Insert the card in an attached smart card reader.
2. When the card is recognized, enter the card's PIN, and then click or tap **Authenticate**.
3. Click or tap **Change PIN**, and then enter the new PIN.

To enroll a contactless or proximity card:

1. Place the card on or very near the appropriate reader.
2. When the card is recognized, click or tap **Enroll**.

To delete an enrolled card:

1. Present the card to the reader.
2. For smart cards only, enter the card's assigned PIN, and then click or tap **Authenticate**.
3. Click or tap **Delete**.

Once the card is enrolled, details about the card are displayed under **Enrolled Cards**. When a card is deleted, it is removed from the list.

To access Proximity, Contactless, and Smart Card Settings, where administrators can specify settings related to card credentials, click or tap **Settings** (requires administrative privileges).

Proximity, Contactless, and Smart Card Settings

To access settings for a card, click or tap the card in the list, and then click or tap the arrow that displays.

To change a smart card PIN:

1. Present the card to the reader
2. Enter the card's assigned PIN, and then click or tap **Continue**.
3. Enter and confirm the new PIN, and then click or tap **Continue**.

To initialize a smart card PIN:

1. Present the card to the reader
2. Enter the card's assigned PIN, and then click or tap **Continue**.
3. Enter and confirm the new PIN, and then click or tap **Continue**.
4. Click or tap **Yes** to confirm the initialization.

To clear card data:

1. Present the card to the reader
2. Enter the card's assigned PIN (for Smart cards only, and then click or tap **Continue**.
3. Click or tap **Yes** to confirm the deletion.

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, enter it again to confirm it, and then click or tap **Apply**.

To delete a PIN:

▲ Click or tap **Delete**, and then click or tap **Yes** to confirm.

To access PIN Settings, where administrators can specify settings related to PIN credentials, click or tap **Settings** (requires administrative privileges).

PIN Settings

On the PIN Settings page, you can specify the minimum and maximum acceptable lengths for the PIN credential.

RSA SecurID

If the administrator has enabled RSA as an authentication credential, and the following conditions are true, you can enroll or delete an RSA SecurID credential.

NOTE: Appropriate setup is required.

- The user must have been created on an RSA Server.
- The RSA SecurID token assigned to the user and the computer must have been joined to the RSA Server domain.
- SecurID software is installed on the computer.
- A connection is available to the properly configured RSA Server.

To enroll an RSA SecurID credential:

▲ Enter your RSA SecurID username and passcode (RSA SecurID Token code or PIN+Token code, depending on your environment), and then click or tap **Apply**.

Upon successful enrollment, a message is displayed, “Your RSA SecurID credential has been successfully enrolled,” and the Delete button is enabled.

To delete an RSA SecurID credential:

▲ Click **Delete**, and then select **Yes** to the popup dialog which asks “Are you sure you want to delete your RSA SecurID credential?”

Password Manager

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

NOTE: Because of the ever-changing structure of Web logon screens, Password Manager may not be able to support all websites at all times.

Password Manager offers the following options:

Password Manager page

- Click or tap an account to automatically launch a web page or application and log on.
- Use categories to organize your accounts.

Password Strength

- See at a glance whether any of your passwords are a security risk.
- When adding login data, check the strength of individual passwords used for websites and applications.
- 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 or tap 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 HP Client Security 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 placed in the logon fields, 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 HP Client Security Help.

NOTE: The administrator of this computer may have configured HP Client Security 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.

To add a logon:

1. Open the logon screen for a website or program.
2. Click or tap the **Password Manager** icon, and then click or tap one of the following, depending on whether the logon screen is for a website or a program:
   - For a website, click or tap **Add [domain name] to Password Manager**.
   - For a program, click or tap **Add this logon screen to Password Manager**.
3. Enter your logon data. Logon fields on the screen, and the corresponding fields on the dialog box, are identified with a bold orange border.
   a. To populate a logon field with one of the preformatted choices, click or tap the arrows to the right of the field.
   b. To view the password for this logon, click or tap **Show password**.
   c. To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.
   d. Click or tap **OK** to select the authentication method that you wish to use (fingerprints, 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 or tap **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 or tap **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:

1. Open the logon screen for a website or program.
2. To display a dialog box where you can edit your logon information, click or tap the **Password Manager** icon, and then click or tap **Edit Logon**.

   Logon fields on the screen, and the corresponding fields on the dialog box, are identified with a bold orange border.

   You can also edit account information from within the Password Manager page, by clicking or tapping the logon to display the editing options, and then selecting **Edit**.
3. Edit your logon information.
   - To edit the **Account name**, enter a new name into the field.
   - To add or edit a **Category** name, enter or modify the name in the **Category** field.
   - To select a **Username** logon field with one of the preformatted choices, click or tap the down arrow to the right of the field.

     Preformatted choices are available only when editing the logon from the Edit command on the Password Manager icon context menu.
   - To select a **Password** logon field with one of the preformatted choices, click or tap the down arrow to the right of the field.

     Preformatted choices are available only when editing the logon from the Edit command on the Password Manager icon context menu.
   - To add additional fields from the screen to your logon, click or tap **More fields**.
   - To view the password for this logon, click or tap the **Show password** icon.
   - To have the logon fields filled in, but not submitted, clear the **Automatically submit logon data** check box.
   - To mark this logon as having a compromised password, select the **This password is compromised** check box.

     After the changes are saved, all other logons sharing the same password will also be marked as compromised. You can then visit each affected account and change the passwords as necessary.
4. Click or tap **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 or double-tap a program or website logon from the **Password Manager Quick Links** menu, or from the Password Manager page within the HP Client Security, 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:

- ▲ Press the **Password Manager** hotkey combination (Ctrl+Windows key+h is the factory setting). To change the hotkey combination, from the HP Client Security Home page, click **Password Manager**, and then click or tap **Settings**.

Organizing logons into categories

Create one or more categories to keep your logons in order.

To assign a logon to a category:

1. From the HP Client Security Home page, click or tap **Password Manager**.
2. Click or tap an account entry, and then click or tap **Edit**.
3. In the **Category** field, enter a category name.
4. Click or tap **Save**.

