ProtectTools

User Guide

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

First Edition: January 2007

Document Part Number: 438371-001

Table of contents

1 Introduction to security

- HP ProtectTools features 2
- Accessing HP ProtectTools Security 3
- Achieving key security objectives 4
  - Protecting against targeted theft 4
  - Restricting access to sensitive data 4
  - Preventing unauthorized access from internal or external locations 5
  - Creating strong password policies 5
- Additional security elements 6
  - Assigning security roles 6
  - Managing HP ProtectTools passwords 6
    - Creating a secure password 8
  - HP ProtectTools Backup and Restore 8
    - Backing up credentials and settings 8
    - Restoring credentials 10
    - Configuring settings 10

2 Credential Manager for HP ProtectTools

- Setup procedures 12
  - Logging on to Credential Manger 12
    - Using the Credential Manager Logon Wizard 12
    - Logging on for the first time 13
  - Registering credentials 13
    - Registering fingerprints 13
      - Setting up the fingerprint reader 14
      - Using your registered fingerprint to log on to Windows 14
    - Registering a Java Card, USB eToken, or virtual token 14
    - Registering a USB eToken 14
    - Registering other credentials 14
- General tasks 15
  - Creating a virtual token 15
  - Changing the Windows logon password 15
  - Changing a token PIN 15
  - Managing identity 16
    - Clearing an identity from the system 16
  - Locking the computer 17
  - Using Windows Logon 17
    - Logging on to Windows with Credential Manager 17
    - Adding an account 18

Removing an account 18
Using Single Sign On 18
Registering a new application 18
Using automatic registration 18
Using manual (drag and drop) registration 19
Managing applications and credentials 19
Modifying application properties 19
Removing an application from Single Sign On 19
Exporting an application 20
Importing an application 20
Modifying credentials 20
Using Application Protection 21
Restricting access to an application 21
Removing protection from an application 21
Changing restriction settings for a protected application 22
Advanced tasks (administrator only) 23
Specifying how users and administrators log on 23
Configuring custom authentication requirements 24
Configuring credential properties 24
Configuring Credential Manager settings 25
Example 1—Using the “Advanced Settings” page to allow Windows logon from Credential Manager 25
Example 2—Using the “Advanced Settings” page to require user verification before Single Sign On 26

3 Embedded Security for HP ProtectTools
Setup procedures 28
Enabling the embedded security chip 28
Initializing the embedded security chip 29
Setting up the basic user account 30
General tasks 31
Using the Personal Secure Drive 31
Encrypting files and folders 31
Sending and receiving encrypted e-mail 31
Changing the Basic User Key password 32
Advanced tasks 33
Backing up and restoring 33
Creating a backup file 33
Restoring certification data from the backup file 33
Changing the owner password 34
Resetting a user password 34
Enabling and disabling Embedded Security 34
Permanently disabling Embedded Security 34
Enabling Embedded Security after permanent disable 34
Migrating keys with the Migration Wizard 35

4 Java Card Security for HP ProtectTools
General tasks 38
Changing a Java Card PIN 38
Selecting the card reader 38

Advanced tasks (administrators only) 39
Assigning a Java Card PIN 39
Assigning a name to a Java Card 40
Setting power-on authentication 40
Enabling Java Card power-on authentication and creating an administrator Java Card 41
Creating a user Java Card 42
Disabling Java Card power-on authentication 42

5 BIOS Configuration for HP ProtectTools
General tasks 44
Managing boot options 44
Enabling and disabling system configuration options 45
Advanced tasks 47
Managing HP ProtectTools add-on module settings 47
Enabling and disabling smart card power-on authentication support 47
Enabling and disabling power-on authentication support for Embedded Security 48
Enabling and disabling Automatic DriveLock hard drive protection 49
Managing Computer Setup passwords 49
Setting the power-on password 50
Changing the power-on password 50
Setting the setup password 50
Changing the setup password 51
Setting password options 51
Enabling and disabling stringent security 51
Enabling and disabling power-on authentication on Windows restart 51

6 Device Access Manager for HP ProtectTools
Starting background service 54
Simple configuration 55
Device class configuration (advanced) 56
Adding a user or a group 56
Removing a user or a group 56
Denying access to a user or group 56
Allowing access to a device class for one user of a group 56
Allowing access to a specific device for one user of a group 57

7 Drive Encryption for HP ProtectTools
Encryption management 60
User management 61
Recovery 62

8 Troubleshooting
Credential Manager for HP ProtectTools 63
Embedded Security for HP ProtectTools 66
Device Access Manager for HP ProtectTools 72
Miscellaneous 73

Glossary 77

Index 79

1 Introduction to security

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

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

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

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

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

HP ProtectTools features

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

Module	Key features
Credential Manager for HP ProtectTools	● Credential Manager acts as a personal password vault. ● Single Sign On remembers multiple passwords for various password-protected Web sites, applications, and network resources. ● Single Sign On offers additional protection by requiring combinations of different security technologies, such as a Java™ Card and biometrics, for user authentication. ● Password storage is protected through encryption and can be hardened through the use of a TPM embedded security chip and/or security device authentication, such as Java Cards or biometrics.
Embedded Security for HP ProtectTools	● Embedded Security uses a Trusted Platform Module (TPM) embedded security chip to help protect against unauthorized access to sensitive user data or credentials stored locally on a PC. ● Embedded Security allows creation of a personal secure drive (PSD) for protecting user data. ● Embedded Security supports third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations.
Java Card Security for HP ProtectTools	● Java Card Security configures the HP ProtectTools Java Card for user authentication before the operating system loads. ● Java Card Security configures separate Java Cards for an administrator and a user.
BIOS Configuration for HP ProtectTools	● BIOS Configuration provides access to power-on user and administrator password management. ● BIOS Configuration provides an alternative to the pre-boot BIOS configuration utility known as f10 Setup. ● DriveLock, enhanced with the embedded security chip, helps protect a hard drive from unauthorized access, even if it is removed from a system, without requiring the user to remember any additional passwords beyond the embedded security chip user password.
Device Access Manager for HP ProtectTools	● Device Access Manager allows IT managers to control access to devices based on user profiles. ● Device Access Manager prevents unauthorized users from removing data using external storage media and from introducing viruses into the system from external media. ● The administrator can disable access to writeable devices for specific individuals or groups of users.
Drive Encryption for HP ProtectTools	● Drive Encryption provides complete, full-volume hard drive encryption. ● Drive Encryption forces pre-boot authentication in order to decrypt and access the data.

Accessing HP ProtectTools Security

To access HP ProtectTools Security from 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 on page 17."

Achieving key security objectives

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

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

Protecting against targeted theft

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

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. See the following procedures:
  - "Enabling and disabling smart card power-on authentication support on page 47"
  - "Enabling and disabling power-on authentication support for Embedded Security on page 48"
  - "Assigning a name to a Java Card on page 40"
  - "Drive Encryption for HP ProtectTools on page 59"
- DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system. See "Enabling and disabling Automatic DriveLock hard drive protection on page 49."
- The Personal Secure Drive feature, provided by the Embedded Security for HP ProtectTools module, encrypts sensitive data to help ensure it cannot be accessed without authentication. See the following procedures:
  - Embedded Security "Setup procedures on page 28"
  - "Using the Personal Secure Drive on page 31"

Restricting access to sensitive data

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

- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be printed or copied from the hard drive onto removable media. See "Device class configuration (advanced) on page 56."
- The DriveLock helps ensure that data cannot be accessed even if the hard drive is removed and installed into an unsecured system. See "Enabling and disabling Automatic DriveLock hard drive protection on page 49."

