HP ProtectTools

Getting Started

First Edition: January 2007

Document Part Number: 419699-001

Table of contents

1 Introduction

HP ProtectTools Security Manager software provides security features that help protect against unauthorized access to the computer, networks, and critical data. Enhanced security functionality is provided by the following software modules:

- Smart Card Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Credential Manager for HP ProtectTools
- Device Access Manager for HP ProtectTools

The software modules available for your computer may vary depending on your model. For example, Embedded Security for HP ProtectTools requires that the Trusted Platform Module (TPM) embedded security chip (select models only) be installed on your computer, and Smart Card Security for HP ProtectTools requires an optional smart card and reader.

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

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

Accessing the HP ProtectTools Security Manager

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

▲ Select **Start > All Programs > HP ProtectTools Security Manager**.

NOTE After you have configured the Credential Manager module, you can also open HP ProtectTools by logging on to Credential Manager directly from the Windows logon screen. For more information, refer to “Logging on to Windows with Credential Manager,” in Chapter 6 "Credential Manager for HP ProtectTools."

Understanding security roles

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

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

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

- Security officer—Defines the security level for the company or network and determines the security features to deploy, such as smart cards, biometric readers, or USB tokens.

NOTE Many of the features in HP ProtectTools can be customized by the security officer in cooperation with HP. For more information, visit 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 smart card BIOS security 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.

Managing HP ProtectTools passwords

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

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

HP ProtectTools password	Set in this HP ProtectTools module	Function
Computer Setup setup password **NOTE** Also known as BIOS administrator, f10 Setup, or Security Setup password	BIOS Configuration, by IT administrator	Protects access to the Computer Setup utility.
Power-on password	BIOS Configuration	Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
Smart card administrator password **NOTE** Also known as BIOS administrator card password	Smart Card Security, by IT administrator	Used for smart card power-on (BIOS) authentication. Allows access to the Computer Setup utility and the computer contents when the computer is turned on, restarted, or restored from hibernation. It also allows for creating recovery files to restore user or administrator cards.
Smart card user password **NOTE** Also known as BIOS user card password	Smart Card Security	Used for smart card power-on (BIOS) authentication. Allows access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
Smart card PIN	Smart Card Security	Protects access to the smart card contents and authenticates users of the smart card. When used for power-on authentication, the smart card PIN also protects access to the Computer Setup utility and to the computer contents.
Smart card recovery file password	Smart Card Security	Protects access to the recovery file that contains the BIOS passwords.
Java™ Card PIN	Java Card Security	Protects access to the Java Card contents and authenticates users of the Java Card. When used for power-on authentication, the Java Card PIN also protects access to the Computer Setup utility and to the computer contents.
Basic User Key password **NOTE** Also known as: Embedded Security password	Embedded Security	Used to access Embedded Security features, such as secure e-mail, file, and folder encryption. When used for power-on authentication, also protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.

HP ProtectTools password	Set in this HP ProtectTools module	Function
Emergency Recovery Token password **NOTE** Also known as: Emergency Recovery Token Key password	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the embedded security chip.
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.
Credential Manager logon password	Credential Manager	This password offers 2 options: • It can be used in a separate logon to access Credential Manager after logging on to Windows. • It can be used in place of the Windows logon process, allowing access to Windows and Credential Manager simultaneously.
Credential Manager recovery file password	Credential Manager, by IT administrator	Protects access to the Credential Manager recovery file.
Windows logon password	Windows Control Panel	Can be used in manual logon or saved on the smart card.

Creating a secure password

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

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

2 Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools manages the smart card setup and configuration for computers equipped with an optional smart card reader.

With Smart Card Security, you can

- Access smart card security features.
- Initialize a smart card so that it can be used with other HP ProtectTools modules, such as Credential Manager for HP ProtectTools.
- Work with the Computer Setup utility to enable smart card authentication in a power-on environment, and to configure separate smart cards for an administrator and a user. This requires a user to insert the smart card and optionally enter a PIN prior to allowing the operating system to load.
- Set and change the password used to authenticate users of the smart card.
- Back up and restore smart card BIOS passwords stored on the smart card.

Initializing the smart card

You must initialize the smart card before using it.

To initialize the smart card:

1. Insert the smart card into the reader.
2. Select **Start > All Programs > HP ProtectTools Security Manager**.
3. In the left pane, click **Smart Card Security**, and then click **Smart Card**.
4. In the right pane, click **Initialize**.
5. Type your name in the first box in the **Initialize the smart card** dialog box.
6. Set and confirm the smart card PIN in the appropriate boxes. The PIN must be between 4 and 8 numeric characters.

   CAUTION To avoid losing access to the computer, do not forget the smart card PIN. If you forget your smart card PIN, it may be impossible to operate the computer. The smart card will be locked and made unusable unless the smart card PIN is entered correctly within 5 attempts. The count for these attempts resets after the correct PIN is entered.

7. Click **OK** to complete the initialization.

Smart card BIOS security mode

When enabled, smart card BIOS security mode requires you to use a smart card to start the computer.

The process of enabling smart card BIOS security mode involves the following steps:

1. Enable Smart Card Power-on Authentication Support in BIOS Configuration. Refer to "Enabling and disabling smart card or Java Card power-on authentication support," in Chapter 5, "BIOS Configuration for HP ProtectTools."

   

   NOTE Enabling this setting allows you to use a smart card for power-on authentication. The smart card BIOS security mode features are unavailable until you enable smart card power-on authentication support.

2. Enable smart card BIOS security mode in Smart Card Security. Refer to "Enabling smart card BIOS security mode and setting the smart card administrator password," later in this chapter.

3. Set the smart card administrator password.

   

   NOTE The smart card administrator password is set as part of the process of enabling smart card BIOS security mode.

The smart card administrator password is not the same as the Computer Setup setup password. The smart card administrator password links the smart card to the computer for identification purposes, and also allows you to do the following:

- Access Computer Setup or the contents of the computer when the computer is turned on.
- Create new administrator and user smart cards.
- Create a recovery file to restore either a user or administrator smart card.

