

# HP ProtectTools Security Manager Guide

---

HP Compaq Business Desktops



© Copyright 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Microsoft and Windows are trademarks of Microsoft Corporation in the U.S. and other countries.

Intel and SpeedStep are trademarks of Intel Corporation in the U.S. and other countries.

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.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company.

HP ProtectTools Security Manager Guide

HP Compaq Business Desktops

First Edition (August 2006)

Document Part Number: 431330-001

## About This Book

This guide provides instructions for configuring and using HP ProtectTools Security Manager.



---

**WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

---



---

**CAUTION** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

---



---

**NOTE** Text set off in this manner provides important supplemental information.

---



# Table of contents

## 1 Introduction

HP ProtectTools Security Manager .....	1
Accessing the ProtectTools Security Manager .....	1
Understanding Security Roles .....	2
Managing ProtectTools Passwords .....	2
Multifactor Authentication Credential Manager Logon .....	5
Creating a Secure Password .....	5
Advanced Tasks .....	6
Managing ProtectTools Settings .....	6
Enabling and Disabling Java Card Power-On Authentication Support .....	6
Enabling and Disabling Power-On Authentication Support for Embedded Security .....	6
Managing Computer Setup Passwords .....	7
Setting the Power-On Password (if available) .....	7
Changing the Power-On Password (if available) .....	7
System Setup .....	8
Changing Power-On Authentication Support .....	8
Changing User Accounts .....	8
Setting the Computer Setup Administrator Password .....	9
Changing the Computer Setup Administrator Password .....	9
Dictionary Attack Behavior with Power-On Authentication .....	10
Dictionary Attack Defense .....	10

## 2 HP BIOS Configuration for ProtectTools

Basic Concepts .....	11
Changing BIOS Settings .....	11

## 3 HP Embedded Security for ProtectTools

Basic Concepts .....	13
Setup Procedures .....	14

## 4 HP Credential Manager for ProtectTools

Basic Concepts .....	15
Launch Procedure .....	15
Logging On for the First Time .....	16

## 5 HP Java Card Security for ProtectTools

Basic Concepts .....	17
----------------------	----

**6 Third-Party Solutions**

**7 HP Client Manager for Remote Deployment**

Background ..... 21  
Initialization ..... 21  
Maintenance ..... 21

**8 Troubleshooting**

Credential Manager for ProtectTools ..... 23  
Embedded Security for ProtectTools ..... 27  
Miscellaneous ..... 33

**Glossary ..... 37**

**Index ..... 41**

# 1 Introduction

## HP ProtectTools Security Manager

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 modules:

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

The modules available for the computer may vary, depending on the model. ProtectTools modules may be preinstalled, supplied on CD that shipped with the computer, or available for purchase from the HP Web site. Visit <http://www.hp.com> for more information.



---

**NOTE** Refer to the ProtectTools Help screens for specific instructions for the ProtectTools modules.

---

To use the Trusted Platform Module (TPM), platforms containing a TPM require both a TCG Software Stack (TSS) and embedded security software. Some models provide the TSS; if the TSS is not provided, it can be purchased from HP. Additionally, TPM-enabling software must be purchased separately for some models. Please see [Third-Party Solutions](#) for more details.

## Accessing the ProtectTools Security Manager

To access the ProtectTools Security Manager from the Microsoft Windows Control Panel:

- ▲ Windows XP: Click **Start > Control Panel > Security Center > ProtectTools Security Manager**.
- ▲ Windows 2000: Click **Start > All Programs > HP ProtectTools Security Manager**.



---

**NOTE** After you have configured the Credential Manager module, you can also log in to Credential Manager directly from the Windows logon screen. For more information, refer to [HP Credential Manager for ProtectTools](#).

---

# Understanding Security Roles

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



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

For 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 ProtectTools can be customized by the security officer in cooperation with HP. For more information, visit <http://www.hp.com>.

- IT administrator—Applies and manages the security features defined by the security officer. Can also enable and disable some features. For example, if the security officer has decided to deploy 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.


Administrators are encouraged to perform “best practices” in restricting end-user privileges and restrictive access to users.

# Managing ProtectTools Passwords

Most of the 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.