Preventing unauthorized access from internal or external locations

If a PC containing confidential data and customer information is accessed from an internal or external location, unauthorized users may be able to gain entry to corporate network resources or data from financial services, an executive, or R&D team, or private information such as patient records or personal financial data. The following features help prevent unauthorized access:

- The pre-boot authentication feature, if enabled, helps prevent access to the operating system. See the following procedures:
  - "Enabling and disabling smart card power-on authentication support on page 47"
  - "Enabling and disabling power-on authentication support for Embedded Security on page 48"
  - "Assigning a name to a Java Card on page 40"
  - "Drive Encryption for HP ProtectTools on page 59"
- Embedded Security for HP ProtectTools helps protect sensitive user data or credentials stored locally on a PC using the following procedures:
  - Embedded Security "Setup procedures on page 28"
  - "Using the Personal Secure Drive on page 31"
- Using the following procedures, Credential Manager for HP ProtectTools helps ensure that an unauthorized user cannot get passwords or access to password-protected applications:
  - Credential Manager "Setup procedures on page 12"
  - "Using Single Sign On on page 18"
- Device Access Manager for HP ProtectTools allows IT managers to restrict access to writeable devices so sensitive information cannot be copied from the hard drive. See "Simple configuration on page 55."
- The Personal Secure Drive feature encrypts sensitive data to help ensure it cannot be accessed without authentication using the following procedures:
  - Embedded Security "Setup procedures on page 28"
  - "Using the Personal Secure Drive on page 31"

Creating strong password policies

If a mandate goes into effect that requires the use of strong password policy for dozens of Web-based applications and databases, Credential Manager for HP ProtectTools provides a protected repository for passwords and Single Sign On convenience using the following procedures:

- Credential Manager "Setup procedures on page 12"
- "Using Single Sign On on page 18"

For stronger security, Embedded Security for HP ProtectTools then protects that repository of user names and passwords. This allows users to maintain multiple strong passwords without having to write them down or try to remember them. See Embedded Security "Setup procedures on page 28."

Additional security elements

Assigning security roles

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

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

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

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

  NOTE: Many of the features in HP ProtectTools can be customized by the security officer in cooperation with HP. For more information, see the HP Web site at http://www.hp.com.

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

Managing HP ProtectTools passwords

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

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

HP ProtectTools password	Set in this HP ProtectTools module	Function
Credential Manager logon password	Credential Manager	This password offers 2 options: • It can be used in a separate logon to access Credential Manager after logging on to Windows. • It can be used in place of the Windows logon process, allowing access to Windows and Credential Manager simultaneously.
Credential Manager recovery file password	Credential Manager, by IT administrator	Protects access to the Credential Manager recovery file.
Basic User Key password **NOTE:** Also known as: Embedded Security password	Embedded Security	Used to access Embedded Security features, such as secure e-mail, file, and folder encryption. When used for power-on authentication, also protects access to the computer contents when the computer is

HP ProtectTools password	Set in this HP ProtectTools module	Function
		turned on, restarted, or restored from hibernation.
Emergency Recovery Token password **NOTE:** Also known as: Emergency Recovery Token Key password	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the embedded security chip.
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.
Java™ Card PIN	Java Card Security	Protects access to the Java Card contents and authenticates users of the Java Card. When used for power-on authentication, the Java Card PIN also protects access to the Computer Setup utility and to the computer contents. Authenticates users of Drive Encryption, if the Java Card token is selected.
Computer Setup password **NOTE:** Also known as BIOS administrator, f10 Setup, or Security Setup password	BIOS Configuration, by IT administrator	Protects access to the Computer Setup utility.
Power-on password	BIOS Configuration	Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
Windows Logon password	Windows Control Panel	Can be used for manual logon or saved on the Java Card.

Creating a secure password

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

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

HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore provides a convenient and quick way to back up and restore credentials from all supported HP ProtectTools modules.

Backing up credentials and settings

You can back up credentials in the following ways:

- Use the HP ProtectTools Backup Wizard to select and back up HP ProtectTools modules
- Back up preselected HP ProtectTools modules

  NOTE: You must set backup options before you can use this method.

- Schedule backups

  NOTE: You must set backup options before you can use this method.

Using the HP ProtectTools Backup Wizard to select and back up HP ProtectTools modules

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **HP ProtectTools**, and then click **Backup and Restore**.
3. In the right pane, click **Backup Options**. The HP ProtectTools Backup Wizard opens. Follow the on-screen instructions to back up credentials.

Setting backup options

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **HP ProtectTools**, and then click **Backup and Restore**.
3. In the right pane, click **Backup Options**. The HP ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.
5. After you set and confirm the **Storage File Password**, select **Remember all passwords and authentication values for future automated backups**.
6. Click **Save Settings**, and then click **Finish**.

Backing up preselected HP ProtectTools modules

NOTE: You must set backup options before you can use this method.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **HP ProtectTools**, and then click **Backup and Restore**.
3. In the right pane, click **Backup**.

Scheduling backups

NOTE: You must set backup options before you can use this method.

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **HP ProtectTools**, and then click **Backup and Restore**.
3. In the right pane, click **Schedule Backups**.
4. On the **Task** tab, select the **Enabled** check box to enable scheduled backups.
5. Click **Set Password** and type and confirm your password in the **Set Password** dialog box. Click **OK**.
6. Click **Apply**. Click the **Schedule** tab. Click the **Schedule Task** arrow and select the automatic backup frequency.
7. Under **Start time**, use the **Start time** arrows to select the exact time for the backup to begin.
8. Click **Advanced** to select a start date, an end date, and recurring task settings. Click **Apply**.

9. Click **Settings**, and select settings for **Scheduled Task Completed**, **Idle Time**, and **Power Management**.
10. Click **Apply**, and then click **OK** to close the dialog box.

Restoring credentials

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

Configuring settings

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **HP ProtectTools**, and then click **Settings**.
3. In the right pane, select your settings, and then click **OK**.

2 Credential Manager for HP ProtectTools

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

- Alternatives to passwords when logging on to Windows, such as using a Java Card or biometric reader to log on to Windows. For additional information, refer to "Registering credentials on page 13."
- Single Sign On feature that automatically remembers credentials for Web sites, applications, and protected network resources.
- Support for optional security devices, such as Java Cards and biometric readers.
- Support for additional security settings, such as requiring authentication using an optional security device to unlock the computer.

Setup procedures

Logging on to Credential 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 Java Card. For additional information, refer to "Registering credentials on page 13."

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. Follow the on-screen instructions to log on to Credential Manager.