Enabling smart card BIOS security mode and setting the smart card administrator password

To enable smart card BIOS security mode and set the smart card administrator password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **BIOS**.
3. In the right pane, under BIOS Security Mode, click **Enable**.
4. Click **Next**.
5. Enter the Computer Setup setup password at the prompt, and then click **Next**.
6. Insert the new administrator smart card, and follow the on-screen instructions. The instructions vary and may include the following tasks:
   - Initializing the smart card. Refer to "Initializing the smart card" for detailed instructions.
   - Setting the smart card administrator password. Refer to "Storing the administrator or user card password" for detailed instructions.
   - Creating a recovery file. Refer to "Creating a recovery file" for detailed instructions.

Disabling smart card BIOS security mode

When disabling smart card BIOS security mode, the smart card administrator and user passwords are disabled, and the use of the smart card is no longer needed to access the computer.

NOTE If smart card BIOS security mode has previously been enabled, the button on the "Smart Card Security BIOS" page changes to Disable.

To disable smart card security:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **BIOS**.
3. In the right pane, under **BIOS Security Mode**, click **Disable**.
4. Insert the card containing the current smart card administrator password, and then click **Next**.
5. Enter the smart card PIN at the prompt and click **Finish**.

Changing the smart card administrator password

The smart card administrator password is set as part of the process for enabling smart card BIOS security mode. You can change the smart card administrator password after it has been set. Refer to "Smart card BIOS security mode," earlier in this chapter, for more information about the smart card administrator password.

NOTE The following procedure updates the smart card administrator password stored on the card and in Computer Setup.

To change the smart card administrator password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **BIOS**.
3. In the right pane, under **BIOS Security Mode**, next to **BIOS administrator card**, click **Change**.
4. Enter the smart card PIN and click **Next**.
5. Insert the new administrator card and click **Next**.
6. Enter the smart card PIN and click **Finish**.

Setting and changing the smart card user password

To set or change the smart card user password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **BIOS**.
3. In the right pane, under **BIOS Security Mode**, next to **BIOS user card**, click the **Set** button.

   NOTE If there is already a user password in Computer Setup, click the **Change** button.

4. Enter the smart card PIN and click **Next**.
5. Insert the new user card and click **Next**.
   - If there is already a user password on the card, the **Finish** dialog box is displayed. Omit steps 6 through 8 and go to step 9.
   - If there is no user password on the card, the BIOS Password Wizard opens.
6. In the BIOS Password Wizard, you can either
   - Enter a password manually.
   - Generate a random 32-byte password.

   NOTE Using a known password enables you to create duplicate cards without using a recovery file. Generating a random password offers more security; however, you must have a recovery file to make backup cards.

7. Under **Boot Requirements**, select the check box if you require the smart card PIN to be entered at startup.

   NOTE If you do not require the smart card PIN to be entered at startup, clear this check box.

8. Enter the smart card PIN and click **OK**. The system prompts you to create a recovery file.

   NOTE It is highly recommended that you create a recovery file. For more information, refer to “Creating a recovery file,” later in this chapter.

9. Enter the smart card PIN in the **Finish** dialog box, and then click **Finish**.

Storing the administrator or user card password

If you want to create a backup card and have already set the administrator password, you can store the password on the new card.

CAUTION This procedure updates only the password on the card and not in Computer Setup. You will not be able to access the computer with the new card.

To store the administrator or user card password:

1. Insert a smart card into the reader.
2. Select **Start > All Programs > HP ProtectTools Security Manager**.
3. In the left pane, click **Smart Card Security**, and then click **BIOS**.
4. In the right pane, under **BIOS Password on Smart Card**, click **Store**.
5. In the BIOS Password Wizard, you can either
   - Enter a password manually.
   - Generate a random 32-byte password.

   NOTE Using a known password enables you to create duplicate cards without using a recovery file. Generating a random password offers more security; however, you must have a recovery file to make backup cards.
6. Under **Access Privilege**, click either **Administrator** or **User** for the type of card.
7. Under **Boot Requirements**, select the check box if you require that the smart card PIN be entered at startup.

   NOTE If you do not require the smart card PIN to be entered at startup, clear this check box.
8. Enter the smart card PIN and click **OK**.
9. Enter the smart card PIN again in the **Finish** dialog box, and then click **Finish**.

   The system prompts you to create a recovery file.

   NOTE It is highly recommended that you create a smart card recovery file. For more information, refer to “Creating a recovery file,” later in this chapter.

General tasks

Updating BIOS smart card settings

To require a smart card PIN when you restart the computer:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **BIOS**.
3. In the right pane, under **Smart Card BIOS Password Properties**, click **Settings**.
4. select the check box to require a PIN at reboot.

NOTE To eliminate this requirement, clear the check box.

5. Enter the smart card PIN and click **OK**.

Selecting the smart card reader

Ensure that the correct smart card reader is selected in Smart Card Security before using the smart card. If the correct reader is not selected in Smart Card Security, some of the features may be unavailable or incorrectly displayed.

To select the smart card reader:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **General**.
3. In the right pane, under **Smart Card Reader**, click the correct reader.
4. Insert the smart card into the reader. The reader information is automatically refreshed.

Changing the smart card PIN

To change the smart card PIN:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **Smart Card**.
3. In the right pane, under **Change PIN**, click **Change PIN**.
4. Type your current smart card PIN.
5. Set and confirm the new PIN.
6. Click **OK** in the confirmation dialog box.

Backing up and restoring smart cards

After you have initialized a smart card and the card is ready for use, it is highly recommended that you create a smart card recovery file. The recovery file can be used to transfer the smart card data from one smart card to another smart card. This file can also be used to back up the original smart card or to restore the data when a smart card is lost or stolen.

CAUTION To avoid having a recovery file that does not match a smart card with updated information, immediately create a new recovery file and store it in a safe place. If you keep a backup smart card, you must also update the information on the backup smart card by restoring the new recovery file onto the backup smart card.

Creating a recovery file

To create a recovery file:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **Smart Card**.
3. In the right pane, under **Recovery**, click **Create**.
4. Enter the smart card PIN and click **OK**.
5. Enter the file path and file name in the **Filename** box.