**Table 1-1** Password Management



ProtectTools Password	Set in this ProtectTools Module	Function
Computer Setup administrator password	BIOS Configuration, by IT administrator	Protects access to the BIOS Computer Setup utility and security settings.
 <b>NOTE</b> Also known as BIOS administrator, F10 Setup, or Security Setup password		
Power-On password	BIOS Configuration	HP ProtectTools Power-On Authentication Support is a TPM-based security tool designed to prevent unauthorized access to the computer as it is powered on. Power-On Authentication Support uses the HP ProtectTools Embedded Security Basic User password. Once Power-On Authentication is enabled in Computer Setup, the password is set when the first/



**Table 1-1 Password Management (continued)**

		next Embedded Security Basic User Key is initialized. The Embedded Security TPM chip protects the password for Power-On Authentication.
Java Card administrator password	Java Card Security, by IT administrator	Links the Java Card to the computer for identification purposes.
 <b>NOTE</b> Also known as BIOS administrator card password		Allows a computer administrator to enable or disable Computer Setup passwords, generate a new administrator card, and create recovery files to restore user or administrator cards.
Java Card PIN	Java Card Security	Protects access to the Java Card contents and to computer access when an optional Java Card and reader is used. Checks to see if Java Card user password is duplicate to pin; it is used to register Java Card authentication
Java Card recovery file password (if available)	Java Card Security	Protects access to the recovery file that contains the BIOS passwords.
Java Card user password (if available)	Java Card Security	Links the Java Card to the computer for identification.
 <b>NOTE</b> Also known as BIOS user card password		Allows a user to create a recovery file to restore a user card.
Basic User password	Embedded Security	Used to access Embedded Security features, such as secure e-mail, file, and folder encryption. When enabled as the BIOS Power-On Authentication support password, protects access to the computer contents when computer is turned on, restarted, or restored from hibernation. Also used to authenticate the Personal Secure Drive (PSD) and to register TPM authentication.
 <b>NOTE</b> Also known as: Embedded Security password, TPM Preboot password		
Emergency Recovery Token password	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the TPM embedded security chip
 <b>NOTE</b> Also known as: Emergency Recovery Token Key		
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.
Credential Manager logon password	Credential Manager	This password offers 2 options: <ul style="list-style-type: none"> <li>• It can be used in place of the Windows logon process, allowing access to Windows and Credential Manager simultaneously.</li> <li>• It can be used in a separate logon to access Credential Manager after logging on to Microsoft Windows</li> </ul>
Credential Manager recovery file password	Credential Manager, by IT administrator	Protects access to the Credential Manager recovery file.

**Table 1-1 Password Management (continued)**

Windows logon password	Windows Control Panel	Can be used in manual logon or saved on the Java Card.
Backup scheduler password	Embedded Security, by IT administrator	Sets backup scheduler for embedded Security
 <b>NOTE</b> A Windows user password is used to configure the backup scheduler for embedded security.		
PKCS #12 Import password	Embedded Security, by IT administrator	Password used for Encryption key from other certificates, if imported
 <b>NOTE</b> Each imported certificate has a password specific to that certificate.		 <b>NOTE</b> Not required for normal software operation; user may opt to set this password when using embedded security to send important certificates
Password Reset Token	Embedded Security, by IT administrator	Customer provided tool allowing the owner to reset the Basic User password if lost; password is used to perform this reset operation
Microsoft Recovery Agent administrator password	Microsoft, by IT Security administrator	Ensure that the Personal Secure Drive (PSD) encrypted data can be recovered. See <a href="http://www.microsoft.com/technet/prodtechnol/winxpro/support/dataprot.mspx">http://www.microsoft.com/technet/prodtechnol/winxpro/support/dataprot.mspx</a> for more information.
 <b>NOTE</b> The Recovery Agent can be any local machine Administrator. If the Recovery Agent is created, then one would need to log in as that administrator and a password is required. The Recovery Agent can decrypt all users' encrypted data just by opening it (no Wizard required).		 <b>NOTE</b> Not required for normal software operation; user may opt to set this password when using embedded security to send important certificates
Virtual Token Master PIN	Credential Manager	Customer option to store owner credentials with Credential Manager
Virtual Token User PIN	Credential Manager	Customer option to store owner credentials with Credential Manager
Backup Identity wizard password	Credential Manager, by IT administrator	Used to protect access to an identity backup when using Credential Manager
Virtual Token Authentication password	Credential Manager	Used to register virtual token authentication by Credential Manager
TPM authentication alias	Credential Manager	Used in place of the Basic User password by credential manager, at the option of administrator or user
Fingerprint logon	Credential Manager	Credential Manager allows the user to replace the Windows password logon with a convenient and secure fingerprint logon. Unlike Password, fingerprint credentials cannot be shared, given away, stolen, or guessed. Used by Credential Manager
USB Token authentication	Credential Manager	Used by Credential Manager as a token authentication instead of a password

## Multifactor Authentication Credential Manager Logon

Credential Manager Logon enables multifactor authentication technology to log on to the Windows operating system. This raises the security of the standard Windows password logon by requiring strong multifactor authentication. This also enhances the convenience of the everyday logon experience by eliminating the need to remember user passwords. A unique feature of Credential Manager Logon is its ability to aggregate multiple account credentials into one user identity, which allows the use of multifactor authentication only once and multiple access to different Windows accounts with the same set of credentials.