To remove an account from a category:

1. From the HP Client Security Home page, click or tap **Password Manager**.
2. Click or tap an account entry, and then click or tap **Edit**.
3. In the **Category** field, erase the category name.
4. Click or tap **Save**.

To rename a category:

1. From the HP Client Security Home page, click or tap **Password Manager**.
2. Click or tap an account entry, and then click or tap **Edit**.
3. In the **Category** field, change the category name.
4. Click or tap **Save**.

Managing your logons

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

Your logons are listed on the Password Manager page.

To manage your logons:

1. From the HP Client Security Home page, click or tap **Password Manager**.
2. Click or tap an existing logon, and then select one of the following options and then follow the on-screen instructions:
   - **Edit**—Edit a logon. For more information, see Editing logons on page 20.
   - **Log in**—Log in to the selected account.
   - **Delete**—Delete the logon for the selected account.

To add an additional logon for a website or program:

1. Open the logon screen for the website or program.
2. Click or tap the **Password Manager** icon to display its context menu.
3. Click or tap **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.

As you are entering a password during the creation of a Password Manager logon for an account, a colored bar is shown beneath the password to indicate the strength of the password. The colors indicate the following values:

- **Red**—Weak
- **Yellow**—Fair
- **Green**—Strong

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 or tap the icon, and then click or tap **Icon Settings** to customize how Password Manager handles possible logon sites.
   - **Prompt to add logons for logon screens**—Click or tap 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.
   - **Do not prompt to add logons for logon screens**—Select the radio button.
2. To add a logon for a screen that has been previously excluded:
   a. Log on to the previously excluded website.
   b. To have Password Manager remember the password for this site, click or tap **Remember** on the popup dialog to save the password and create a logon for the screen.
3. To access additional Password Manager settings, click or tap the Password Manager icon, click or tap **Open Password Manager**, and then click or tap **Settings** on the Password Manager page.

Importing and exporting logons

On the HP Password Manager Import and Export page, you can import logons saved by web browsers on your computer. You can also import data from an HP Client Security backup file and export data to an HP Client Security backup file.

▲ To launch the Import and export page, click or tap **Import and export** on the Password Manager page.

To import passwords from a browser:

1. Click or tap the browser from which you want to import passwords (only installed browsers are displayed).
2. Clear the check box for any accounts for which you do not want to import passwords.
3. Click or tap **Import**.

Importing data from, or exporting data to, an HP Client Security backup file can be accomplished through the associated links (under **Other Options)** on the Import and export page.

NOTE: This feature imports and exports only Password Manager data. For information about backing up and restoring additional HP Client Security data, see Backing up and restoring your data on page 26.

To import data from an HP Client Security backup file:

1. From the HP Password Manager Import and Export page, click or tap **Import data from an HP Client Security backup file**.
2. Verify your identity.
3. Select the previously created backup file or enter the path in the field provided, and then click or tap **Browse**.
4. Enter the password used to protect the file, and then click or tap **Next**.
5. Click or tap **Restore**.

To export data to an HP Client Security backup file:

1. From the HP Password Manager Import and Export page, click or tap **Export data from an HP Client Security backup file**.
2. Verify your identity, and then click or tap **Next**.
3. Enter a name for the backup file. By default, the file is saved to your Documents folder. To specify a different location, click or tap **Browse**.
4. Enter and confirm a password to protect the file, and then click or tap **Save**.

Settings

You can specify settings for personalizing Password Manager:

- **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**.

- **Open Password Manager with Ctrl+Win+h**—The default hotkey that opens the **Password Manager Quick Links** menu is Ctrl+Windows key+h.

  To change the hotkey, click or tap this option, and then enter a new key combination. Combinations may include one or more of the following: ctrl, alt, or shift, and any alphabetic or numeric key.

  Combinations reserved for Windows or Windows applications cannot be used.

- To return the settings to the factory default values, click or tap **Restore defaults**.

Advanced Settings

Administrators can access the following options by selecting the **Gear** (settings) icon on the HP Client Security Home page.

- **Administrator Policies**—Allows you to configure logon and session policies for administrators.
- **Standard User Policies**—Allows you to configure logon and session policies for standard users.
- **Security Features**—Allows you to increase the security of your computer by protecting your Windows account using strong authentication and/or by enabling authentication before Windows startup.

- **Users**—Allows you to manage users and their credentials.
- **My Policies**—Allows you to review your authentication policies and enrollment status.
- **Backup and Restore**—Allows you to back up or restore HP Client Security data.
- **About HP Client Security**—Displays version information about HP Client Security.

Administrator Policies

You can configure logon and session policies for administrators of this computer. Logon policies set here govern the credentials required for a local administrator to log on to Windows. Session policies set here govern the credentials required for a local administrator to verify identity within a Windows session.

By default, all new or changed policies are enforced immediately after tapping or clicking **Apply**.

To add a new policy:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Administrator Policies**.
3. Click or tap **Add new policy**.
4. Click the down arrows to select primary and (optional) secondary credentials for the new policy, and then click or tap **Add**.
5. Click **Apply**.

To delay the enforcement of a new or changed policy:

1. Click or tap **Enforce this policy immediately**.
2. Select **Enforce this policy on the specific date**.
3. Enter a date or use the popup calendar to select a date when this policy should be enforced.
4. If desired, select when to remind users about the new policy.
5. Click **Apply**.

Standard User Policies

You can configure logon and session policies for standard users of this computer. Logon policies set here govern the credentials required for a standard user to log on to Windows. Session policies set here govern the credentials required for a standard user to verify identity within a Windows session.

By default, all new or changed policies are enforced immediately after tapping or clicking **Apply**.

To add a new policy:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Standard User Policies**.
3. Click or tap **Add new policy**.
4. Click the down arrows to select primary and (optional) secondary credentials for the new policy, and then click or tap **Add**.
5. Click **Apply**.

To delay the enforcement of a new or changed policy:

1. Click or tap **Enforce this policy immediately**.
2. Select **Enforce this policy on the specific date**.
3. Enter a date or use the popup calendar to select a date when this policy should be enforced.
4. If desired, select when to remind users about the new policy.
5. Click **Apply**.

Security Features

You can enable HP Client Security Features that help protect against unauthorized access to the computer.

To set up security features:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Security Features**.
3. Enable security features by selecting the check boxes, and then click or tap **Apply**. The more features you select, the more secure your computer is.