   CAUTION To avoid loss of access to the computer, do not save the recovery file on the computer hard drive; you will not be able to access the file without the smart card. Also, a recovery file saved on the hard drive may be accessible to others, posing a security risk.

6. Set and confirm a recovery file password, and then click **OK**.

CAUTION To prevent the loss of the smart card recovery file data, do not forget the recovery file password. You cannot re-create your card from the recovery file if you forget the password.

Restoring smart card data

You can restore the smart card data from the recovery file. This is especially useful if a card was lost or stolen, or if you want to create a backup smart card. If you use a card with previous data saved on it, the data will be overwritten.

Before you begin, you will need the following:

- Access to a computer with Smart Card Security software installed
- Smart card recovery file
- Smart card recovery file password
- Smart card

To restore a smart card:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Smart Card Security**, and then click **Smart Card**.
3. Insert the diskette or other media containing the smart card recovery file.
4. Insert a smart card into the reader. If the card is not initialized, you will be prompted to initialize it. For detailed instructions on initializing the smart card, refer to "Initializing the smart card," earlier in this chapter.
5. In the right pane, under **Recovery**, click **Restore**.
6. Ensure that the correct recovery file name is selected, and enter the recovery file password.
7. Enter the smart card PIN.
8. Click **OK**. The original smart card contents are restored to the new smart card.

Creating a backup smart card

It is highly recommended that you create duplicate smart cards for backup purposes. Two methods can be used to create a backup card, depending upon whether the smart card password was manually or randomly generated.

To create a replacement smart card with a randomly generated smart card password:

- Insert a smart card into the reader, and then load the appropriate recovery file onto it. For more information, refer to "Restoring smart card data," earlier in this chapter.

To create a replacement smart card with a manually generated smart card password:

1. Initialize a new smart card. For instructions, refer to "Initializing the smart card," earlier in this chapter.
2. Store the administrator or user card password on the new smart card. For instructions, refer to "Storing the administrator or user card password," earlier in this chapter.

3 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools manages the Java Card setup and configuration for computers equipped with an optional smart card reader.

With Java Card Security, you can

- Access Java Card security features.
- Work with the Computer Setup utility to enable Java Card authentication in a power-on environment, and to configure separate Java Cards for an administrator and a user. This requires a user to insert the Java Card and enter a PIN to allow the operating system to load.
- Set and change the PIN used to authenticate users of the Java Card.
- Back up and restore power-on authentication data on the Java Card.

General tasks

The “General” page allows you to perform the following tasks:

- Change a Java Card PIN
- Select the smart card reader

NOTE The smart card reader uses both Java Cards and smart cards. This feature is available if you have more than one smart card reader on the computer.

Changing a Java Card PIN

To change a Java Card PIN:

NOTE The Java Card PIN must be between 4 and 8 numeric characters.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **General**.
3. Insert a Java Card (with an existing PIN) into the smart card reader.
4. In the right pane, click **Change**.
5. In the **Change PIN** dialog box, enter the current PIN in the **Current PIN** box.
6. Enter a new PIN in the **New PIN** box, and then enter the PIN again in the **Confirm New PIN** box.
7. Click **OK**.

Selecting the smart card reader

Ensure that the correct smart card reader is selected in Java Card Security before using the Java Card. If the correct reader is not selected in Java Card Security, some of the features may be unavailable or incorrectly displayed.

To select the smart card reader:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **General**.
3. Insert the Java Card into the smart card reader.
4. In the right pane, under **Smart Card Reader**, click the correct reader.

Advanced tasks (administrators only)

The “Advanced” page allows you to perform the following tasks:

- Assign a Java Card PIN
- Assign a name to a Java Card
- Set power-on authentication
- Back up and restore Java Cards

NOTE You must have a Computer Setup setup password in order to get to the “Advanced” page.

Assigning a Java Card PIN

You must assign a PIN to a Java Card before it can be used for power-on authentication.

To assign a Java Card PIN:

NOTE The Java Card PIN must be between 4 and 8 numeric characters.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **General**.
3. Insert a new Java Card into the smart card reader.
4. When the **Change PIN** dialog box opens, enter a new PIN in the **New PIN** box, and then enter the PIN again in the **Confirm New PIN** box.
5. Click **OK**.

Assigning a name to a Java Card

You must assign a name to a Java Card before it can be used for power-on authentication.

To assign a name to a Java Card:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. Insert the Java Card into the smart card reader.

   NOTE If you have not assigned a PIN to this card, the Change PIN dialog box opens, allowing you to enter a new PIN.

5. In the right pane, under **Java Card** name, click **Change**.
6. Enter a name for the Java Card in the **Name** box.
7. Enter the current Java Card PIN in the **PIN** box.
8. Click **OK**.

Setting power-on authentication

When enabled, power-on authentication requires you to use a Java Card to start the computer.

The process of enabling Java Card power-on authentication involves the following steps:

1. Enable Java Card power-on authentication support in BIOS Configuration or Computer Setup. Refer to "Enabling and disabling smart card or Java Card power-on authentication support," in Chapter 5, "BIOS Configuration for HP ProtectTools."
2. Enable Java Card power-on authentication in Java Card Security. Refer to "Enabling Java Card power-on authentication and creating an administrator Java Card," later in this chapter.
3. Create and enable the administrator Java Card.

Enabling Java Card power-on authentication and creating an administrator Java Card

To enable Java Card power-on authentication:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Computer Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. Insert the Java Card into the smart card reader.

   NOTE If you have not assigned a PIN to this card, the **Change PIN** dialog box opens, allowing you to enter a new PIN.

5. In the right pane, under **Power-on authentication**, select the **Enable** check box.
6. If you do not have DriveLock enabled, enter the Java Card PIN, and then click **OK**.

   – or –

   If you do have DriveLock enabled:

   a. click **Make Java card identity unique**.

      – or –

      click **Make the Java card identity the same as the DriveLock password**.

      NOTE If DriveLock is enabled on the computer, you can set the Java Card identity to be the same as the DriveLock user password, which allows you to validate both DriveLock and the Java Card using only the Java Card when starting the computer.

   b. If applicable, enter your DriveLock user password in the **DriveLock password** box, and then enter it again in the **Confirm password** box.

   c. Enter the Java Card PIN.

   d. Click **OK**.