Multifactor user authentication supports any combination of user passwords, dynamic or single-use passwords, TPM, Java Cards, USB tokens, virtual tokens, and biometrics. Credential Manager also supports alternative authentication methods, providing the possibility for multiple user access privileges for the same application or service. A user can consolidate all credentials, application password, and network accounts into a single data unit called User Identity. User identity is always encrypted and protected with multifactor authentication.

## 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, "Mary22Cat45".
- 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.

# Advanced Tasks

## Managing ProtectTools Settings

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

### Enabling and Disabling Java Card Power-On Authentication Support

If this option is available, enabling it allows you to use the Java Card for user authentication when you turn on the computer.



---

**NOTE** To fully enable the Power-On Authentication feature, you must also configure the Java Card using the Java Card Security for ProtectTools module.

---

To enable Java Card Power-On Authentication support:

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



---

**NOTE** To disable Java Card Power-On Authentication, select **Disable**.

---

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

### Enabling and Disabling Power-On Authentication Support for Embedded Security

If this option is available, enabling it allows the system to use the TPM embedded security chip 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 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, select **BIOS Configuration**.
3. Enter your Computer Setup administrator password at the BIOS administrator password prompt, and then click **OK**.
4. In the left pane, select **Security**.
5. Under **Embedded Security**, select **Enable Power-On Authentication Support**.



---

**NOTE** To disable Power-On Authentication for Embedded Security, select **Disable**.

---

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

## Managing Computer Setup Passwords

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



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

The power-on password can protect the computer 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 administrator password protects the configuration settings and system identification information in Computer Setup. After this password is set, it must be entered to access Computer Setup.

If you have set an administrator password, you will be prompted for the password before opening the BIOS Configuration portion of ProtectTools.



**NOTE** After you have set an administrator password, the **Set** button on the **Passwords** page is replaced by a **Change** button.

### Setting the Power-On Password (if available)

To set the power-on password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, select **BIOS Configuration**, and then select **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 **ProtectTools** window to save your changes.

### Changing the Power-On Password (if available)

To change the power-on password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, select **BIOS Configuration**, and then select **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** and **Verify New Password** boxes.

6. Click **OK** in the **Passwords** dialog box.
7. Click **Apply**, and then click **OK** in the **ProtectTools** window to save your changes.

## System Setup

1. Initialize HP ProtectTools Embedded Security.
2. Initialize Basic User Key.

HP Power-On Authentication Support starts as soon as the Basic User Key is set and the Basic User password is set for Power-On. After the next reboot, HP ProtectTools Power-On Authentication Support is initialized and the Basic User password must be used to start the computer. Once Power-On Authentication Support is functioning, the option to enter the BIOS Setup is no longer seen. If the user enters the Setup password at the Power-On Authentication Support window, the user enters the BIOS.

If Embedded Security Basic User password is already set, then the password must be changed to establish password protection using Power On Authentication.

## Changing Power-On Authentication Support

Password Power-On Authentication Support uses the Embedded Basic User password. To change the password:

1. Enter F10 BIOS settings (must have Setup Password as described in Setup steps above) and navigate to **Security > Embedded Security Device > Reset authentication credential**.
2. Press the arrow key to change the setting from **Do not reset** to **Reset**
3. Navigate to **Security Manager > Embedded Security > User Settings > Basic User Password > Change**.
4. Enter the old password, then enter and confirm the new password.
5. Reboot into Power-On Authentication Support.

The password window requests the user enter the old password first.

6. Enter the old password and enter the new password. (Entering the wrong new password three times will flash a new window stating that the password is invalid and Power-On Authentication will revert back to the original Embedded Security Password F1 = Boot.

At this point, the passwords will not be synchronized and user must change the Embedded Security password again to re synchronize them.)

## Changing User Accounts

Power-On Authentication only supports a single user at a time. The following steps can be used to change user accounts that control Power-On Authentication.

1. Navigate to **F10 BIOS > Security > Embedded Security Device > Reset authentication credential**.
2. Press the arrow key to move the cursor sideways, then press any key to continue.
3. Press **F10** twice, then **Enter** to **Save Changes and Exit**.

4. Create/logon to a targeted change Microsoft Windows user.
5. Open Embedded Security and initialize a Basic User Key for the new Windows user account. If a Basic User Key already exists, change the Basic User password to take ownership of Power-On Authentication.