   These settings apply to all users.

   - **Windows Logon Security**—Protects your Windows accounts by requiring the use of HP Client Security credentials for access.
   - **Pre-Boot Security (Power-on authentication)**—Protects your computer before Windows startup. This selection is not available if the BIOS does not support it.
   - **Allow One Step logon**—This setting allows skipping Windows logon if authentication was previously performed at the Power–on authentication or Drive Encryption level.
4. Click or tap **Users**, and then click or tap the user's tile.

Users

You can monitor and manage this computer's HP Client Security users.

To add another Windows user to HP Client Security:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Users**.
3. Click or tap **Add another Windows user to HP Client Security**.
4. Enter the name of the user that you want to add, and then click or tap **OK**.
5. Enter the user's Windows password.

   A tile for the added user is displayed on the User page.

To delete a Windows user from HP Client Security:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Users**.

3. Click or tap the name of the user that you want to delete.
4. Click or tap **Delete User**, and then click or tap **Yes** to confirm.

To display a summary of logon and session policies enforced for a user:

▲ Click or tap **Users**, and then click or tap the user's tile.

My Policies

You can display your authentication policies and enrollment status. The My Policies page also provides links to the Administrators Policies and Standard User Policies pages.

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **My Policies**.

   Logon and session policies enforced for the currently logged on user are displayed.

The My Policies page also provides links to Administrator Policies on page 24 and Standard User Policies on page 24.

Backing up and restoring your data

It is recommended that you back up your HP Client Security 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 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 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 Client Security 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. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Administrator Policies**.
3. Click or tap **Backup and Restore**.
4. Click or tap **Backup**, and then verify your identity.
5. Select the module that you want to include in the backup, and then click or tap **Next**.
6. Enter a name for the storage file. By default, the file is saved to your Documents folder. To specify a different location, click or tap **Browse**.
7. Enter and confirm a password to protect the file.
8. Click or tap **Save**.

To restore your data:

1. From the HP Client Security Home page, click or tap the **Gear** icon.
2. On the Advanced Settings page, click or tap **Administrator Policies**.

3. Click or tap **Backup and Restore**.
4. Select **Restore**, and then verify your identify.
5. Select the previously created storage file. Enter the path in the field provided. To specify a different location, click or tap **Browse**.
6. Enter the password used to protect the file, and then click or tap **Next**.
7. Select the modules for which you want to restore data.
8. Click or tap **Restore**.

5 HP Drive Encryption (select models only)

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

The HP Client Security Home screen allows Windows administrators to activate Drive Encryption, back up the encryption key, and select or deselect drive(s) or partition(s) for encryption. For more information, see the HP Client Security software Help.

The following tasks can be performed with Drive Encryption:

- Selecting Drive Encryption settings:
  - 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 Client Security:

1. From the Start screen, click or tap the **HP Client Security** app (Windows 8).

   – or –

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

2. Click or tap the **Drive Encryption** icon.

General tasks

Activating Drive Encryption for standard hard drives

Standard hard drives are encrypted using software encryption. Follow these steps to encrypt a drive or a disk partition:

1. Launch **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. Select the check box for the drive or partition that you want to encrypt, and then click or tap **Backup Key**.

NOTE: For better security, select the **Disable sleep mode for increased security** check box. When you disable sleep mode, there is absolutely no risk that the credentials used to unlock the drive are stored in memory.

3. Select one or more of the backup options, and then click or tap **Backup**. For more information, see Backing up encryption keys on page 32.
4. You can continue to work while the encryption key is being backed up. Do not reboot your computer.

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).

For more information, see the HP Client Security software Help.

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. Hardware encryption is much faster than software encryption. However, you cannot choose which disk partitions to encrypt. The entire disk, including any disk partitions, is encrypted.

To encrypt specific partitions, then you must use software encryption. Be sure to clear the **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** check box.

Follow these steps to activate Drive Encryption for self-encrypting drives:

1. Launch **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. Select the check box for the drive that you want to encrypt, and then click or tap **Backup Key**.

NOTE: For better security, select the **Disable Sleep Mode for added security** check box. When you disable sleep mode, there is absolutely no risk that the credentials used to unlock the drive are stored in memory.

3. Select one or more of the backup options, and then click or tap **Backup**. For more information, see Backing up encryption keys on page 32.
4. You can continue to work while the encryption key is being backed up. Do not reboot your computer.

NOTE: For self-encrypting drives, you are prompted to shut down the computer.

For more information, see the HP Client Security software Help.

Deactivating Drive Encryption

1. Launch **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. Clear the check box for all encrypted drives, and then click or tap **Apply**.

   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 in 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 increased 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 Client Security and if One-Step Logon is enabled (by default), you can log in 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, or swipe a registered finger.

Multiple user logon:

1. On the **Select user to logon** page, select the user to logon from the drop-down list, and then click or tap **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

- Gemalto Cyberflex Access 64k V2c

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

Encrypting additional hard drives

It is highly recommended that you use HP Drive Encryption 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. Launch **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. 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 Drive Encryption to view and change the encryption status (Not Encrypted or Encrypted) of all of the hard drives on the computer.

- 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)

Encrypting or decrypting individual drive partitions (software encryption only)

Administrators can use Drive Encryption 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 **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. Under **Drive Status**, select or clear the check box next to each hard drive partition that you want to encrypt or decrypt, and then click or tap **Apply**.

NOTE: When a partition is being encrypted or decrypted, a progress bar displays the percentage of partition encrypted.

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.

Disk management

- **Nickname**—You can give your drives or partitions names for easier identification.
- **Disconnected drives**—Drive Encryption can track disks that are removed from the computer. A disk that is removed from the computer is automatically moved to the Disconnected list. If the disk is returned to the system, it will once again appear in the Connected list.
- If you no longer need to track or manage the disconnected drive, you can remove the disconnected drive from the Disconnected list.
- Drive Encryption remains activated until the check boxes for all connected drives are cleared, and the Disconnected list is empty.

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.

1. Launch **Drive Encryption**. For more information, see Opening Drive Encryption on page 28.
2. Select the check box for a drive, then click or tap **Backup Key**.
3. Under **Create HP Drive Encryption recovery key**, select one or more of the following options:
   - **Removable Storage**—Select the check box, and then select the storage device where the encryption key will be saved.
   - **SkyDrive**—Select the check box. You must be connected to the Internet. Log into Microsoft SkyDrive, and then click or tap **Yes**.