7. When you are prompted to create a recovery file, refer to "Creating a recovery file," or you can click **Cancel** and create a recovery file at a later time.

Creating a user Java Card

NOTE Power-on authentication and an administrator card must be set up in order to create a user Java Card.

To create a user Java Card:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. Insert a Java Card that will be used as a user card.
5. In the right pane, under **Power-on authentication**, click **Create** next to **User card identity**.
6. Enter a PIN for the user Java Card, and then click OK.

Disabling Java Card power-on authentication

When you disable Java Card power-on authentication, the use of the Java Card is no longer needed to access the computer.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. Insert the Java Card, enter the PIN, and then click **OK**.
5. In the right pane, under **Power-on authentication**, clear the **Enable** check box.

Backing up and restoring Java Cards

After you have assigned power-on authentication identity to a Java Card, it is highly recommended that you create a Java Card recovery file. The recovery file can be used to transfer the Java Card power-on authentication identity data from one Java Card to another Java Card. This file can also be used to back up the original Java Card or to restore the data when a Java Card is lost or stolen.

CAUTION To avoid having a recovery file that does not match a Java Card containing updated information, immediately create a new recovery file on removable media and put it in a safe place. If you keep a backup Java Card, you must also update the information on the backup Java Card by restoring the new recovery file onto the backup Java Card.

Creating a recovery file

To create a recovery file:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. In the right pane, under **Recovery**, click **Create**.
5. Enter the file path and file name in the **Filename** box.

   CAUTION To avoid loss of access to the computer, do not save the recovery file on the computer hard drive; you will not be able to access the file without the Java Card. Also, a recovery file saved on the hard drive may be accessible to others, posing a security risk.

6. Enter a recovery file password in the **Recovery file password** box, and then enter it again in the **Confirm password** box.
7. Enter the Java Card PIN, and then click **OK**.

CAUTION To prevent the loss of the Java Card recovery file data, do not forget the recovery file password. You cannot re-create your card from the recovery file if you forget the password.

Restoring Java Card data

You can restore the Java Card data from the recovery file. This is especially useful if a card was lost or stolen, or if you want to create a backup Java Card. If you use a card with previous data saved on it, the data will be overwritten.

Before you begin, you will need the following:

- Access to a computer with Java Card Security software installed
- Java Card recovery file
- Java Card recovery file password
- Java Card

To restore a Java Card:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Java Card Security**, and then click **Advanced**.
3. When the **Setup Password** dialog box displays, enter your Computer Setup setup password, and then click **OK**.
4. Insert the diskette or other media containing the Java Card recovery file.
5. Insert a Java Card into the reader. If the card has not been assigned a PIN, you will be prompted to create a PIN. For detailed instructions on assigning a PIN to the Java Card, refer to "Assigning a Java Card PIN," earlier in this chapter.
6. In the right pane, under Recovery, click **Restore**.
7. Ensure that the correct recovery file name is selected, and enter the recovery file password.
8. Enter the Java Card PIN.
9. Click **OK**.

   The original Java Card contents are restored to the new Java Card.

Creating a backup Java Card

It is highly recommended that you create duplicate Java Cards for backup purposes.

To create a replacement Java Card:

- Insert a Java Card into the reader, and then load the appropriate recovery file onto it. For more information, refer to "Restoring Java Card data," earlier in this chapter.

4 Embedded Security for HP ProtectTools

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

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

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

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

Setup procedures

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

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

Enabling the embedded security chip

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

To enable the embedded security chip:

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

Initializing the embedded security chip

In the initialization process for Embedded Security, you will

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

To initialize the embedded security chip:

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

   The HP ProtectTools Embedded Security Initialization Wizard opens.

2. Click **Next**.
3. Set and confirm an owner password, and then click **Next**.

   The Setup Emergency Recovery dialog box opens.

4. Click **Next** to accept the default recovery archive location, or click the **Browse** button to choose a different location, and then click **Next**.
5. Set and confirm the emergency recovery token password, and then click **Next**.
6. Click **Browse** and choose the location for the emergency recovery archive, and then click **Next**.
7. Click **Next** on the “Summary” page.

   - If you do not want to set up a basic user account at this time, clear the **Start the Embedded Security User Initialization Wizard** check box, and then click **Finish**. You can start the wizard manually to set up a basic user account at any time by following the instructions in the next section.
   - If you want to set up a basic user account, select the **Start the Embedded Security User Initialization Wizard** check box, and then click **Finish**. The Embedded Security User Initialization Wizard opens. Refer to the instructions in the next section for more details.

Setting up the basic user account

Setting up a basic user account in Embedded Security

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

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

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

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

   The Embedded Security User Initialization Wizard opens.
4. Click **Next**.
5. Set and confirm the Basic User Key password, and then click **Next**.
6. Click **Next** to confirm settings.
7. Select the security features you want, and then click **Next**.
8. Click **Next** again.

   NOTE To use secure e-mail, you must first configure the e-mail client to use a digital certificate that is created with Embedded Security. If a digital certificate is not available, you must obtain one from a certification authority. For instructions on configuring your e-mail and obtaining a digital certificate, refer to the e-mail client online Help.
9. If more than one encryption certificate exists, select the appropriate certificate, and then click **Next**.
10. Select the drive letter and label for the PSD, and then click **Next**.
11. Select the size and location of the PSD, and then click **Next**.
12. Click **Next** on the “Summary” page.
13. Click **Finish**.

General tasks

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

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

Using the Personal Secure Drive

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

Encrypting files and folders

When working with encrypted files, consider the following rules:

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

To encrypt files and folders:

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

Sending and receiving encrypted e-mail

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

Changing the Basic User Key password

To change the Basic User Key password:

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

Advanced tasks

Backing up and restoring

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

Creating a backup file

To create a backup file:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Backup**.
3. In the right pane, click **Backup**.
4. Click **Browse** to choose the location where the backup file will be saved.
5. Select whether to add the emergency recovery archive to the backup information.
6. Click **Next**.
7. Click **Finish**.