Power-On Authentication now accepts only the new user's Basic User password.



**CAUTION** Many products are available to the customer that protect data through software encryption, hardware encryption and hardware. Most are managed using passwords. Failure to manage these tools and passwords can lead to data loss and hardware lockout up to and including replacement. Please review all appropriate help files before attempting to use these tools.

## Setting the Computer Setup Administrator Password

To set the Computer Setup administrator password:

1. Select **Start > All Programs > HP ProtectTools Security Manager**.
2. In the left pane, select **BIOS Configuration**, and then select **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 **ProtectTools** window to save your changes.

## Changing the Computer Setup Administrator Password

To change the Computer Setup administrator password:

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

## Dictionary Attack Behavior with Power-On Authentication

A dictionary attack is a method used to break into security systems by systematically testing all possible passwords to break a security system. A dictionary attack against Embedded Security could try to detect the Owner password, the Basic User password, or password-protected keys. Embedded Security offers an enhanced Dictionary Attack Defense.

### Dictionary Attack Defense

Embedded Security's defense against dictionary password attack is to detect failed authentication attempts and temporarily disable the TPM when a certain failure threshold is reached. Once the failure threshold is reached, not only is the TPM disabled and a reboot required, but ever increasing lockout timeouts are enforced. During the timeout, entering the correct password will be ignored. Entering the wrong password will double the last timeout.

Additional documentation on this process is located in the Embedded Security Help. Click **Welcome to the HP Embedded Security for ProtectTools Solution > Advanced Embedded Security Operation > Dictionary Attack Defense**.



---

**NOTE** Normally, a user receives warnings that their password is incorrect. The warnings state how many more attempts the user gets prior to the TPM disabling itself.

The Power-On Authentication process takes place in the ROM before the OS is loaded. Dictionary Attack Defense is operational, but the only warning the user will get is the X key symbol.

---



# 2 HP BIOS Configuration for ProtectTools

## Basic Concepts

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

With BIOS Configuration, you can

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



---

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

---

## Changing BIOS Settings

BIOS Configuration allows you to manage various computer settings that would otherwise be accessible only by pressing **F10** at startup and entering the Computer Setup utility. Refer to the *Computer Setup (F10) Utility Guide* on the *Documentation and Diagnostics CD* that shipped with the computer for information on settings and features. To access the Help files for BIOS Configuration, click **Security Manager > BIOS Configuration > Help**.



---

**NOTE** Refer to the ProtectTools Help screens for specific instructions for ProtectTools BIOS Configuration.

---



# 3 HP Embedded Security for ProtectTools

## Basic Concepts

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

- Enhanced Microsoft Encrypting File System (EFS) file and folder encryption
- Creation of a Personal Secure Drive (PSD) for encrypting user data
- Data management functions, such as backing up and restoring the key hierarchy
- Support for third-party applications that use MSCAPI (such as Microsoft Outlook and Microsoft Internet Explorer) and applications that use PKCS#11 (such as Netscape) for protected digital certificate operations when using the Embedded Security software

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

The hardware consists of a TPM that meets the Trusted Computing Group requirements of TPM 1.2 standards. The chip is integrated with the system board. Some TPM implementations (depending on model purchased) integrate the TPM as part of the NIC. In these NIC and TPM configurations, on-chip memory and off-chip memory, functions, and firmware are located on an external flash integrated with the system board. All TPM functions are encrypted or protected to ensure secure flash or communications.

The software also provides a function called PSD. The PSD is a function in addition to the EFS-based file/folder encryption, and it uses the Advanced Encryption Standard (AES) encryption algorithm. It is important to note that HP ProtectTools Personal Secure Drive cannot function unless the TPM is unhidden, enabled with appropriate software installed with ownership, and the user configuration initialized.

# Setup Procedures

---



**CAUTION** To reduce security risk, it is highly recommended that the IT administrator immediately initialize the TPM embedded security chip. If the TPM embedded security chip is not initialized, an unauthorized user or a computer worm could gain access to the computer or a virus could initialize the TPM embedded security chip and restrict access to the PC.

---

The TPM embedded security chip can be enabled in the BIOS Computer Setup utility, BIOS Configuration for ProtectTools, or HP Client Manager.

To enable the TPM 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. 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**.