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. Follow the on-screen instructions to complete registering your fingerprints and setting up the fingerprint reader.
3. To set up the fingerprint reader for a different Windows user, log on to Windows as that user and then repeat steps 1 and 2.

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, USB eToken, or virtual token

NOTE: You must have a card reader configured for this procedure. If you do not have a reader installed, you can register a virtual token as described in "Creating a virtual token on page 15."

1. 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. Follow the on-screen instructions.

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. Follow the on-screen instructions.

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. Follow the on-screen instructions.

General tasks

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

- 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 on page 25.”

Creating a virtual token

A virtual token works very much like a Java Card or USB eToken. 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 on page 14.”

4. Follow the on-screen instructions.

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

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 on page 25."

For added security, you can configure the Lock Workstation feature to require a Java Card, biometric reader, or token to unlock the computer. For more information, see "Configuring Credential Manager settings on page 25."

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 then click your name.
4. Type your password in the **Password** box, and then 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. Follow the on-screen instructions.

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 Java Card, a fingerprint reader, or a token before logging on to a secure site or program. This is particularly useful when logging on to programs or Web sites that contain personal information, such as bank account numbers. For more information, refer to "Configuring Credential Manager settings on page 25."

Registering a new application

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

Using automatic registration

1. Open an application that requires you to log on.
2. Click the Credential Manager SSO icon in the program or Web site password dialog box.
3. Type your password for the program or Web site, and then click **OK**. The **Credential Manager Single Sign On** dialog box opens.

4. Click **More** and select from the following options:
   - Do not use SSO for this site or application.
   - Prompt to select account for this application.
   - Fill in credentials but do not submit.
   - Authenticate user before submitting credentials.
   - Show SSO shortcut for this application.
5. Click **Yes** to complete the registration.

Using manual (drag and drop) registration

1. 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. Follow the on-screen instructions.

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**.

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**.

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. Follow the on-screen instructions.

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**.

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 selections:
   - Use AND to combine the authentication methods

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

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

Configuring credential properties

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

To configure the credentials:

1. 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. You can modify the credential using one of the following choices:
   - To register the credential, click **Register**, and then follow the on-screen instructions.
   - To delete the credential, click **Clear**, and then click **Yes** in the confirmation dialog box.
   - To modify the credential properties, click **Properties**, and then follow the on-screen instructions.
5. Click **Apply**, and then click **OK**.

Configuring Credential Manager settings

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

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

To modify Credential Manager settings:

1. 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**.

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**.
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 on page 17.”

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**.
6. Restart the computer.

3 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 perform the following tasks:

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

To initialize the embedded security chip:

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

   The HP ProtectTools Embedded Security Initialization Wizard opens.

2. Follow the on-screen instructions.

Setting up the basic user account

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

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

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

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

1. If the Embedded Security User Initialization Wizard is not open, 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. Follow the on-screen instructions.

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

General tasks

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

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

Using the Personal Secure Drive

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

Encrypting files and folders

When working with encrypted files, consider the following rules:

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

To encrypt files and folders:

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

Sending and receiving encrypted e-mail

Embedded Security enables you to send and receive encrypted e-mail, but the procedures vary depending upon the program you use to access your e-mail. For more information, refer to the Embedded Security 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**. The HP Embedded Security for ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.

Restoring certification data from the backup file

To restore data from the backup file:

1. 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**. The HP Embedded Security for ProtectTools Backup Wizard opens.
4. Follow the on-screen instructions.

Changing the owner password

To change the owner password:

1. 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. Type your owner password at the prompt, and then click **OK**.

Enabling Embedded Security after permanent disable

To enable Embedded Security after permanently disabling it:

1. 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.

4 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 card reader.

With Java Card Security, you can accomplish the following tasks:

- Access Java Card Security features
- Work with the Computer Setup utility to enable Java Card authentication in a power-on environment
- Configure separate Java Cards for an administrator and a user. A user must insert the Java Card and type a PIN before the operating system will load
- Set and change the PIN used to authenticate users of the Java Card

General tasks

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

- Change a Java Card PIN
- Select the card reader

NOTE: The card reader uses both Java Cards and smart cards. This feature is available if you have more than one 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 card reader.
4. In the right pane, click **Change**.
5. In the **Change PIN** dialog box, type the current PIN in the **Current PIN** box.
6. Type a new PIN in the **New PIN** box, and then type the PIN again in the **Confirm New PIN** box.
7. Click **OK**.

Selecting the card reader

Be sure that the correct card reader is selected in Java Card Security before using the Java Card. If the correct reader is not selected, some of the features may be unavailable or incorrectly displayed. In addition, the card reader drivers must be correctly installed, as shown in Windows Device Manager.

To select the 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 card reader.
4. In the right pane, under **Selected 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 Windows administrator privileges in order to display the "Advanced" page.

Assigning a Java Card PIN

You must assign a name and a PIN to a Java Card before it can be used in Java Card Security.

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 **Advanced**.
3. Insert a new Java Card into the card reader.
4. When the **New Card** dialog box opens, type a new name in the **New display name** box, type a new PIN in the **New PIN** box, and then type the new 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. Insert the Java Card into the card reader.

   NOTE: If you have not assigned a PIN to this card, the **New Card** dialog box opens, allowing you to type a new name and PIN.

4. In the right pane, under **Display name**, click **Change**.
5. Type a name for the Java Card in the **Name** box.
6. Type the current Java Card PIN in the **PIN** box.
7. 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. For more information, see "Enabling and disabling smart card power-on authentication support on page 47."
2. Enable Java Card power-on authentication in Java Card Security.
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. Insert the Java Card into the card reader.

   NOTE: If you have not assigned a name and PIN to this card, the **New Card** dialog box opens, allowing you to type a new name and PIN.

4. In the right pane, under **Power-on authentication**, select the **Enable** check box.
5. Type your Computer Setup password in the **Computer Setup Password** dialog box, and then click **OK**.
6. If you do not have DriveLock enabled, type 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, type your DriveLock user password in the **DriveLock password** box, and then type it again in the **Confirm password** box.

   c. Type the Java Card PIN.

   d. Click **OK**.

7. When you are prompted to create a recovery file, click **Cancel** to create a recovery file at a later time or click **OK** and follow the on-screen instructions in the HP ProtectTools Backup Wizard to create a recovery file now.

   NOTE: For more information, see “HP ProtectTools Backup and Restore on page 8.”

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. Insert a Java Card that will be used as a user card.
4. In the right pane, under **Power-on authentication**, click **Create** next to **User card identity**.
5. Type 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. Insert the administrator Java Card.
4. In the right pane, under **Power-on authentication**, clear the **Enable** check box.
5. Type a PIN for the Java Card, and then click **OK**.

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 accomplish the following objectives:

- Manage power-on passwords and administrator passwords.
- Configure other power-on authentication features, such as enabling 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. Type 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 password. For more information about setting the Computer Setup password, refer to "Setting the setup password on page 50."

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.

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. Type 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 any of the following system configuration options 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 add-on module settings

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

Enabling and disabling smart card power-on authentication support

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

NOTE: To fully enable the power-on authentication feature, you must also configure a smart card using the 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. Type 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.

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. Type 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.