Restoring certification data from the backup file

To restore data from the backup file:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Embedded Security**, and then click **Backup**.
3. In the right pane, click **Restore**.
4. Click **Browse** to select the backup file from the stored location.
5. Click **Next**.
6. Select whether to start the Embedded Security User Initialization Wizard.
   - If you choose to start the initialization wizard, click Finish, and then follow the on-screen instructions to complete the initialization. For more information, refer to "Setting up the basic user account," earlier in this chapter.
   - If you choose not to start the initialization wizard, click **Finish**.

Changing the owner password

To change the owner password:

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

Resetting a user password

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

Enabling and disabling Embedded Security

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

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

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

Permanently disabling Embedded Security

To permanently disable Embedded Security:

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

Enabling Embedded Security after permanent disable

To enable Embedded Security after permanently disabling it:

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

Migrating keys with the Migration Wizard

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

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

5 BIOS Configuration for HP ProtectTools

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

With BIOS Configuration, you can

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

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

General tasks

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

Managing boot options

You can use BIOS Configuration to manage various settings for tasks that run when you turn on or restart the computer.

To manage boot options:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.

   NOTE The BIOS administrator password prompt is displayed only if you have already set the Computer Setup setup password. For more information about setting the Computer Setup setup password, refer to "Setting the setup password," later in this chapter.

4. In the left pane, click **System Configuration**.
5. In the right pane, select the delays (in seconds) for f9, f10 and f12, and for **Express Boot Popup Delay (Sec)**.
6. Enable or disable **MultiBoot**.
7. If you have enabled MultiBoot, select the boot order by selecting a boot device, and then clicking the up arrow or the down arrow to adjust its order in the list.
8. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Enabling and disabling system configuration options

NOTE Some of the items listed below may not be supported by your computer.

To enable or disable devices or security options:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.
4. In the left pane, click **System Configuration**, and then enable or disable a system configuration option, or configure a system configuration option in the right pane:
   - Port Options
     - Serial Port
     - Infrared Port
     - Parallel Port
     - SD Slot
     - USB Port
     - 1394 Port
     - Cardbus Slot
     - ExpressCard slot
   - Boot Options
     - f9, f10, and f12 Delay (Sec)
     - MultiBoot
     - Express Boot Popup Delay (Sec)
     - CD-ROM Boot
     - Floppy Boot
     - Internal Network Adapter Boot
     - Internal Network Adapter Boot Mode (PXE or RPL)
     - Boot Order
   - Device Configurations
     - NumLock at Boot
     - Swapping fn/Ctrl Keys
     - Multiple Pointing Devices
     - USB Legacy Support

- Parallel port mode (standard, bidirectional, EPP, or ECP)
- Data Execution Prevention
- SATA Native Mode
- Dual Core CPU
- Automatic Intel® SpeedStep Functionality Support
- Fan Always on While on AC Power
- BIOS DMA Data Transfers
- Intel or AMD PSAE Execution Disable

- Built-In Device Options
  - Embedded WLAN Device Radio
  - Embedded WWAN Device Radio
  - Embedded Bluetooth® Device Radio
  - LAN/WLAN Switching
  - Wake on LAN from Off

5. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes and exit.

Advanced tasks

Managing HP ProtectTools settings

Some of the features of HP ProtectTools Security Manager can be managed in BIOS Configuration.

Enabling and disabling smart card or Java Card power-on authentication support

Enabling this option allows you to use the smart card or the Java Card for user authentication when you turn on the computer.

NOTE To fully enable the power-on authentication feature, you must also configure the smart card using the Smart Card Security for HP ProtectTools or Java Card Security for HP ProtectTools module.

To enable smart card power-on authentication support:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.
4. In the left pane, click **Security**.
5. Under **Smart Card Security**, click **Enable**.

   

   NOTE To disable smart card power-on authentication, click **Disable**.

6. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Enabling and disabling power-on authentication support for Embedded Security

Enabling this option allows the system to use the TPM embedded security chip (if available) for user authentication when you turn on the computer.

NOTE To fully enable the power-on authentication feature, you must also configure the TPM embedded security chip using the Embedded Security for HP ProtectTools module.

To enable power-on authentication support for embedded security:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.
4. In the left pane, click **Security**.
5. Under **Embedded Security**, click **Enable Power-on Authentication Support**.

   

   NOTE To disable power-on authentication for Embedded Security, click **Disable**.

6. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Enabling and disabling Automatic DriveLock hard drive protection

When this option is enabled, the DriveLock passwords will be automatically generated and set in the drive, and protected by the TPM embedded security chip.

NOTE The automatically generated passwords will not be set in the drive until the computer is restarted and you successfully enter the TPM embedded security password at the password prompt.

The option to enable Automatic DriveLock is unavailable unless

- The computer has a TPM security chip installed and initialized. For instructions on how to enable and initialize the TPM security chip, refer to "Enabling the embedded security chip" and "Initializing the embedded security chip" in Chapter 4, "Embedded Security for HP ProtectTools."
- No DriveLock passwords have already been enabled.

NOTE If you have already manually set DriveLock passwords on the computer, you must first disable them before you can set Automatic DriveLock protection.

To enable or disable Automatic DriveLock protection:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.
4. In the left pane, click **Security**.
5. Under **Embedded Security**, click **Enable** next to **Automatic DriveLock Support**.

   NOTE To disable automatic DriveLock protection for Embedded Security, click **Disable**.

6. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Managing Computer Setup passwords

You can use BIOS Configuration to set and change the power-on and setup passwords in Computer Setup, and also to manage various password settings.

CAUTION The passwords you set through the "Passwords" page in BIOS Configuration are saved immediately upon clicking the **Apply** or **OK** button in the HP ProtectTools window. Make sure you remember what password you have set, because you will not be able to undo a password setting without supplying the previous password.

The power-on password can protect your notebook from unauthorized use.

NOTE After you have set a power-on password, the Set button on the "Passwords" page is replaced by a Change button.

The Computer Setup setup password protects the configuration settings and system identification information in Computer Setup. After this password is set, it must be entered to access Computer Setup.

If you have set a setup password, you will be prompted for the password before opening the BIOS Configuration portion of HP ProtectTools.

NOTE After you have set a setup password, the Set button on the “Passwords” page is replaced by a Change button.