**NOTE** Refer to the ProtectTools Help screens for specific instructions for ProtectTools Embedded Security.

---

# 4 HP Credential Manager for ProtectTools

## Basic Concepts

Credential Manager for ProtectTools has security features that provide a secure and convenient computing environment. These features include the following:

- Alternatives to passwords when logging on to Microsoft Windows, such as using a Java Card or biometric reader
- Single Sign On feature that automatically remembers credentials (user ids and passwords) 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 with an optional security device to unlock the computer and access applications
- Enhanced encryption for stored passwords, when implemented with a TPM embedded security chip

## Launch Procedure

To launch Credential Manager, if available:

1. Click **Start > Control Panel > Security Center > ProtectTools Security Manager > Credential Manager**.
2. Click **Log On** in the upper right corner of the panel.

You can choose to log on to Credential Manager in any of the following ways:

- Credential Manager Logon Wizard (preferred)
- ProtectTools Security Manager



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

## Logging On for the First 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.

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



---

**NOTE** Refer to the ProtectTools Help screens for specific instructions for ProtectTools Security Manager.

---

# 5 HP Java Card Security for ProtectTools

## Basic Concepts

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

With Java Card Security for ProtectTools, you can

- Access Java Card Security features
- Initialize a Java Card so that it can be used with other ProtectTools modules, such as Credential Manager for ProtectTools
- If available, work with the Computer Setup utility to enable Java Card authentication in a preboot environment, and to configure separate Java Cards for an administrator and a user. This requires a user to insert the Java Card and optionally enter a PIN prior to allowing the operating system to load.
- If available, set and change the password used to authenticate users of the Java Card
- If available, back up and restore Java Card BIOS passwords stored on the Java Card
- If available, save the BIOS password on the Java Card



---

**NOTE** Refer to the ProtectTools Help screens for specific instructions for ProtectTools Security Manager.

---





## 6 Third-Party Solutions

Platforms containing a TPM require both a TCG Software Stack (TSS) and embedded security software. All models provide the TSS; embedded security software must be purchased separately for some models. For those models, an NTRU TSS is provided to support customer third-party purchase of embedded security software. We recommend third-party solutions such as Wave Embassy Trust Suite.



# 7 HP Client Manager for Remote Deployment

## Background

HP Trustworthy platforms equipped with a Trusted Platform Module (TPM) ship with the TPM deactivated (default state). Enabling the TPM is an administrative option protected by HP BIOS-enforced policies. The administrator must be present to enter BIOS configuration options (F10 options) to enable the TPM. Furthermore, the Trusted Computing Group (TCG) specifications mandate that explicit human (physical) presence must be established in order to activate a TPM. This mandate ensures that a user's privacy rights are respected (by providing an opt-in model for use) and that a rogue application, virus, or Trojan horse does not enable the TPM for malicious use. The establishment of physical presence and the requirement for an administrator's local presence pose an interesting challenge for IT managers trying to deploy this technology across a large enterprise.

## Initialization

HP Client Manager (HPCM) provides a method of remotely enabling the TPM and taking ownership of the TPM in the enterprise environment. This method does not require the physical presence of the IT administrator, yet it still meets the TCG requirement.

HPCM allows the IT administrator to set certain BIOS options and then reboot the system to enable the TPM on the remote system. During this reboot, the BIOS, by default, displays a prompt; in response, the end user must press a key to prove physical presence, as specified by the TCG. The remote system then continues to boot, and the script completes by taking ownership of the TPM on the system. During this procedure, an emergency recovery archive and an emergency recovery token are created on a location designated by the IT administrator.

HPCM does not execute the TPM user initialization on the remote system, since the user must be allowed to choose the password. TPM user initialization must be performed by the end user of that system.

## Maintenance

HP Client Manager can be used to reset the user password remotely without the IT Administrator being made aware of the user password. HPCM can also remotely recover the user credentials. Proper administrator passwords must be supplied for both of these functions.




# 8 Troubleshooting

## Credential Manager for ProtectTools

Short description	Details	Solution
Using Credential Manager Network Accounts option, a user can select which domain account to log into. When TPM authentication is used, this option is not available. All other authentication methods work properly.	Using TPM authentication, the user is only logged into the local computer.	Using Credential Manager Single Sign On tools allows user to authenticate other accounts.
USB token credential is not available with login to Windows XP Service Pack 1.	<p>After installing USB token software, registering the USB token credential, and setting Credential Manager as primary login, the USB Token is neither listed nor available in the Credential Manager/gina logon.</p> <p>When logging back into Windows, log off Credential Manager, re-log back into Credential Manager and reselect token as primary login, the token login operation functions normally.</p>	<p>This only occurs with Windows XP Service Pack 1; update Windows version to Service Pack 2 via Windows Update to correct.</p> <p>To work around if retaining Service Pack 1, re-log back into Windows using another credential (Windows password) in order to log off and re-log back into Credential Manager.</p>
Some application Web pages create errors that prevent user from performing or completing tasks.	Some Web-based applications stop functioning and report errors due to the disabling functionality pattern of Single Sign On. For example, an ! in a yellow triangle is observed in Internet Explorer indicating an error has occurred.	<p>Credential Manager Single Sign On does not support all software Web interfaces. Disable Single Sign On support for the specific Web page by turning off Single Sign On support. Please see complete documentation on Single Sign On, which is available in the Credential Manager help files.</p> <p>If a specific Single Sign On cannot be disabled for a given application, call HP Service and Support and request 3rd level support through your HP Service contact.</p>
No option to <b>Browse for Virtual Token</b> during the login process.	User cannot move the location of registered virtual token in Credential Manager because the option to browse was removed due to security risks.	The browse option was removed from current product offerings because it allowed non-users to delete and rename files and take control of Windows.
Login with TPM authentication does not give the <b>Network Accounts</b> option.	Using the <b>Network Accounts</b> option, a user can select which domain account to log into. When TPM authentication is used, this option is not available.	HP is researching a workaround for future product enhancements.