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 type the TPM embedded security password at the password prompt.

The option to enable Automatic DriveLock is available only if the computer has a TPM security chip installed and initialized and no DriveLock passwords are enabled. For instructions on how to enable and initialize the TPM security chip, refer to “Enabling the embedded security chip on page 28,” and “Initializing the embedded security chip on page 29.”

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. Type 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.

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. Be sure that 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 password protects the configuration settings and system identification information in Computer Setup. After this password is set, it must be used 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.

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.

Setting the setup password

To set the Computer 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.

Changing the setup password

To change the Computer 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.

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.

Enabling and disabling power-on authentication on Windows restart

This option allows you to enhance security by requiring users to type 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.

6 Device Access Manager for HP ProtectTools

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

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

Starting background service

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

Simple configuration

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

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

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

1. 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 or a group to be added to the list of available users and groups, and then click **OK.**
7. Click **OK**.

Removing a user or a group

1. 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**, click the user or group to be denied access.
5. Click **Deny** next to the user or group to be denied access.
6. Click **Apply**, and then click **OK**.

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

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

To allow access to one user but not the group:

1. 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**.

7 Drive Encryption for HP ProtectTools

⚠ **CAUTION:** If you decide to uninstall the Drive Encryption module, you must first decrypt all encrypted drives. If you do not, you will not be able to access the data on encrypted drives unless you have registered with the Drive Encryption recovery service (see “Recovery on page 62”). Reinstalling the Drive Encryption module will not enable you to access the encrypted drives.

Encryption management

Encrypting a drive

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **Encryption Management**.
3. In the right pane, click **Activate**. The Drive Encryption for HP ProtectTools Wizard opens.
4. Follow the on-screen instructions to activate encryption.

NOTE: You will need to specify a diskette, flash storage device, or some other USB-connected storage media on which the recovery information will be stored.

Change encryption

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **Encryption Management**.
3. In the right pane, click **Change encryption**. Select the disks to encrypt in the **Change Encryption** dialog box, and then click **OK**.
4. Click **OK** again to begin encryption.

Decrypting a drive

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **Encryption Management**.
3. In the right pane, click **Deactivate**.

User management

Add a user

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **User Management**.
3. In the right pane, click **Add**. Click a user name in the **User Name** list or type a user name in the **Username** box. Click **Next**.
4. Type the Windows password for the selected user, and then click **Next**.
5. Select an authentication method for the new user, and then click **Finish**.

Remove a user

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **User Management**.
3. In the right pane, click a user name to remove in the **User Name** list. Click **Remove**.
4. Click **Yes** to confirm that you want to remove the selected user.

Change token

Change the authentication method for a user as follows:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **User Management**.
3. In the right pane, select a user name from the **User Name** list, and then click **Change Token**.
4. Type the user's Windows Password, and then click **Next**.
5. Select a new authentication method, and then click **Finish**.
6. If you selected a Java Card as the authentication method, type the Java Card password when prompted, and then click **OK**.

Set password

Set a password or change the authentication method for a user as follows:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **User Management**.
3. In the right pane, select the user from the **User Name** list, and then click **Set Password**.
4. Type the user's Windows Password, and then click **Next**.
5. Select the new authentication method, and then click **Finish**.
6. If you selected a Java Card as the authentication method, type the Java Card password when prompted, and then click **OK**.

Recovery

The following two safety measures are available to you:

- If you forget your password, you cannot access your encrypted drives. You may, however, register with the Drive Encryption recovery service to enable you to access your computer if you forget your password.
- You may back up your Drive Encryption keys on a diskette, flash storage device, or some other USB-connected storage media.

Registering with the Drive Encryption recovery service

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **Recovery**.
3. In the right pane, click **Click here to register**. Type the requested information to complete the security backup procedure.

Backing up your Drive Encryption keys

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, click **Drive Encryption**, and then click **Recovery**.
3. In the right pane, click **Click here to backup your keys**.
4. Select a diskette, flash storage device, or some other USB-connected storage media on which to save the recovery information, and then click **Next**. The Drive Encryption for HP ProtectTools Wizard opens.
5. Follow the on-screen instructions to back up the Drive Encryption keys.

NOTE: You will need to specify a diskette, flash storage device, or some other USB-connected storage media on which the recovery information will be stored.

8 Troubleshooting

Credential Manager for HP ProtectTools

Short description	Details	Solution
Using the Credential Manager Network Accounts option, a user can select which domain account to log on to. When TPM authentication is used, this option is not available. All other authentication methods work properly.	Using TPM authentication, the user is only logged on to the local computer.	Using Credential Manager Single Sign On tools allows the user to authenticate other accounts.
The USB token credential is not available with logon to Windows XP Service Pack 1.	After installing USB token software, registering the USB token credential, and setting Credential Manager as primary logon, the USB Token is neither listed nor available in the Credential Manager/ GINA logon. After logging back on to Windows, logging off Credential Manager, re-logging on to Credential Manager and reselecting the token as the primary logon, the token logon operation functions normally.	Update Windows to Service Pack 2 via Windows Update. If retaining Service Pack 1, log back on to Windows using another credential (Windows password) in order to log off and re-log back on to Credential Manager.
Some application Web pages create errors that prevent the user from performing or completing tasks.	Some Web-based applications stop functioning and report errors due to the disabling functionality pattern of Single Sign On. For example, an **!** in a yellow triangle is observed in Internet Explorer, indicating an error has occurred.	Credential Manager Single Sign On does not support all software Web interfaces. Disable Single Sign On support for the specific Web page by turning off Single Sign On support. See complete documentation on Single Sign On, which is available in the Credential Manager online Help files. If a specific Single Sign On cannot be disabled for a given application, call HP technical support and request 3rd-level support through your HP Service contact.
The option to **Browse for Virtual Token** is not displayed during the logon process.	The user cannot move the location of a registered virtual token in Credential Manager because the option to browse was removed to reduce security risks.	The browse option was removed because it allowed non-users to delete and rename files and take control of Windows.
Domain administrators cannot change Windows password even with authorization.	This happens after a domain administrator logs on to a domain and registers the domain identity with Credential Manager using an account with Administrator's rights on the domain and the local PC. When the domain	Credential Manager cannot change a domain user's account password through **Change Windows password**. Credential Manager can only change the local PC account passwords. The domain user can change his/her password through the **Windows security > Change password** option, but, since the