Setting the power-on password

To set the power-on password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.
3. In the right pane, next to **Power-On Password**, click **Set**.
4. Type and confirm the password in the **Enter Password** and **Verify Password** boxes.
5. Click **OK** in the Passwords dialog box.
6. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Changing the power-on password

To change the power-on password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.
3. In the right pane, next to **Power-On Password**, click **Change**.
4. Type the current password in the **Old Password** box.
5. Set and confirm the new password in the **Enter New Password** box.
6. Click **OK** in the **Passwords** dialog box.
7. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Setting the setup password

To set the Computer Setup setup password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.
3. In the right pane, next to **Setup Password**, click **Set**.
4. Type and confirm the password in the **Enter Password** and **Confirm Password** boxes.
5. Click **OK** in the **Passwords** dialog box.
6. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Changing the setup password

To change the Computer Setup setup password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.
3. In the right pane, next to **Setup Password**, click **Change**.
4. Type the current password in the **Old Password** box.
5. Type and confirm the new password in the **Enter New Password** and **Verify New Password** boxes.
6. Click **OK** in the **Passwords** dialog box.
7. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Setting password options

You can use BIOS Configuration for HP ProtectTools to set password options to enhance the security of your system.

Enabling and disabling stringent security

CAUTION To prevent the computer from becoming permanently unusable, record your configured setup password, power-on password, or smart card PIN in a safe place away from your computer. Without these passwords or PIN, the computer cannot be unlocked.

Enabling stringent security provides enhanced protection for the power-on and administrator passwords and other forms of power-on authentication.

To enable or disable stringent security:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.
3. In the right pane, under **Password Options**, enable or disable **Stringent Security**.

   NOTE If you want to disable stringent security, clear the **Enable Stringent Security** check box.

4. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

Enabling and disabling power-on authentication on Windows restart

This option allows you to enhance security by requiring users to enter a power-on, TPM, or smart card password when Windows restarts.

To enable or disable power-on authentication on Windows restart:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **BIOS Configuration**, and then click **Security**.

3. In the right pane, under **Password Options**, enable or disable **Require password on restart**.
4. Click **Apply**, and then click **OK** in the HP ProtectTools window to save your changes.

6 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools has security features that provide protection against unauthorized access to your computer. These features include the following:

- Alternatives to passwords when logging on to Windows, such as using a smart card or biometric reader to log on to Windows. For additional information, refer to “Registering credentials,” later in this chapter.
- Single Sign On feature that automatically remembers credentials for Web sites, applications, and protected network resources.
- Support for optional security devices, such as smart cards and biometric readers.
- Support for additional security settings, such as requiring authentication using an optional security device to unlock the computer.

Setup procedures

Logging on to Credential Manger

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

- Credential Manager Logon Wizard (preferred)
- HP ProtectTools Security Manager icon in the notification area
- HP ProtectTools Security Manager

NOTE If you use the Credential Manager Logon prompt on the Windows Logon screen to log on to Credential Manager, you are logged on to Windows at the same time.

The first time you open Credential Manager, log on with your regular Windows Logon password. A Credential Manager account is then automatically created with your Windows logon credentials.

After logging on to Credential Manager, you can register additional credentials, such as a fingerprint or a smart card. For additional information, refer to “Registering credentials,” later in this chapter.

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

Using the Credential Manager Logon Wizard

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

1. Open the Credential Manager Logon Wizard in any of the following ways:
   - From the Windows logon screen
   - From the notification area, by double-clicking the **HP ProtectTools Security Manager** icon
   - From the “Credential Manager” page of ProtectTools Security Manager, by clicking the **Log On** link in the upper-right corner of the window
2. Click **Next**.
3. Type your user name in the **User name** box.
4. Enter a password in the **Password** box, and then click **Next**.
5. Click **Finish**.

Logging on for the first time

Before you begin, you must be logged on to Windows with an administrator account, but not logged on to Credential Manager.

1. Open HP ProtectTools Security Manager by double-clicking the HP ProtectTools Security Manager icon in the notification area. The HP ProtectTools Security Manager window opens.
2. In the left pane, click **Credential Manager**, and then click **Log On** in the upper-right corner of the right pane. The Credential Manager Logon Wizard opens.
3. Type your Windows password in the **Password** box, and then click **Next**.

Registering credentials

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

Registering fingerprints

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

Setting up the fingerprint reader

1. After logging on to Credential Manager, swipe your finger across the fingerprint reader. The Credential Manager Registration Wizard opens.
2. Click **Next**.

   NOTE By default, Credential Manager requires registration of *at least* 2 different fingers.

   The right index finger is the default finger for enrolling the first fingerprint. You can change the default by clicking the finger you want to register first, on either the left hand or the right hand. When you click a finger, it will be outlined to show it has been selected.

3. Slowly swipe your finger downward over the fingerprint sensor. Follow the instructions in the wizard and continue swiping the same finger over the fingerprint sensor until the finger on the screen turns green.

   NOTE Multiple swipes are necessary to register a fingerprint.

   If you need to start over during the fingerprint registration process, right-click the highlighted finger on the screen and then click **Clear** or **Clear All**.

4. Follow the instructions in the wizard to register a second finger.

   NOTE If you click **Finish** before registering at least two fingers, an error message is displayed. Click **OK** to continue.

5. When you have successfully registered at least two fingers, click **Next**.
6. If you wish to log on to Windows by swiping your finger, be sure the **Yes, I want to use Credential Manager to logon to Windows** check box is selected. Click **Finish**.
7. To set up the fingerprint reader for a different Windows user, log on to Windows as that user and then repeat steps 1 through 6.

Using your registered fingerprint to log on to Windows

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

Registering a Java Card, smart card, token, or virtual token

NOTE You must have a smart card reader configured for this procedure. If you do not have a reader installed, you can register a virtual token as described in "Creating a virtual token."

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Register Smart Card or Token**. The Credential Manager Registration Wizard opens.
4. Click **Next**.

5. Click the authentication method you want to register, and then click **Next**.
6. Follow the on-screen instructions to complete the registration.

Registering a USB eToken

1. Be sure that the USB eToken drivers are installed.

   NOTE Refer to the USB eToken user guide for more information.