Short description	Details	Solution
Domain administrators cannot change Windows password even with authorization.	This happens after a domain administrator logs on to a domain and registers the domain identity with Credential Manager using an account with Administrator's rights on the domain and the local PC. When the domain administrator attempts to change the Windows password from Credential Manager, the administrator gets an error logon failure: <b>User account restriction</b> .	Credential Manager cannot change a domain user's account password through <b>Change Windows password</b> . Credential Manager can only change the local PC account passwords. The domain user can change his/her password through <b>Windows security &gt; Change password</b> option, but, since the domain user does not have a physical account on the local PC, Credential Manager can only change the password used to log in.
Credential Manager Single Sign On default settings should be set to prompt to prevent loop.	Single Sign On default is set to log users automatically. However, when creating the second of two different password-protected documents, Credential Manager uses the last password recorded—the one from the first document.	HP is researching a workaround for future product enhancements.
Incompatibility issues with Corel WordPerfect 12 password gina.	If the user logs in 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 <b>Connect</b> button on screen.	If the Single Sign On credentials for Remote Desktop Connection (RDP) are set to <b>Connect</b> , Single Sign On, upon relaunch, always enters <b>Save As</b> instead of <b>Connect</b> .	HP is researching a workaround for future product enhancements.
ATI Catalyst configuration wizard is not usable with Credential Manager.	Credential Manager Single Sign On conflicts with the ATI Catalyst configure wizard.	Disable the Credential Manager Single Sign On.
When logging in using TPM authentication, the <b>Back</b> button on screen skips the option to choose another authentication method.	If user using TPM login authentication for Credential Manager enters his/her password, the <b>Back</b> button does not work properly, but instead immediately displays the Windows login screen.	HP is researching a workaround for future product enhancements.
Credential Manager opens out of standby when it is configured not to.	When <b>use Credential Manager log on to Windows</b> is not selected as an option, allowing the system to go into S3 suspend and then waking the system causes the Credential Manager logon to Windows to open.	<p>With no administrator password set, user cannot log on to Windows through Credential Manager because of account restrictions invoked by the Credential Manager.</p> <ul style="list-style-type: none"> <li>Without Java Card/token, user can cancel the Credential Manager login and user will see the Microsoft Windows login. User can log in at this point.</li> <li>With Java Card/token, the following workaround allows the user to enable/disable opening of Credential Manager upon Java Card insertion.</li> </ul> <ol style="list-style-type: none"> <li>Click <b>Advanced Settings</b>.</li> <li>Click <b>Service &amp; Applications</b>.</li> <li>Click <b>Java Cards and Tokens</b>.</li> </ol>