     NOTE: To use the HP Drive Encryption backup key that is stored on SkyDrive, you must download it from SkyDrive to a removable storage device, and then insert the storage device in this computer.
   - **TPM** (select models only)—Allows you to recover your data using your TPM password.

     CAUTION: If the TPM is cleared or the computer is damaged, you will lose access to the backup. If this method is selected, another backup method should also be selected.
4. Click or tap **Backup**.

   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 **Backup Key** option in Drive Encryption.

1. Insert the removable storage device that contains your backup key.
2. Turn on the computer.

3. When the HP Drive Encryption login dialog box opens, click or tap **Recovery**.
4. Enter the file path or name that contains your backup key, and then click or tap **Recovery**.
5. When the confirmation dialog box opens, click or tap **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 HP Client Security software Help.

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

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

NOTE: If your SpareKey has not been initialized in HP Client Security, 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 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.

6 HP File Sanitizer (select models only)

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

File Sanitizer cannot be used to sanitize or bleach the following types of drives:

- Solid-state drives (SSD), including RAID volumes that span an SSD device
- External drives connected by USB, Firewire, or eSATA interface

If a shred or bleach operation is attempted on an SSD, a warning message is displayed, and the operation is not performed.

Shredding

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

You can schedule a future shred time, or you can manually activate shredding by selecting the **File Sanitizer** icon on the HP Client Security Home screen or using the **File Sanitizer** icon on the Windows desktop. For more information, refer to Setting a shred schedule on page 36, Right-click shredding on page 38, or Manually starting a shred operation on page 38.

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

Free space bleaching

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

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

NOTE: Free space bleaching provides no additional security to shredded assets.

You can set a future free space bleaching time, or you can manually activate free space bleaching of previously shredded assets by selecting the **File Sanitizer** icon on the HP Client Security Home screen or using the **File Sanitizer** icon on the Windows desktop. For more information, refer to Setting a free space bleaching schedule on page 36, Manually starting free space bleaching on page 38, or Using the File Sanitizer icon on page 37.

Opening File Sanitizer

1. From the Start screen, click or tap the **HP Client Security** app (Windows 8).

   – or –

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

2. Under **Data**, click or tap **File Sanitizer**.

– or –

▲ Double-click or double-tap the **File Sanitizer** icon on the Windows desktop.

– or –

▲ Right-click or tap and hold the **File Sanitizer** icon on the Windows desktop, and then select **Open File Sanitizer**.

Setup procedures

Shredding—File Sanitizer securely deletes or shreds selected categories of assets.

1. Under **Shredding**, select the check box for each type of file to be shredded, or clear the check box if you do not want to shred those files.
   - **Recycle Bin**—Shreds all items inside the Recycle Bin.
   - **Temporary system files**—Shreds all files found in the system temporary folder. The following environment variables are searched in the following order, and the first path found is considered as the system folder:
     - TMP
     - TEMP
   - **Temporary Internet files**—Shreds copies of Web pages, images, and media that are saved by Web browsers for faster viewing.
   - **Cookies**—Shreds all files stored on a computer by Web sites to save preferences, such as login information.
2. To start shredding, click or tap **Shred**.

Bleaching—Writes random data to free space and prevents recovery of deleted items.

▲ To start bleaching, click or tap **Bleach**.

File Sanitizer Options—Select the check box to enable each of the following options, or clear the check box to disable an option:

- **Enable Desktop icon**—Displays the File Sanitizer icon on the Windows Desktop.
- **Enable right-click**—Allows you to right-click or tap and hold an asset, and then select **HP File Sanitizer – Shred**.
- **Ask for Windows password before manual shredding**—Requires authentication with Windows password before manually shredding an item.
- **Shred Cookies and Temporary Internet Files on browser close**—Shreds all selected Web-related assets, such as browser URL history, when you close a Web browser.

Setting a shred schedule

You can schedule a time to perform shredding automatically, or you can also shred assets manually at any time. For more information, refer to Setup procedures on page 35.

1. Open File Sanitizer, and then click or tap **Settings**.
2. To schedule a future time to shred selected assets, under **Shred Schedule**, select **Never**, **Once**, **Daily**, **Weekly**, or **Monthly**, and then select a day and time:
   a. Click or tap the hour, minute, or AM/PM field.
   b. Scroll until the desired value is displayed at the same level as the other fields.
   c. Click or tap the white space surrounding the time setting fields.
   d. Repeat for each field until the correct schedule has been selected.
3. The following four types of assets are listed:
   - **Recycle Bin**—Shreds all items inside the Recycle Bin.
   - **Temporary system files**—Shreds all files found in the system temporary folder. The following environment variables are searched in the following order, and the first path found is considered as the system folder:
     - TMP
     - TEMP
   - **Temporary Internet files**—Shreds copies of Web pages, images, and media that are saved by Web browsers for faster viewing.
   - **Cookies**—Shreds all files stored on a computer by Web sites to save preferences, such as login information.

   If checked, these assets are shredded at the scheduled time.
4. To select additional custom assets to be shredded:
   a. Under **Scheduled Shred List**, click or tap **Add folder**, and then navigate to the file or folder.
   b. Click or tap **Open**, and then click or tap **OK**.

   To remove an asset from the Scheduled Shred List, clear the check box for the asset.

Setting a free space bleaching schedule

Free space bleaching provides no additional security to shredded assets.

1. Open File Sanitizer, and then click or tap **Settings**.
2. To schedule a future time to bleach your hard drive, under **Bleach Schedule**, select **Never**, **Once**, **Daily**, **Weekly**, or **Monthly**, and then select a day and time.
   a. Click or tap the hour, minute, or AM/PM field.
   b. Scroll until the desired time is displayed in the same level as the other fields.
   c. Click or tap the white space surrounding the time setting fields.
   d. Repeat until the correct schedule has been selected.

NOTE: The free space bleaching operation can take a significant length of time. Be sure that your computer is connected to AC power. Although free space bleaching is performed in the background, increased processor usage may affect your computer's performance. Free space bleaching can be performed after hours or when the computer is not in use.