2. Select **Start > All Programs > HP ProtectTools Security Manager**.
3. In the left pane, click **Credential Manager**.
4. In the right pane, click **Register Smart Card or Token**. The Credential Manager Registration Wizard opens.
5. Click **Next**.
6. Under **Device Type**, click **USB eToken**, and then click **Next**.
7. Follow the on-screen instructions to complete the registration.

Registering other credentials

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Register Credentials**. The Credential Manager Registration Wizard opens.
4. Click **Next**.
5. Click the authentication method you want to register, and then click **Next**.
6. Follow the on-screen instructions to complete the registration.

General tasks

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

- Creating a virtual token
- Changing the Windows logon password
- Managing a token PIN
- Managing identity
- Locking the computer

NOTE This option is available only if the Credential Manager classic logon prompt is enabled. See “Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager.”

Creating a virtual token

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

To create a new virtual token:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Virtual Token**. The Credential Manager Registration Wizard opens.

NOTE If Virtual Token is not an option, use the procedure for “Registering other credentials.”

4. Click **Next**.
5. Click **Virtual Token**, and then click **Next**.
6. Enter a name and location for the virtual token file (or click **Browse** to find a file location), and then click **Next**.
7. Set and confirm a master PIN and a user PIN.
8. Click **Finish**.

Changing the Windows logon password

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Change Windows Password**.
4. Type your old password in the **Old password** box.

5. Type your new password in the **New password** and **Confirm password** boxes.
6. Click **Finish**.

Changing a token PIN

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Change Token PIN**.
4. Select the token for which you want to change the PIN, and then click **Next**.
5. Follow the on-screen instructions to complete the PIN change.

Managing identity

Backing up an identity

It is recommended that you back up your identity in Credential Manager, in case of data loss or accidental removal.

To back up an identity:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Backup Identity**.
4. Select the elements you want to back up, and then click **Next**.
5. On the “Device Type” page, select the device type you want to use to store the backup, and then click **Next**.

   NOTE You will need to know the password or PIN for the device you select for the backup file.

6. Follow the on-screen instructions, and then click **Finish**.

Restoring an Identity

To restore an identity:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Restore Identity**.
4. On the “Device Type” page, select the device type where the backup is stored, and then click **Next**.

   NOTE You will need to know the password or PIN for the device you select for the backup file.

5. Follow the on-screen instructions, and then click **Finish**.
6. Click **Yes** in the confirmation dialog box.

Clearing an identity from the system

NOTE This does not affect your Windows user account.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Clear Identity for this Account**.
4. Click **Yes** in the confirmation dialog box. Your identity is logged off and removed from the system.

Locking the computer

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

NOTE This option is available only if the Credential Manager classic logon prompt is enabled. See "Example 1—Using the "Advanced Settings" page to allow Windows logon from Credential Manager."

For added security, you can configure the Lock Workstation feature to require a smart card, biometric reader, or token to unlock the computer. For more information, refer to "Configuring Credential Manager settings," later in this chapter.

To lock the computer:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**.
3. In the right pane, click **Lock Workstation**. The Windows logon screen is displayed. You must use a Windows password or the Credential Manager Logon Wizard to unlock the computer.

Using Windows Logon

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

Logging on to Windows with Credential Manager

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

1. If you have registered your fingerprint to log on to Windows, swipe your finger to log on.
2. If you have not registered your fingerprint to log on to Windows, click the keyboard icon in the upper-left corner of the screen next to the fingerprint icon. The Credential Manager Logon Wizard opens.
3. Click the **User name** arrow and click your name.
4. Type your password in the **Password** box and click **Next**.
5. Select **More > Wizard Options**.
   a. If you want this to be the default user name the next time that you log on to the computer, select the **Use last user name on next logon** check box.
   b. If you want this logon policy to be the default method, select the **Use last policy on next logon** check box.
6. Follow the on-screen instructions. If your authentication information is correct, you will be logged on to your Windows account and to Credential Manager.

Adding an account

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, click **Windows Logon**, and then click **Add a Network Account**. The Add Network Account Wizard opens.
4. Type the user name for the new account in the **User name** box, or click **Browse** to find a user name.
5. Click the domain from the list of available domains.
6. Type and confirm the password.

NOTE If you want Credential Manager to validate this account, be sure the **Validate network account when Next or Finish button clicked** check box is selected.

7. Click **Finish**.

Removing an account

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, click **Windows Logon**, and then click **Manage Network Accounts**. The **Manage Network Accounts** dialog box opens.
4. Click the account you want to remove, and then click **Remove**.
5. In the confirmation dialog box, click **Yes**.
6. Click **OK**.

Using Single Sign On

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

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

NOTE You can also configure Single Sign On to validate your authentication credentials with a smart card, fingerprint reader, or token before logging on to a secure site or program. This is particularly useful when logging on to programs or Web sites that contain personal information, such as bank account numbers. For more information, refer to “Configuring Credential Manager settings,” later in this chapter.

Registering a new application

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

Using automatic registration

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

Using manual (drag and drop) registration

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, click **Single Sign On**, and then click **Register New Application**. The SSO Application Wizard opens.
4. Run the application you want to register until you reach the page with the password box.
5. On the “Drag and Drop Registration” page of the SSO Application Wizard, select the type of activity you want to automate.

   

   NOTE In most cases, the activity you want to automate will be the **Logon simple dialog**.
6. Click and drag the icon from the wizard page over the area of the application where the password box is located. Release the pointer when the area is highlighted.
7. On the “Application Information” page of the SSO Application Wizard, enter the name and description for the application.
8. Click **Finish**.
9. Type the logon credential—for example, the user name and password—into the application box.
10. In the Credential Manager Single Sign On dialog box, either confirm the credential name or right-click the name and modify it. Click **Yes**.
11. Click **More** and select from the following options:
    - Do not use SSO for this site or application.
    - Prompt to select account for this application.
    - Fill in credentials but do not submit.

- Authenticate user before submitting credentials.
- Show SSO shortcut for this application.