Short description	Details	Solution
	administrator attempts to change the Windows password from Credential Manager, the administrator gets an error logon failure: **User account restriction**.	domain user does not have a physical account on the local PC, Credential Manager can only change the password used to log on.
Credential Manager has incompatibility issues with Corel WordPerfect 12 password GINA.	If the user logs on to Credential Manager, creates a document in WordPerfect, and saves with password protection, Credential Manager cannot detect or recognize, either manually or automatically, the password GINA.	HP is researching a workaround for future product enhancements.
Credential Manager does not recognize the **Connect** button on screen.	If the Single Sign On credentials for Remote Desktop Connection (RDP) are set to **Connect**, when Single Sign On is relaunched, it always enters **Save As** instead of **Connect**.	HP is researching a workaround for future product enhancements.
Users can lose all Credential Manager credentials protected by the TPM.	If the TPM module is removed or damaged, users lose all credentials protected by the TPM.	This is as designed. The TPM Module is designed to protect the Credential Manager credentials. HP recommends that the user back up their identity from Credential Manager prior to removing the TPM module.
The user is unable to log on to Credential Manager after transitioning from sleep mode to hibernation on Windows XP Service Pack 1 only.	After allowing system to transition into hibernation and sleep mode, the Administrator or user is unable to log on to Credential Manager and the Windows logon screen remains displayed no matter which logon credential (password, fingerprint, or Java Card) is selected.	Update Windows to Service Pack 2 via Windows Update. Refer to Microsoft knowledge base article 813301 at http://www.microsoft.com for more information on the cause of the issue. In order to log on, the user must select Credential Manager and log on. After logging on to Credential Manager, the user is prompted to log on to Windows (the user may have to select the Windows logon option) to complete the logon process. If the user logs on to Windows first, then the user must manually log on to Credential Manager.
Restoring Embedded Security causes Credential Manager to fail.	Credential Manager fails to register any credentials after the ROM is restored to factory settings.	Credential Manager fails to access the TPM if the ROM is reset to factory settings after installing Credential Manager. The TPM embedded security chip can be enabled using the f10 Computer Setup utility, BIOS Configuration, or HP Client Manager. To enable the TPM embedded security chip using Computer Setup, follow these steps: 1. Open Computer Setup by turning on or restarting the computer, and then pressing f10 while the **f10 = ROM Based Setup** message is displayed in the lower-left corner of the screen. 2. Use the arrow keys to select **Security > Setup Password**. Set a password. 3. Select **Embedded Security Device**. 4. Use the arrow keys to select **Embedded Security Device—Disable**. Use the arrow keys to change it to **Embedded Security Device—Enable**. 5. Select **Enable > Save changes and exit**.

Short description	Details	Solution
		HP is investigating resolution options for future customer software releases.
The security **Restore Identity** process loses association with virtual token.	When user restores identity, Credential Manager can lose the association with the location of the virtual token at logon screen. Even though Credential Manager has the virtual token registered, the user must reregister the token to restore the association.	This is currently by design. When uninstalling Credential Manager without keeping identities, the system (server) part of the token is destroyed, so the token cannot be used anymore for logging on, even if the client part of the token is restored through identity restore. HP is investigating long-term options for resolution.

Embedded Security for HP ProtectTools

Short description	Details	Solution
Encrypting folders, subfolders, and files on PSD causes an error message.	If the user copies files and folders to the PSD and tries to encrypt folders/files or folders/subfolders, the **Error Applying Attributes** message is displayed. The user can encrypt the same files on the C:\ drive or an extra installed hard drive.	This is as designed. Moving files/folders to the PSD automatically encrypts them. There is no need to “double-encrypt” the files/ folders. Attempting to double-encrypt them on the PSD using EFS produces this error message.
Cannot Take Ownership With Another OS In MultiBoot Platform.	If a drive is set up for multiple OS boot, ownership can only be taken with the platform initialization wizard in one operating system.	This is as designed, for security reasons.
An unauthorized administrator can view, delete, rename, or move the contents of encrypted EFS folders.	Encrypting a folder does not stop an unauthorized user with administrative rights to view, delete, or move contents of the folder.	This is as designed. It is a feature of EFS, not the Embedded Security TPM. Embedded Security uses Microsoft EFS software, and EFS preserves file/folder access rights for all administrators.
The user has no encrypt options when attempting to restore the hard drive using FAT32.	If the user attempts to restore the hard drive using FAT32, there will be no encrypt options for any files/folders using EFS.	This is as designed. Software should not be installed on a restore with a FAT32 partition. Microsoft EFS is supported only on NTFS and does not function on FAT32. This is a feature of Microsoft EFS and is not related to HP ProtectTools software.
The user is able to encrypt or delete the recovery archive XML file.	By design, the ACLs for this folder are not set; therefore, a user can inadvertently or purposely encrypt or delete the file, thus making it inaccessible. After this file has been encrypted or deleted, no one can use the TPM software.	This is as designed. Users have access rights to an emergency archive so that they can save/update their Basic User Key backup copy. Users should be instructed never to encrypt or delete the recovery archive files.
Embedded Security EFS interaction with Symantec Antivirus or Norton Antivirus produces longer encryption/decryption and scan times.	Encrypted files interfere with Symantec Antivirus or Norton Antivirus 2005 virus scan. During the scan process, the Basic User password prompt asks the user for a password every 10 files or so. If the user does not type a password, the Basic User password prompt times out, allowing NAV2005 to continue with the scan. Encrypting files using Embedded Security EFS takes longer when Symantec Antivirus or Norton Antivirus is running.	To reduce the time required to scan Embedded Security EFS files, the user can either type the encryption password before scanning or decrypt before scanning. To reduce the time required to encrypt/decrypt data using Embedded Security EFS, the user should disable Auto-Protect on Symantec Antivirus or Norton Antivirus.
The emergency recovery archive cannot be saved to removable media.	If the user inserts a MultiMediaCard or Secure Digital (SD) Memory Card when creating the emergency recovery archive path during Embedded Security initialization, an error message is displayed.	This is as designed. Storage of the recovery archive on removable media is not supported. The recovery archive can be stored on a network drive or on another local drive other than the C drive.

Short description	Details	Solution
Errors occur after a power loss interrupts Embedded Security initialization.	If there is a power loss during the initialization of the Embedded Security chip, the following issues occur: ● When attempting to launch the Embedded Security Initialization Wizard, the following error message is displayed: **The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.** ● When attempting to launch the User Initialization Wizard, the following error message is displayed: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.**	Perform the following procedure to recover from the power loss: **NOTE:** Use the arrow keys to select various menus, menu items, and to change values (unless otherwise specified). 1. Start or restart the computer. 2. Press f10 when the **f10=Setup** message appears on the screen. 3. Select the appropriate language option. 4. Press enter. 5. Select **Security > Embedded Security**. 6. Set the **Embedded Security Device** option to **Enable**. 7. Press f10 to accept the change. 8. Select **File > Save Changes and Exit**. 9. Press enter. 10. Press f10 to save the changes and exit the utility.
The Computer Setup (**f10**) Utility password can be removed after enabling the TPM Module.	Enabling the TPM module requires a Computer Setup (**f10**) Utility password. When the module has been enabled, the user can remove the password. This allows anyone with direct access to the system to reset the TPM module and cause possible loss of data.	This is as designed. The Computer Setup (**f10**) Utility password can only be removed by a user who knows the password. However, HP strongly recommends having the Computer Setup (**f10**) Utility password protected at all times.
The PSD password box is no longer displayed when the system becomes active after standby status	When a user logs on to the system after creating a PSD, the TPM asks for the Basic User password. If the user does not type the password and the system initiates Standby, the password dialog box is no longer available when the user resumes.	This is by design. The user has to log off and back on to view the PSD password box again.
No password is required to change the Security Platform Policies.	Access to Security Platform Policies (both Machine and User) does not require a TPM password for users who have administrative rights on the system.	This is by design. Any administrator can modify the Security Platform Policies with or without TPM user initialization.
When a certificate is viewed, it shows as non-trusted.	After setting up HP ProtectTools and running the User Initialization Wizard, the user has the ability to view the certificate issued; however, when the certificate is viewed, it shows as non-trusted. While the certificate can be installed at this point by clicking the install button, installing it does not make it trusted.	Self-signed certificates are not trusted. In a properly configured enterprise environment, EFS certificates are issued by online Certification Authorities and are trusted.