Protecting files from shredding

To protect files or folders from shredding:

1. Open File Sanitizer, and then click or tap **Settings**.
2. Under **Never Shred List**, click or tap **Add folder**, and then navigate to the file or folder.
3. Click or tap **Open**, and then click or tap **OK**.

NOTE: Files in this list are protected as long as they remain in the list.

To remove an asset from the exclusions list, clear the check box for the asset.

General tasks

Use File Sanitizer to perform the following tasks:

- **Use the File Sanitizer icon to initiate shredding**—Drag files to the **File Sanitizer** icon on the Windows desktop. For details, refer to Using the File Sanitizer icon on page 37.
- **Manually shred a specific asset or all selected assets**—Shred items at any time without waiting for a scheduled shred time. For details, refer to Right-click shredding on page 38 or Manually starting a shred operation on page 38.
- **Manually activate free space bleaching**—Activate free space bleaching at any time. For details, refer to Manually starting free space bleaching on page 38.
- **View the log files**—View shred and free space bleaching log files, which contain any errors or failures from the last shred or free space bleaching operation. For details, refer to Viewing the log files on page 39.

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

Using the File Sanitizer icon

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

When you start a shred operation manually, the standard shred list on the File Sanitizer view is shredded (see Setup procedures on page 35).

You can start a shred operation manually in one of the following ways:

1. Open File Sanitizer (see Opening File Sanitizer on page 35), and then click or tap **Shred**.
2. When the confirmation dialog box opens, be sure that the assets that you want to shred are checked, and then click or tap **OK**.

– or –

1. Right-click or tap and hold the **File Sanitizer** icon on the Windows desktop, and then click or tap **Shred Now**.
2. When the confirmation dialog box opens, be sure that the assets that you want to shred are checked, and then click or tap **Shred**.

Right-click shredding

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

If **Enable right-click shredding** has been selected on the File Sanitizer view, you can shred an asset as follows:

1. Navigate to the document or folder you want to shred.
2. Right-click or tap and hold the file or folder, and then select **HP File Sanitizer – Shred**.

Manually starting a shred operation

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

When you start a shred operation manually, the standard shred list on the File Sanitizer view is shredded (see Setup procedures on page 35).

You can start a shred operation manually in one of the following ways:

1. Open File Sanitizer (see Opening File Sanitizer on page 35), and then click or tap **Shred**.
2. When the confirmation dialog box opens, be sure that the assets that you want to shred are checked, and then click or tap **OK**.

– or –

1. Right-click or tap and hold the **File Sanitizer** icon on the Windows desktop, and then click or tap **Shred Now**.
2. When the confirmation dialog box opens, be sure that the assets that you want to shred are checked, and then click or tap **Shred**.

Manually starting free space bleaching

When you start a bleach operation manually, the standard shred list on the File Sanitizer view is bleached (see Setup procedures on page 35).

You can start a bleach operation manually in one of the following ways:

1. Open File Sanitizer (see Opening File Sanitizer on page 35), and then click or tap **Bleach**.
2. When the confirmation dialog box opens, click or tap **OK**.

– or –

1. Right-click or tap and hold the **File Sanitizer** icon on the Windows desktop, and then click or tap **Bleach Now**.
2. When the confirmation dialog box opens, click or tap **Bleach**.

Viewing the log files

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

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

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

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

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

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

7 HP Device Access Manager (select models only)

HP 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 43.

Windows® operating system administrators use HP 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.

HP Device Access Manager is automatically configured with the following settings during completion of the HP Client Security Setup Wizard:

- Just In Time Authentication (JITA) Removable Media is enabled for Administrators and Users.
- The device policy allows full access to other devices.

Opening Device Access Manager

1. From the Start screen, click or tap the **HP Client Security** app (Windows 8).

   – or –

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

2. Under **Device**, click or tap **Device Permissions**.

   - Standard users can view their current device access (see User view on page 41).
   - Administrators can view and make changes to the device access that is currently configured for the computer by clicking or tapping **Change**, and then entering the Administrator password (see System view on page 41).

User view

When **Device Permission**s is selected, the User view is displayed. Depending on the policy, standard users and administrators can view their own access for device classes or individual devices on this computer.

- **Current user**—The name of the user who is currently logged on is displayed.
- **Device Class**—The types of devices are displayed.
- **Access**—Your currently configured access to types of devices or specific devices is displayed.
- **Duration**—The time limit for your access to CD/DVD-ROM drives or removable disk drives is displayed.
- **Settings**—Administrators can change which drives have access controlled by Device Access Manager.

System view

On the System view, administrators can allow or deny access to devices on this computer for the Users group or the Administrators group.

▲ Administrators can access the System view by clicking or tapping **Change**, entering an Administrator password, and then selecting from the following options:

- **Device Access Manager**—To turn HP Device Access Manager with Just In Time Authentication on or off, click or tap **On** or **Off**.
- **Users and groups on this PC**—Displays the Users Group or Administrators group that are allowed or denied access to the selected device classes.
- **Device Class**—Displays the device classes and devices that are installed on the system or that may have been installed on the system previously. To expand the list, click the **+** icon. All devices connected to the computer are shown, and the Administrators and Users group are expanded to show their membership. To refresh the list of devices, click the round arrow (refresh) icon.
  - Protection is usually applied for a device class. If access is set to **Allow**, the selected user or group will be able to access any device in the device class.
  - Protection can also be applied to specific devices.
  - Configure Just In Time authentication (JITA), allowing selected users access to DVD/CD-ROM drives or removable disk drives by authenticating themselves. For more information, see JITA configuration on page 42.
  - Allow or deny access to other device classes, such as removable media (such as USB flash drives), serial and parallel ports, Bluetooth® devices, modem devices, PCMCIA/ExpressCard devices, 1394 devices, fingerprint reader, and smart card reader. If fingerprint reader and smart card reader are denied, they can be used as authentication credentials, but they cannot be used at Session policy level.

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

  - When you select a setting at the Group or Device Class level, and you are asked whether to apply the setting to the child objects:

    Yes—The setting will propagate.

No—The setting will not propagate.

- Some device classes, such as DVD and CD-ROM, may be further controlled by allowing or denying access separately for read and write operations.