12. Click **Yes** to complete the registration.

Managing applications and credentials

Modifying application properties

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Single Sign On**, click **Manage Applications and Credentials**.
4. Click the application entry you want to modify, and then click **Properties**.
5. Click the **General** tab to modify the application name and description. Change the settings by selecting or clearing the check boxes next to the appropriate settings.
6. Click the **Script** tab to view and edit the SSO application script.
7. Click **OK** to save your changes.

Removing an application from Single Sign On

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Single Sign On**, click **Manage Applications and Credentials**.
4. Click the application entry you want to remove, and then click **Remove**.
5. Click **Yes** in the confirmation dialog box.
6. Click **OK**.

Exporting an application

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

To export an application:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Single Sign On**, click **Manage Applications and Credentials**.
4. Click the application entry you want to export. Then click **More > Applications > Export Script**.
5. Follow the on-screen instructions to complete the export.
6. Click **OK**.

Importing an application

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Single Sign On**, click **Manage Applications and Credentials**.
4. Click the application entry you want to import. Then select **More > Applications > Import Script**.
5. Follow the on-screen instructions to complete the import.
6. Click **OK**.

Modifying credentials

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Single Sign On**, click **Manage Applications and Credentials**.
4. Click the application entry you want to modify, and then click **More**.
5. Select any of the following options:
   - Applications
     - Add New
     - Remove
     - Properties
     - Import Script
     - Export Script
   - Credentials
     - Create New
   - View Password

     NOTE You must authenticate your identity before viewing the password.
6. Follow the on-screen instructions.
7. Click **OK** to save changes.

Using Application Protection

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

- Category of user
- Time of use
- User inactivity

Restricting access to an application

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Application Protection**, click **Manage Protected Applications**. The Application Protection Service dialog box opens.
4. Select a category of user whose access you want to manage.

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

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

Removing protection from an application

To remove restrictions from an application:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.

3. In the right pane, under **Application Protection**, click **Manage Protected Applications**. The Application Protection Service dialog box opens.
4. Select a category of user whose access you want to manage.

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

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

Changing restriction settings for a protected application

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Services and Applications**.
3. In the right pane, under **Application Protection**, click **Manage Protected Applications**. The Application Protection Service dialog box opens.
4. Select a category of user whose access you want to manage.

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

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

Advanced tasks (administrator only)

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

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

Specifying how users and administrators log on

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

To specify how users or administrators log on:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Authentication and Credentials**.
3. In the right pane, click the **Authentication** tab.
4. Click the category (**Users** or **Administrators**) from the category list.
5. Click the type or combination of authentication methods from the list.
6. Click **Apply**, and then click **OK** to save your changes.

Configuring custom authentication requirements

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

To configure custom requirements:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Authentication and Credentials**.
3. In the right pane, click the **Authentication** tab.
4. Click the category (**Users** or **Administrators**) from the category list.
5. Click **Custom** in the list of authentication methods.
6. Click **Configure**.
7. Select the authentication methods you want to use.
8. Choose the combination of methods by clicking one of the following:
   - Use AND to combine the authentication methods

     (Users will have to authenticate with all of the methods you checked each time they log on.)
   - Use OR to require one of two or more authentication methods

     (Users will be able to choose any of the selected methods each time they log on.)
9. Click **OK**.
10. Click **Apply**, and then click **OK** to save your changes.

Configuring credential properties

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

To configure the credentials:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Authentication and Credentials**.
3. In the right pane, click the **Credentials** tab.
4. Click the credential type you want to modify:
   - To register the credential, click **Register**, and then follow the on-screen instructions.
   - To delete the credential, click **Clear**, and then click **Yes** in the confirmation dialog box.
   - To modify the credential properties, click **Properties**, and then follow the on-screen instructions.
5. Click **Apply**, and then click **OK**.

Configuring Credential Manager settings

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

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

To modify Credential Manager settings:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Settings**.
3. In the right pane, click the appropriate tab for the settings you want to modify.
4. Follow the on-screen instructions to modify the settings.
5. Click **Apply**, and then click **OK** to save your changes.

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

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

NOTE Selecting the **Use Credential Manager with classic logon prompt** check box allows you to lock your computer. See “Locking the computer.”

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

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Credential Manager**, and then click **Settings**.
3. In the right pane, click the **Single Sign On** tab.
4. Under **When registered logon dialog or Web page is visited**, select the **Authenticate user before submitting credentials** check box.
5. Click **Apply**, and then click **OK** to save your changes.
6. Restart the computer.

7 Device Access Manager for HP ProtectTools

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

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

Starting background service

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

Simple configuration

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

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

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

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

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

5. Click **OK**.

Device class configuration (advanced)

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

Adding a user or a group

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

Removing a user or a group

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

Denying access to a user or group

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

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

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

To allow access to one user but not the group:

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

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

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

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

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

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Device Access Manager**, and then click **Device Class Configuration**.
3. In the device list, click the device class that you want to configure, and then navigate to the folder below that.
4. Under **User/Groups**, add the group to be denied access.
5. Click **Deny** next to the group to be denied access.
6. Navigate to the specific device to be allowed for the user in the device list.
7. Click **Add**. The Select Users or Groups dialog box opens.
8. Select **Advanced > Find Now** to search for users or groups to add.
9. Click a user to be allowed access, and then click **OK**.
10. Click **Allow** to grant this user access.
11. Click **Apply**, and then click **OK**.

Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Emergency recovery archive Protected storage area that allows the re-encryption of basic user keys from one platform owner key to another.

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

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

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

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

Migration A task that allows the management, restoration, and transfer of keys and certificates.

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

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

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

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

Reboot Process of restarting the computer.

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

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

Smart card administrator password Password that links an administrator smart card with the computer in Computer Setup for identification at startup or restart. This password can be set manually by the administrator or randomly generated.

Smart card user password Password that links a user smart card with the computer in Computer Setup for identification at startup or restart. This password can be set manually by the administrator or randomly generated.

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

Trusted Platform Module (TPM) embedded security chip (select models only) Integrated security chip that can protect highly sensitive user information from malicious attackers. It is the root-of-trust in a given platform. The TPM provides cryptographic algorithms and operations that meets the Trusted Computing Group (TCG) specifications.

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

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

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

Index