Short description	Details	Solution
An intermittent encrypt and decrypt error occurs: **The process cannot access the file because it is being used by another process.**	This is an extremely intermittent error during file encryption or decryption which occurs because the file is being used by another process, even though that file or folder is not being processed by the operating system or other applications.	To resolve the failure: 1. Restart the system. 2. Log off. 3. Log back on.
Data loss in removable storage occurs if the storage media is removed prior to completing the new data generation or transfer.	Removing storage media such as a MultiBay hard drive still shows PSD availability and does not generate errors while adding/modifying data to the PSD. After the system is restarted, the PSD does not reflect file changes that occurred while the removable storage was unavailable.	Do not remove a PSD before data generation or transfer is complete. This issue is only experienced if the user accesses the PSD, then removes the hard drive before completing new data generation or transfer. If the user attempts to access the PSD when the removable hard drive is not present, an error message is displayed stating that **the device is not ready**.
During uninstall, if the user has not initialized the Basic User and opens the Administration tool, the **Disable** option is not available and Uninstaller will not continue until the Administration tool is closed.	The user has the option of uninstalling either without disabling the TPM or by first disabling the TPM (through the Administration tool), and then uninstalling. Accessing the Administration tool requires Basic User Key initialization. If basic initialization has not occurred, all options are inaccessible to the user. Since the user has explicitly chosen to open the Administration tool (by clicking **Yes** in the dialog box prompting **Click Yes to open Embedded Security Administration tool**), uninstall waits until the Administration tool is closed. If the user clicks **No** in that dialog box, the Administration tool does not open at all and uninstall proceeds.	The Administration tool is used for disabling the TPM chip, but that option is not available unless the Basic User Key has already been initialized. If it has not been initialized, select **OK** or **Cancel** to continue with the uninstallation.
Intermittent system lockup occurs after creating PSD on 2-user accounts and using fast-user-switching in 128-MB system configurations.	The system may lock up with a black screen and nonresponding keyboard and mouse instead of showing welcome (logon) screen when using fast-switching with minimal RAM.	The root cause is suspected to be a timing issue in low memory configurations. Integrated graphics uses UMA architecture taking 8 MB of memory, which leaves only 120 MB available to the user. The error is generated when this 120 MB is shared by both users who are logged on and are fast-user-switching. The workaround is to reboot the system and increase memory configuration (HP does not ship 128-MB configurations with security modules).
EFS User Authentication (password request) times out with **access denied**.	The EFS User Authentication password reopens after the user clicks **OK** or the system exits Standby.	This is by design—to avoid issues with Microsoft EFS, a 30-second watchdog timer was created to generate the error message).
Minor truncation during setup of Japanese is observed in functional descriptions.	Functional descriptions during custom setup option during installation wizard are truncated.	HP will correct this in a future release.
EFS Encryption works without a password being typed in the prompt.	By allowing the prompt for User password to time out, encryption is still available on a file or folder.	The ability to encrypt does not require password authentication, since this is a feature of the Microsoft EFS encryption. Decryption will require the user password to be supplied.

Short description	Details	Solution
Secure e-mail is supported, even when secure e-mail is not specified in the User Initialization Wizard or when secure e-mail configuration is disabled in user policies.	Embedded security software and the wizard do not control settings of an e-mail client (Outlook, Outlook Express, or Netscape).	This behavior is as designed. Configuration of TPM e-mail settings does not prohibit editing encryption settings directly in an e-mail client. Usage of secure e-mail is set and controlled by 3rd-party applications. The HP wizard allows linkage to the three reference applications for immediate customization.
Running Large Scale Deployment a second time on the same PC or on a previously initialized PC overwrites Emergency Recovery and Emergency Token files. The new files are useless for recovery.	Running Large Scale Deployment on any previously initialized HP ProtectTools Embedded Security system renders existing Recovery Archives and Recovery Tokens useless by overwriting those XML files.	HP is working to resolve the XML-file-overwrite issue and will provide a solution in a future SoftPaq.
Automated logon scripts do not function during user restore in Embedded Security.	The error occurs after the user performs the following actions: ● Initializes owner and user in Embedded Security (using the default locations—**My Documents**). ● Resets the chip to factory settings in the BIOS. ● Reboots the computer. ● Begins to restore Embedded Security. During the restore process, Credential Manager asks if the system can automate the logon to Infineon TPM User Authentication. If the user selects **Yes**, the location of SPEmRecToken is automatically displayed in the text box. Even though this location is correct, the following error message is displayed: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.**	Click the **Browse** button on the screen to select the location, and the restore process proceeds.
Multiple-User PSDs do not function in a fast-user-switching environment.	This error occurs when multiple users have been created and given a PSD with the same drive letter. If an attempt is made to fast-user-switch between users when the PSD is loaded, the second user's PSD is unavailable.	The second user's PSD will be available only if it is reconfigured to use another drive letter or if the first user is logged off.
The PSD is disabled and cannot be deleted after formatting the hard drive on which the PSD was generated.	The PSD icon is still visible, but the error message **drive is not accessible** is displayed when the user attempts to access the PSD. The user is not able to delete the PSD and the following message is displayed: **your PSD is still in use, please be sure that your PSD contains**	As designed: If a customer force-deletes or disconnects from the storage location of the PSD data, the Embedded Security PSD drive emulation continues to function and will produce errors based on lack of communication with the missing data. Resolution: After the next reboot, the emulations fail to load and user can delete the old PSD emulation and create a new PSD.

Short description	Details	Solution
	no open files and is not accessed by another process. The user must reboot the system in order to delete the PSD and it is not loaded after reboot.	
An internal error is detected when the user is restoring from the Automatic Backup Archive.	In Embedded Security, if the user clicks the **Restore under Backup** option to restore from the automatic backup Archive and then selects **SPSystemBackup.xml**, the Restore Wizard fails and the following error message is displayed: **The selected Backup Archive does not match the restore reason. Please select another archive and continue.**	If the user selects **SpSystemBackup.xml** when the SpBackupArchive.xml is required, the Embedded Security Wizard fails and displays the following message: **An internal Embedded Security error has been detected.** The user must select the correct XML file to match the required reason. The processes are working as designed and function properly; however, the internal Embedded Security error message is not clear and should state a more appropriate message. HP is working to enhance this in future products.
The security system exhibits a restore error with multiple users.	During the restore process, if the administrator selects users to restore, the users not selected are not able to restore the keys when trying to restore at a later time. A **decryption process failed** error message is displayed.	The non-selected users can be restored by resetting the TPM, running the restore process, and selecting all users before the next default daily backup runs. If the automated backup runs, it overwrites the non-restored users and their data is lost. If a new system backup is stored, the previous unselected users cannot be restored. Also, the user must restore the entire system backup. An Archive Backup can be restored individually.
Resetting System ROM to default hides the TPM.	Resetting the system ROM to default hides the TPM to Windows. This does not allow the security software to operate properly and makes TPM-encrypted data inaccessible.	Unhide the TPM in BIOS: Open the Computer Setup (**f10**) Utility, navigate to **Security > Device security**, and then modify the field from **Hidden** to **Available**.