NOTE: The Administrators group cannot be added to the User List.

- **Access**—Click or tap the down arrow, and then select one of the following access types to allow or deny access:
  - **Allow – Full Access**
  - **Allow – Read Only**
  - **Allow – JITA Required**—For more information, see JITA configuration on page 42.

    If this access type is selected, under **Duration**, click or tap the down arrow to select a time limit.
  - **Deny**
- **Duration**—Click or tap the down arrow to select a time limit for access to CD/DVD-ROM drives or removable disk drives (see JITA configuration on page 42).

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** view have been restricted.

The JITA period can be authorized for a set number of minutes or Unlimited. Unlimited users will have access to the device from the time they authenticate until the time they log off the system.

If the user is given a limited JITA period, one minute before the JITA period expires, the user is asked whether to extend the access. 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 Disk drives

Creating a JITA policy for a user or group

Administrators can allow users or groups to access devices using Just In Time Authentication (JITA).

1. Launch **Device Access Manager**, and then click or tap **Change**.
2. Select the user or group, and then under **Access** for either **Removable Disk drives** or **DVD/CD-ROM drives** click or tap the down arrow, and then select **Allow – JITA Required**.
3. Under **Duration**, click or tap the down arrow to select a time period for JITA access.

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

Disabling a JITA policy for a user or group

Administrators can disable user or group access to devices using Just In Time Authentication.

1. Launch **Device Access Manager**, and then click or tap **Change**.
2. Select the user or group, and then under **Access** for either **Removable Disk drives** or **DVD/CD-ROM drives** click or tap the down arrow, and then select **Deny**.

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

Settings

The **Settings** view allows administrators to view and change the drives which have access controlled by Device Access Manager.

NOTE: Device Access Manager must be enabled when the list of drive letters is configured (see System view on page 41).

Unmanaged device classes

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

- Input/output devices
  - CD-ROM
  - Disk drive
  - Floppy disk controller (FDC)
  - Hard disk controller (HDC)
  - Human interface device (HID) class
  - Infrared human interface devices
  - Mouse
  - Multi-port serial
  - Keyboard
  - Plug and play (PnP) printers
  - Printer
  - Printer upgrade
- Power
  - Advanced power management (APM) support
  - Battery
- Miscellaneous
  - Computer
  - Decoder
  - Display
  - Intel® unified display driver

- Legacard
- Media driver
- Medium changer
- Memory technology
- Monitor
- Multifunction
- Net client
- Net service
- Net trans
- Processor
- SCSI adapter
- Security accelerator
- Security devices
- System
- Unknown
- Volume
- Volume snapshot

8 HP Trust Circles

HP Trust Circles is a file and document security application, that combines folder file encryption with a convenient trusted-circle document-sharing capability. The application encrypts files placed in user-specified folders, protecting them within a trust circle. Once protected, the files can be used and shared only by members in the circle of trust. If a protected file is received by a non-member, the file remains encrypted, and the non-member cannot access the contents.

Opening Trust Circles

1. On the Start screen, click or tap the **HP Client Security** app.

   – or –

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

2. Under **Data**, click or tap **Trust Circles**.

Getting started

There are two ways to send email invitations and to reply to them:

- **Using Microsoft® Outlook**—Using Trust Circles with Microsoft Outlook automates the processing of any Trust Circle invitations and responses from other Trust Circle users.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)**—When you enter your name, email address, and password, Trust Circles uses your email service to send email invitations to the members selected to join your trust circle.

To set up your basic profile:

1. Enter your name and your email address, and then click or tap **Next**.

   The name is visible to any members who are invited to join your trust circle. The email address is used to send, receive, or reply to invitations.

2. Enter the password for the email account, and then click or tap **Next**.

   A test email is sent to ensure that the email settings are accurate.

   NOTE: The computer must be connected to a network.

3. In the **Trust Circle Name** field, enter a name for the trust circle, and then click or tap **Next**.
4. Add members and folders, and then click or tap **Next**. The trust circle is created with any folders that were selected and sends email invitations to any members that were selected. If, for any reason, an invitation cannot be sent, a notification is displayed. Members can be invited again at any time from the Trust Circle view by clicking **Your Trust Circles**, and then double-clicking or double-tapping the trust circle. For more information, see Trust Circles on page 46.

Trust Circles

You can create a trust circle during initial setup after you enter your email address, or on the Trust Circle view:

▲ From the Trust Circle view, click or tap **Create Trust Circle**, and then enter a name for the trust circle.

- To add members to the trust circle, click or tap the **M+** icon beside **Members**, and then follow the on-screen instructions.
- To add folders to the trust circle, click or tap the **+** icon beside **Folders**, and then follow the on-screen instructions.

Adding folders to a trust circle

Adding folders to a new trust circle:

- During the creation of a trust circle, you can add folders by clicking or tapping the **+** icon beside **Folders**, and then following the on-screen instructions.

  – or –

- In Windows Explorer, right-click or tap and hold a folder that is not currently part of a trust circle, select **Trust Circle**, and then select **Create Trust Circle from Folder**.

TIP: You can select one or more folders.

Adding folders to an existing Trust Circle:

- From the Trust Circle view, click **Your Trust Circles**, double-click or double-tap the existing trust circle to display the current folders, click or tap the **+** icon beside **Folders**, and then follow the on-screen instructions.

  – or –

- In Windows Explorer, right-click or tap and hold a folder that is not currently part of a trust circle, select **Trust Circle**, and then select **Add to existing Trust Circle from Folder**.

TIP: You can select one or more folders.

Once a folder has been added to a trust circle, Trust Circles encrypts the folder and its contents automatically. Once all of the files are encrypted, a notification is displayed. In addition, a green lock symbol is displayed on all encrypted folder icons and file icons within the folders indicating that they are fully protected.

Adding members to a trust circle

Three steps are required to add members to a trust circle:

1. **Invite**—First, the owner of the trust circle invites the member(s). The Invitation email can be sent to multiple users or distribution lists/groups.
2. **Accept**—The invitee receives the invitation and chooses whether to accept or decline. If the invitee accepts the invitation, an email response is sent to the inviter. If the invitation has been sent to a group, each member receives an invitation and chooses to accept or decline.
3. **Enroll**—The inviter has a final opportunity to decide whether to add the member to the trust circle. If the inviter decides to enroll the member, an email is sent to the invitee acknowledging

the response. The inviter and invitee can optionally verify the security of the Invitation process. A verification code is displayed for the invitee, which must be read to the inviter over the phone. Once the code has been verified, the inviter can send the final enrollment email.