Short description	Details	Solution
		<p>4. Click when Java Card/token is inserted.</p> <p>5. Select the <b>Advise to log-on</b> checkbox.</p>
Users lose all Credential Manager credentials protected by the TPM, if the TPM module is removed or damaged.	If the TPM module is removed or damaged, users lose all credentials protected by the TPM.	<p>This is as designed.</p> <p>The TPM Module is designed to protect the Credential Manager credentials. HP recommends that the user back up identity from Credential Manager prior to removing the TPM module.</p>
Credential Manager not being set as primary logon in Windows 2000.	During Windows 2000 install, the logon policy is set for manual or auto logon admin. If auto logon is chosen, then the Windows default registry settings sets the default auto admin logon value at 1, and Credential Manager does not override this.	<p>This is as designed.</p> <p>If user wishes to modify operating system level settings for auto admin logon values for bypassing the edit path is <code>HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon</code></p> <p> <b>CAUTION</b> Use Registry Editor at your own risk! Using the Registry Editor (regedit) incorrectly can cause serious problems that may require you to reinstall the operating system. There is no guarantee that problems resulting from the incorrect use of Registry Editor can be solved.</p>
Fingerprint logon message appears whether or not fingerprint reader is installed or registered.	If user selects Windows logon, the following desktop alert appears in the Credential Manager task bar: <b>You can place your finger on the fingerprint reader to log on to Credential Manager.</b>	The purpose of the desktop alert is to notify the user that fingerprint authentication is available, if it is configured.
Credential Manager logon window for Windows 2000 states <b>insert card</b> when no reader is attached.	The Windows Credential Manager Welcome screen suggests the user can log on with <b>insert card</b> when no Java Card reader is attached.	The purpose of the alert is to notify the user that Java Card authentication is available, if it is configured.
Unable to log into 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, Administrator or user is unable to log into Credential Manager and the Windows logon screen remains displayed no matter which logon credential (password, finger print or Java Card) is selected.	<p>This issue appears to be resolved in Service Pack 2 from Microsoft. Refer to Microsoft knowledge base article 813301 at <a href="http://www.microsoft.com">http://www.microsoft.com</a> for more information on the cause of the issue.</p> <p>In order to log on, user must select Credential Manager and log in. After logging into Credential Manager, user is prompted to log in to Windows (user may have to select the Windows login option) to complete login process.</p> <p>If user logs into Windows first, then user must manually log into Credential Manager.</p>
Restoring Embedded Security causes Credential Manager to fail.	Credential Manager fails to register any credentials after the ROM is restored to factory settings.	<p>The HP Credential Manager for ProtectTools fails to access the TPM if the ROM was reset to factory settings after the Credential Manager installation.</p> <p>The TPM embedded security chip can be enabled in the BIOS Computer Setup utility, BIOS Configuration for</p>

Short description	Details	Solution
		<p>ProtectTools, or HP Client Manager. To enable the TPM embedded security chip:</p> <ol style="list-style-type: none"> <li>1. Open Computer Setup by turning on or restarting the computer, and then pressing <b>F10</b> while the <b>F10 = ROM Based Setup</b> message is displayed in the lower-left corner of the screen.</li> <li>2. Use the arrow keys to select <b>Security &gt; Setup Password</b>. Set a password.</li> <li>3. Select <b>Embedded Security Device</b>.</li> <li>4. Use the arrow keys to select <b>Embedded Security Device—Disable</b>. Use the arrow keys to change it to <b>Embedded Security Device—Enable</b>.</li> <li>5. Select <b>Enable &gt; Save changes and exit</b>.</li> </ol> <p>HP is investigating resolution options for future customer software releases.</p>
<p>Security <b>Restore Identity</b> process loses association with virtual token.</p>	<p>When user restores identity, Credential Manager can lose association with the location of the virtual token at login screen. Even though Credential Manager has the virtual token registered, user must reregister the token to restore association.</p>	<p>This is currently by design.</p> <p>When uninstalling Credential Manager without keeping identities, the system (server) part of the token is destroyed, so the token cannot be used anymore for logon, even if the client part of the token is restored through identity restore.</p> <p>HP is investigating long-term options for resolution.</p>



# Embedded Security for ProtectTools

Short description	Details	Solution
Encrypting folders, sub folders, and files on PSD causes error message.	If the user copies files and folders to the PSD and tries to encrypt folders/files or folders/subfolders, the <b>Error Applying Attributes</b> message appears. The user can encrypt the same files on the C:\ drive on 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 using on the PSD using EFS will produce 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.
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.
Encrypted folders with EFS in Windows 2000 are not shown highlighted in green.	Encrypted folders with EFS are highlighted in green in Windows XP, but not in Windows 2000.	This is as designed.  It is a feature of EFS that it does not highlight encrypted folders in Windows 2000, but it does in Windows XP. This is true whether or not an Embedded Security TPM is installed.
EFS does not require a password to view encrypted files in Windows 2000.	If a user sets up the Embedded Security, logs on as an administrator, then logs off and back on as the administrator, the user can subsequently see files/folders in Windows 2000 without a password. This occurs only in the first administrator account on Windows 2000. If a secondary administrator account is being logged into, this does not occur.	This is as designed.  It is a feature of EFS in Windows 2000. EFS in Windows XP, by default, will not let the user open files/folders without a password.
Software should not be installed on a restore with FAT32 partition.	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.  Microsoft EFS is supported only on NTFS and will not function on FAT32. This is a feature of Microsoft's EFS and is not related to HP ProtectTools software.
Windows 2000 User can share to the network any PSD with the hidden (\$) share.	Windows 2000 User can share to the network any PSD with the hidden (\$) share. The hidden share can be accessed over the network using the hidden (\$) share.	The PSD is not normally shared on the network, but it can be through the hidden (\$) share in Windows 2000 only. HP recommends always having the built-in Administrator account password-protected.
User is able to encrypt or delete the recovery archive XML file.	By design, the ACLs for this folder is not set; therefore, a user can inadvertently or purposely encrypt or delete the file, making it inaccessible. Once 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 in order to save/update their Basic User Key backup copy. Customers should adopt a 'best practices' security approach and instruct users never to encrypt or delete the recovery archive files.
HP ProtectTools Embedded Security EFS interaction with Symantec Antivirus or Norton Antivirus produces longer	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	To reduce the time required to scan HP ProtectTools Embedded Security EFS files, the user can either enter the encryption password before scanning or decrypt before scanning.