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

Device Access Manager for HP ProtectTools

Short description	Details	Solution
Users have been denied access to devices within Device Access Manager, but the devices are still accessible.	Simple Configuration and/or Device Class Configuration have been used within Device Access Manager to deny users access to devices. Despite being denied access, users can still access the devices.	Verify that the HP ProtectTools Device Locking service has started. As an administrative user, browse to **Control Panel > Administrative Tools > Services**. In the **Services** window, search for the **HP ProtectTools Device Locking/Auditing** service. Be sure that the service is started and that the startup type is **Automatic**.
A user has unexpected access to a device or a user is unexpectedly denied access to a device.	Device Access Manager has been used to deny users access to some devices and allow users access to other devices. When the user is using the system, they can access devices they believe Device Access Manager has denied and are denied access to devices they believe Device Access Manager should allow.	The Device Class Configuration within Device Access Manager should be used to investigate the Users device settings. Select **Security Manager > Device Access Manager > Device Class Configuration**. Expand the levels in the Device Class tree and review the settings applicable to the User. Check for any “Deny” permissions that may be set on the user or any Windows Group of which they may be a member, e.g., Users, Administrators.
Allow or deny—which takes precedence?	Within Device Class Configuration, the following configuration has been set: ● The Allow permission has been granted to a Windows group (e.g., BUILTIN\Administrators) and the Deny permission has been granted to another Windows group (e.g., BUILTIN\Users) at the same level in the device class hierarchy (e.g., DVD/CD-ROM Drives). If a user is a member of both those groups (e.g., Administrator), which takes precedence?	The user is denied access to the device. Deny takes precedence over Allow. Access is denied due to the way in which Windows works out the effective permission for the device. One group is denied, and one group is allowed, but the user is a member of both groups. The user is denied because denying access is given precedence over allowing access. One workaround is to deny the Users group at the DVD/CD-ROM Drives level and to allow the Administrators group at the level below DVD/CD-ROM Drives. A further workaround would be to have specific Windows groups, one for allowing access to DVD/CD and one for denying access to DVD/CD. Specific users would then be added to the appropriate group.

Miscellaneous

Software Impacted—Short description	Details	Solution
Security Manager—Warning received: **The security application can not be installed until the HP Protect Tools Security Manager is installed**.	All security applications such as Embedded Security, Java Card Security, and biometrics are extendable plug-ins for the Security Manager interface. Security Manager must be installed before an HP-approved security plug-in can be loaded.	The Security Manager software must be installed before installing any security plug-in.
TPM Firmware Update Utility for models containing Broadcom-enabled TPMs—The tool provided through HP support Web site reports **ownership required**.	This is the expected behavior of the TPM firmware utility for models containing Broadcom-enabled TPMs. The firmware upgrade tool allows the user to upgrade the firmware, with or without an endorsement key (EK). When there is no EK, no authorization is required to complete the firmware upgrade. When there is an EK, a TPM owner must exist, since the upgrade requires owner authorization. After the successful upgrade, the platform must be restarted for the new firmware to take effect. If the BIOS TPM is factory-reset, ownership is removed and firmware update capability is prevented until the Embedded Security Software platform and User Initialization Wizard have been configured. **NOTE:** A reboot is always recommended after performing a firmware update. The firmware version is not identified correctly until after the reboot.	1. Reinstall Embedded Security Software. 2. Run the Platform and User Configuration Wizard. 3. Be sure that the system contains Microsoft .NET framework 1.1 installation: a. Click **Start**. b. Click **Control Panel**. c. Click **Add or remove programs**. d. Be sure that **Microsoft .NET Framework 1.1** is listed. 4. Check the hardware and software configuration: a. Click **Start**. b. Click **All Programs**. c. Click **HP ProtectTools Security Manager**. d. Select **Embedded Security** from the tree menu. e. Click **More Details**. The system should have the following configuration: ● Product version = V4.0.1 ● Embedded Security State: Chip State = Enabled, Owner State = Initialized, User State = Initialized ● Component Info: TCG Spec. Version = 1.2 ● Vendor = Broadcom Corporation ● FW Version = 2.18 (or greater) ● TPM Device driver library version 2.0.0.9 (or greater) 5. If the FW version does not match 2.18, download and update the TPM firmware. The TPM Firmware SoftPaq is a support download available on the HP Web site at http://www.hp.com.
HP ProtectTools Security Manager—Intermittently,	Intermittently (1 in 12 instances), an error is created by using the close button in the	This is related to a timing dependency on plug-in services load time when closing and restarting Security

Software Impacted—Short description	Details	Solution
an error is returned when closing the Security Manager interface.	upper right of the screen to close Security Manager before all plug-in applications have finished loading.	Manager. Since PTHOST.exe is the shell housing the other applications (plug-ins), it depends on the ability of the plug-in to complete its load time (services). Closing the shell before the plug-in has had time to complete loading is the root cause. Allow Security Manager to complete the services loading message (seen at top of Security Manager window) and all plug-ins listed in left column. To avoid failure, allow a reasonable time for these plug-ins to load.
HP ProtectTools—Unrestricted access or uncontrolled administrator privileges pose security risk.	Numerous risks are possible with unrestricted access to the client PC, including the following: ● Deletion of PSD ● Malicious modification of user settings ● Disabling of security policies and functions	Administrators are encouraged to follow “best practices” in restricting end-user privileges and restricting user access. Unauthorized users should not be granted administrative privileges.
The BIOS and OS Embedded Security passwords are out of synch.	If a user does not validate a new password as the BIOS Embedded Security password, the BIOS Embedded Security password reverts back to the original embedded security password through **f10** BIOS.	This is functioning as designed; these passwords can be re-synchronized by changing the OS Basic User password and authenticating it at the BIOS Embedded Security password prompt.
Only one user can log on to the system after TPM preboot authentication is enabled in BIOS.	The TPM BIOS PIN is associated with the first user who initializes the user setting. If a computer has multiple users, the first user is, in essence, the administrator. The first user will have to give his TPM user PIN to other users to use to log on.	This is functioning as designed; HP recommends that the customer's IT department follow good security policies for rolling out their security solution and ensuring that the BIOS administrator password is configured by IT administrators for system level protection.
The user has to change their PIN to make TPM preboot work after a TPM factory reset.	The user has to change their PIN or create another user to initialize their user setting to make TPM BIOS authentication work after reset. There is no option to make TPM BIOS authentication work.	This is as designed; the factory reset clears the Basic User Key. The user must change his user PIN or create a new user to re-initialize the Basic User Key.
Power-on authentication support is not set to default using Embedded Security **Reset to Factory Settings**	In Computer Setup, the **Power-on authentication support** option is not being reset to factory settings when using the Embedded Security Device option **Reset to Factory Settings**. By default, **Power-on authentication support** is set to **Disable**.	The **Reset to Factory Settings** option disables Embedded Security Device, which hides the other Embedded Security options (including **Power-on authentication support**). However, after reenabling Embedded Security Device, **Power-on authentication support** remains enabled. HP is working on a resolution, which will be provided in future Web-based ROM SoftPaq offerings.