Adding members to a new trust circle:

▲ During the creation of a trust circle, you can add members by clicking or tapping the **M+** icon beside **Members**, and then following the on-screen instructions.

- If you are using Outlook, select contacts from the Outlook address book, and then click **OK**
- If you are using another email service, either add new email addresses manually to Trust Circle, or you can have them retrieved from the email address registered on Trust Circle.

Adding members to an existing trust circle:

▲ From the Trust Circle view, click **Your Trust Circles**, double-click or double-tap the existing trust circle to display the current members, click or tap the **M+** icon beside **Members**, and then follow the on-screen instructions.

- If you are using Outlook, select contacts from the Outlook address book, and then click **OK**.
- If you are using another email service, either add new email addresses manually to Trust Circle, or you can have them retrieved from the email address registered on Trust Circle.

Adding files to a trust circle

You can add files into a trust circle in one of the following ways:

- Copy or move the file into an existing trust circle folder.

  – or –

- In Windows Explorer, right-click or tap and hold a file that is not currently encrypted, select **Trust Circle**, and then select **Encrypt**. You will be prompted to select the trust circle to which the file should be added.

TIP: You can select one or more files.

Encrypted folders

Any member of a trust circle can view and edit files that belong to that trust circle.

NOTE: Trust Circle Manager/Reader does not sync files between members.

Files must be shared by existing means, such as email, ftp, or cloud storage providers. Files copied to, moved to, or created within a trust circle folder are protected immediately.

Removing folders from a trust circle

Removing a folder from a trust circle decrypts the folder and all its contents and removing their protection.

- From the Trust Circle view, click or tap **Your Trust Circles**, double-click or double-tap the existing trust circle to display the current folders, and then click or tap the **trash can** icon beside that folder.

  – or –

- In Windows Explorer, right-click or tap and hold a folder that is currently part of a trust circle, select **Trust Circle**, and then select **Remove from trust circle**.

TIP: You can select one or more folders.

Removing a file from a trust circle

To remove a file from a trust circle, in Windows Explorer, right-click or tap and hold a file that is not currently encrypted, select **Trust Circle**, select **Decrypt File**.

Removing members from a trust circle

A member who has been fully enrolled cannot be removed from a trust circle. An alternative would be to create a new trust circle with all other members, move all files and folders to the new trust circle, and then delete the old trust circle. This will ensure that any new files that the member receives will not be accessible, but anything that has been shared previously will remain accessible to the member of the old trust circle.

If a member is not fully enrolled (either the member has been invited to join the trust circle or has not accepted the invitation to the trust circle), you can remove the member from the trust circle in one of the following ways:

- From the Trust Circle view, click or tap **Your Trust Circles**, and then double-click or double-tap the trust circle to show the current list of members. Click or tap the **trash can** icon beside the name of the member to be removed.
- From the Trust Circle view, click or tap **Members**, and then double-click or double-tap the member to show the trust circles in which they are members. Click or tap the **trash can** icon next to a trust circle to remove the member from that trust circle .

Deleting a trust circle

To delete a trust circle, ownership is required.

▲ From the Trust Circle view, click or tap **Your Trust Circles**, click or tap the **trash can** icon beside the trust circle to be deleted.

This removes the trust circle from the page and sends emails to all members of the trust circle informing them that the trust circle has been deleted. Any files or folders that were included in that trust circle are decrypted.

Setting preferences

From the Trust Circle view, click or tap **Preferences**. Three tabs are displayed

- **Email Settings**

Option	Description
Username	The username currently in use is displayed. To change it, enter a new username in the text box. Changes are saved automatically.
Email Address	The currently used email account is displayed. To change it, click or tap **Change Email Settings**, and then follow the on-screen instructions.

Option	Description
New Member Confirmation	Select from the following options: ◦ **Confirm Automatically**—After receiving acceptance from invitee(s), they are confirmed into the trust circle without any manual input, and a confirmation email is sent to the invitee(s). ◦ **Confirm Manually**—After receiving acceptance from invitees(s), manual input is required to enroll the new members into the trust circle, and then a confirmation email is sent to the invitee(s). ◦ **Require Verification**—After receiving acceptance from invitee(s), a verification code is required to fully enroll the invitee(s). The owner of the trust circle must contact the invitee(s) and acquire the verification code from them. After entering the correct code, the confirmation emails are sent.
Periodic Authentication	Periodic authentication requires the user to enter the Windows password after the specified timeout (recorded in minutes) and also while performing sensitive operations. This setting allows users the authentication to turn on or off.
Authentication Timeout	Select the specified timeout period (recorded in minutes) before authentication is required.
Don't show confirmation message	Select the check box to disable displaying confirmation messages, or clear the check box to display confirmation messages.
I'd like to help improve the HP Trust Circle through anonymous usage tracking	Select the check box to participate in the program, or clear the check box if you do not want to participate.

- **Backup/Restore**

Option	Description
Backup	Copies your Trust Circle Manager/Reader application data (settings and trust circles) to a backup file. In the event of a crash or system failure, you can use this file to restore your new installation of Trust Circles to the state saved in the file. **NOTE:** Only your Trust Circle application data is saved (trust circles, settings, and members). The actual files in the trust circle folders are not backed up. Those files should be backed up separately. To back up Trust Circle settings and user data: **1.** Click or tap **Backup**. **2.** Choose a filename and directory for the backup file, and then click or tap **Save**. **3.** Enter a password, confirm it, and then click or tap **OK**. This password will be required to restore this file.
Restore	Restores settings and trust circles from a backup file, usually after a system crash or migration to another computer. To restore Trust Circle Manager's settings and user data: **1.** Click or tap **Restore**. **2.** Navigate to the directory and filename of the backup file, and then click or tap **Open**. **3.** Enter the password that was set up while making the backup.

- **About**—The Trust Circle Manager/Reader software version is displayed. Links are displayed to allow you to upgrade Trust Circle Manager to the Pro version or to display the HP privacy statement.