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

Glossary

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 Java Card Security that, when enabled, requires the use of a Java Card and a valid PIN for user authentication.

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

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 type the DriveLock password when the computer starts up.

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

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

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

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 Java 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.

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 Java Card or biometric reader, it is used to authenticate the owner to a computer.

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

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

Index

A

access
- controlling 53
- preventing unauthorized 5

accessing HP ProtectTools Security 3

account
- basic user 30
- Credential Manager 13

administrator tasks
- Credential Manager 23
- Java Card 39

advanced tasks
- BIOS Configuration 47
- Credential Manager 23
- Device Access Manager 56
- Embedded Security 33
- Java Card 39

Automatic DriveLock 49

B

background service, Device Access Manager 54

backing up and restoring
- certification information 33
- Embedded Security 33
- HP ProtectTools modules 8
- Single Sign On data 20

basic user account 30

Basic User Key password
- changing 32
- setting 30

biometric readers 14

BIOS administrator password 7

BIOS Configuration for HP ProtectTools
- add-on module settings, managing 47
- Automatic DriveLock 49
- boot options 44
- password options, setting 51
- power-on authentication 48
- power-on authentication on Windows restart 51
- power-on password, changing 50
- power-on password, setting 50
- setup password, changing 51
- setup password, setting 50
- smart card power-on authentication 47
- stringent security 51
- system configuration options 45

BIOS setup password
- changing 51
- setting 50

boot options 44

C

Computer Setup
- administrator password 7
- password, changing 51
- password, setting 50
- passwords, managing 49

controlling device access 53

Credential Manager for HP ProtectTools
- account, adding 18
- account, removing 18
- administrator tasks 23
- application protection 21
- application protection, removing 21
- changing application restriction setting 22
- credential properties, configuring 24
- credentials, registering 13
- custom authentication requirements 24
- fingerprint log on 14
- fingerprint reader 14
- identity 16
- identity, clearing 16
- identity, removing 16
- locking computer 17
- logging on 12
- logon password 6
- logon specifications 23
- logon wizard 12
- new account, creating 13
- recovery file password 6
- registering fingerprints 13
- registering Java Card 14
- registering other credentials 14
- registering token 14
- registering virtual token 14
- restriction application access 21
- settings, configuring 25
- setup procedures 12
- Single Sign On (SSO) 18
- SSO application, exporting 20
- SSO application, importing 20
- SSO application, modifying properties 19
- SSO application, removing 19
- SSO applications and credentials 19
- SSO automatic registration 18
- SSO credentials, modifying 20
- SSO manual registration 19
- SSO new application 18
- token PIN, changing 15
- troubleshooting 63

USB eToken, registering 14
user verification 26
virtual token, creating 15
Windows Logon 17
Windows logon password, changing 15
Windows logon, allow 25

D
data, restricting access to 4
decrypting a drive 59
Device Access Manager for HP ProtectTools
background service 54
device class configuration 56
device class, allowing access to one 56
device, allowing access to one 57
simple configuration 55
troubleshooting 72
user or group, adding 56
user or group, denying access to 56
user or group, removing 56
device options 45
disabling
Automatic DriveLock 49
device options 45
Embedded Security 34
Embedded Security, permanently 34
Java Card power-on authentication 42
power-on authentication 47
smart card authentication 47
stringent security 51
Drive Encryption for HP ProtectTools
adding a user 61
changing a token 61
changing authentication 61
changing encryption 60
decrypting a drive 60
Drive Encryption keys 62
Drive Encryption recovery service 62
encrypting a drive 60
removing a user 61
setting a password 61

E
Embedded Security for HP ProtectTools
backup file, creating 33
basic user account 30
Basic User Key 30
Basic User Key password, changing 32
certification data, restoring 33
enabling after permanent disable 34
enabling and disabling 34
enabling TPM chip 28
encrypted e-mail 31
encrypting files and folders 31
initializing chip 29
migrating keys 35
owner password, changing 34
password 6
permanently disabling 34
Personal Secure Drive 31
resetting user password 34
setup procedures 28
troubleshooting 66
emergency recovery 29
emergency recovery token password
definition 7
setting 29
enabling
Automatic DriveLock 49
device options 45
Embedded Security 34
Embedded Security after permanent disable 34
Java Card power-on authentication 41
power-on authentication 47
smart card authentication 47
stringent security 51
TPM chip 28
encrypting a drive 59
encrypting files and folders 31
encryption
methods 60
user authentication 61
users 61

F
f10 Setup password 7
features, HP ProtectTools 2
fingerprints, Credential Manager 13

H
HP ProtectTools Backup and Restore 8
HP ProtectTools features 2
HP ProtectTools Security, accessing 3

I
identity, managing
Credential Manager 16
identity, removing
Credential Manager 16
initializing embedded security chip 29

J
Java Card Security for HP ProtectTools
administrator tasks 39
advanced tasks 39
assigning name 40
creating administrator 41
Credential Manager 14
PIN 7
PIN, assigning 39
PIN, changing 38
power-on authentication, disabling 42
power-on authentication, enabling 41
power-on authentication, setting 40
reader, selecting 38
user, creating 42

K
key security objectives 4

L
locking computer 17

N
network account 18

O
objectives, security 4

owner password
  changing 34
  definition 7
  setting 29

P
password
  Basic User Key 32
  changing owner 34
  changing power-on 50
  changing setup 51
  Computer Setup, managing 49
  emergency recovery token 29
  guidelines 8
  HP ProtectTools 6
  managing 6
  owner 29
  policies, creating 5
  resetting user 34
  secure, creating 8
  setting options 51
  setting power-on 50
  setting setup 50
  Windows logon 15
personal secure drive (PSD) 31
power-on authentication
  enabling and disabling 47
  on Windows restart 51
power-on password
  definition 7
  setting and changing 50
properties
  application 19
  authentication 23
  credential 24

R
recovering encrypted data 62
registering
  application 18
  credentials 13
restricting
  access to sensitive data 4
  device access 53

S
security
  key objectives 4
  roles 6
security roles 6
security setup password 7
Single Sign On
  automatic registration 18
  exporting applications 20
  manual registration 19
  modifying application properties 19
  removing applications 19
stringent security 51

T
targeted theft, protecting against 4
token, Credential Manager 14
TPM chip
  enabling 28
  initializing 29
troubleshooting
  Credential Manager 63
  Device Access Manager 72
  Embedded Security 66
  miscellaneous 73

U
unauthorized access, preventing 5
USB eToken, Credential Manager 14

V
virtual token 15
virtual token, Credential Manager 14, 15

W
Windows Logon
  Credential Manager 17
  password 7
Windows network account 18