9 Theft recovery (select models only)

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

Once activated, Computrace is configured from the Absolute Software Customer Center. From the Customer Center, the administrator can configure Computrace 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:

1. Connect to the Internet.
2. Open HP Client Security. For more information, see Opening HP Client Security on page 9.
3. 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.

10 Localized password exceptions

At the Power-on authentication level and the HP Drive Encryption level, password localization support is limited. For more information, see Windows IMEs not supported at the Power-on authentication level or the Drive Encryption level on page 51.

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. Launch HP Client Security, and then enter the Windows password.
- 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 Special key handling on page 52.
  2. Launch HP Client Security, and then enter the Windows password.

Windows IMEs not supported at the Power-on authentication level or the 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 Power-on authentication or Drive Encryption level. A Windows password cannot be entered with an IME at the Power-on authentication 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 Client Security can support the configuration.

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

Password changes using keyboard layout that is also supported

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

NOTE: Administrators can resolve this problem by using the HP Client Security Users page (accessed from the **Gear** icon on the Home page) to remove the user from HP Client Security, selecting the desired keyboard layout in the operating system, and then running the HP Client Security 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 Power-on authentication 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 Power-on authentication and HP Drive Encryption.

- Unsupported characters are listed in the following table:

Language	Windows	BIOS	Drive Encryption
Arabic	The ﻻ, ﻷ, and ﻹ keys generate two characters.	The ﻻ, ﻷ, and ﻹ keys generate one character.	The ﻻ, ﻷ, and ﻹ keys generate one character.
Canadian French	ç, è, à, and é with caps lock are Ç, È, À, and É in Windows.	ç, è, à, and é with caps lock are ç, è, à, and é in the Power-on authentication.	ç, è, à, and é with caps lock are ç, è, à, and é in HP Drive Encryption.
Spanish	40a is not supported. It nevertheless works because the software converts it to c0a. However, because of subtle differences between the keyboard layouts, it is recommended that Spanish-speaking users change their Windows keyboard layout to 1040a (Spanish Variation) or 080a (Latin American).	n/a	n/a

Language	Windows	BIOS	Drive Encryption
US international	◦ The ¡, ¤, ‘, ’, ¥, and × keys on the top row are rejected. ◦ The å, ®, and Þ keys on the second row are rejected. ◦ The á, ð, and ø keys on the third row are rejected. ◦ The æ key on the bottom row is rejected.	n/a	n/a
Czech	◦ The ğ key is rejected. ◦ The į key is rejected. ◦ The ų key is rejected. ◦ The ė, ı, and ż keys are rejected. ◦ The ģ, ķ, ļ, ņ, and ţ keys are rejected.	n/a	n/a
Slovakian	The ż key is rejected.	◦ The š, ś, and ş keys are rejected when typed, but they are accepted when entered with the soft keyboard. ◦ The ţ dead key generates two characters.	n/a
Hungarian	The ż key is rejected.	The ţ key generates two characters.	n/a
Slovenian	The żŻ key is rejected in Windows, and the alt key generates a dead key in the BIOS.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, and Š keys are rejected in the BIOS.	n/a
Japanese	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. Administrators can activate Drive Encryption with the HP Client Security Setup Wizard or HP Client Security. The activation process consists of activating the software, encrypting the drive, and creating the initial backup encryption key on a removable storage device.

administrator
See *Windows administrator*.

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

authentication
The process of verifying that you are the person you claim to be, through the use of credentials, including your Windows password, your fingerprint, a smart card, a contactless card, or a proximity card.

automatic shredding
Shredding that you schedule in File Sanitizer.

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.

Bluetooth
Technology that uses radio transmissions to enable Bluetooth-enabled computers, printers, mice, mobile phones, and other devices for wireless communication over a short distance.

connected device
A hardware device that is connected to a port on the computer.

contactless card
A plastic card containing a computer chip that can be used for authentication.

credential
A specific piece of information or a hardware device used to authenticate an individual user.

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

See Drive Encryption pre-boot authentication.

Drive Encryption pre-boot authentication
A login screen that is displayed before Windows starts. Users must enter their Windows user name and their password or smart card PIN, or swipe a registered finger. If one-step logon is selected, then entering the correct information at the Drive Encryption login screen allows direct access to Windows without having to log in again at the Windows login 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 HP Client Security.

free space bleaching
The writing of random data over deleted assets and unused space. This process reduces the existence of the deleted asset so that the original asset is more difficult to recover.

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

hardware encryption
The use of self-encrypting drives meeting Trusted Computing Group's OPAL specification for self-encrypting drive management to complete instantaneous encryption. Hardware encryption is instantaneous and might take only a few minutes, but software encryption might take several hours.

Home page
A central location where you can access and manage the features and settings in HP Client Security.

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

Just In Time Authentication
See the HP Device Access Manager software Help.

logon
An object within HP Client Security 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.

manual shred
Immediate shredding of an asset or selected assets, which bypasses a scheduled shred.

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

PIN
A personal identification number for an enrolled user to be used for authentication.

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.

proximity card
A plastic card containing a computer chip that can be used for authentication in conjunction with other credentials for additional security.

reboot
The process of restarting the computer.

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

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

shred
The execution of an algorithm that overwrites the data contained in an asset with meaningless data.

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

smart card
A hardware device that can be used with a PIN for authentication.

software encryption
The use of software to encrypt the hard drive sector by sector. This process is slower than hardware encryption

Trust Circle
Provides data containment by binding the data to a defined group of trusted users. This prevents data from falling into the wrong hands either accidentally or intentionally. Secured with CryptoMill’s Zero Overhead Key Management technology, data is cryptographically bound to a circle of trust. This prevents decryption of documents or other sensitive information outside of the trust circle

Trust Circle folder
Any folder protected by a trust circle.

Trust Circle Manager/Reader
The Trust Circle Reader can only accept invitations sent out by Trust Circle Manager users. However, Trust Circle Manager allows the creation of trust circles. Features include inviting someone via email to a trust circle and accepting trust circle invitations from others. Once a trust circle is established among peers, files protected by that trust circle can be shared securely.

Trusted Platform Module (TPM) 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.

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
A user who is authorized to log on to a network or to an individual computer.

Index