Short description	Details	Solution
encryption/decryption and scan times.	user does not enter a password, the Basic User password prompt times out, allowing NAV2005 to continue with the scan. Encrypting files using HP ProtectTools Embedded Security EFS takes longer when Symantec Antivirus or Norton Antivirus is running.	To reduce the time required to encrypt/decrypt data using HP ProtectTools Embedded Security EFS, the user should disable Auto-Protect on Symantec Antivirus or Norton Antivirus.
Cannot save emergency recovery archive to removable media.	If the user inserts an MMC or SD 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 another local drive other than the C drive.
Cannot encrypt any data in the Windows 2000 French (France) environment.	There is no <b>Encrypt</b> selection when right-clicking a file icon.	This is a Microsoft operating system limitation. If the locale is changed to anything else (French (Canada), for example), then the <b>Encrypt</b> selection will appear.  To work around the problem, encrypt the file as follows: right-click the file icon and select <b>Properties &gt; Advanced &gt; Encrypt Contents</b> .
Errors occur after experiencing a power loss while taking ownership during the Embedded Security Initialization.	<p>If there is a power loss while initializing the Embedded Security chip, the following issues will occur:</p> <ul style="list-style-type: none"> <li>When attempting to launch the Embedded Security Initialization Wizard, the following error is displayed: <b>The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.</b></li> <li>When attempting to launch the User Initialization Wizard, the following error is displayed: <b>The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.</b></li> </ul>	<p>Perform the following procedure to recover from the power loss:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <b>NOTE</b> Use the Arrow keys to select various menus, menu items, and to change values (unless otherwise specified). </div> <ol style="list-style-type: none"> <li>Start or restart the computer.</li> <li>Press <b>F10</b> when the <b>F10=Setup</b> message appears on screen (or as soon as the monitor LED turns green).</li> <li>Select the appropriate language option.</li> <li>Press <b>Enter</b>.</li> <li>Select <b>Security &gt; Embedded Security</b>.</li> <li>Set the <b>Embedded Security Device</b> option to <b>Enable</b>.</li> <li>Press <b>F10</b> to accept the change.</li> <li>Select <b>File &gt; Save Changes and Exit</b>.</li> <li>Press <b>ENTER</b>.</li> <li>Press <b>F10</b> to save the changes and exit the F10 Setup utility.</li> </ol>
Computer Setup (F10) Utility password can be removed after enabling TPM Module.	Enabling the TPM module requires a Computer Setup (F10) Utility password. Once 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	When a user logs on the system after creating a PSD, the TPM asks for the	This is by design.

Short description	Details	Solution
the system becomes active after Standby status	Basic User password. If the user does not enter the password and the system goes into Standby, the password dialog box is no longer available when the user resumes.	The user has to log off and back on to view the PSD password box again.
No password 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.
Microsoft EFS does not fully work in Windows 2000.	An administrator can access encrypted information on the system without knowing the correct password. If the administrator enters an incorrect password or cancels the password dialog, the encrypted file will open as if the administrator had entered the correct password. This happens regardless of the security settings used when encrypting the data. This occurs only in the first administrator account on Windows 2000.	The Data Recovery Policy is automatically configured to designate an administrator as a recovery agent. When a user key cannot be retrieved (as in the case of entering the wrong password or canceling the Enter Password dialog), the file is automatically decrypted with a recovery key.  This is due to the Microsoft EFS. Please refer to Microsoft Knowledge Base Technical Article Q257705 at <a href="http://www.microsoft.com">http://www.microsoft.com</a> for more information.  The documents cannot be opened by a non-administrator user
When viewing a certificate, 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 viewing the certificate, 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.
Intermittent encrypt and decrypt error occurs: <b>The process cannot access the file because it is being used by another process.</b>	Extremely intermittent error during file encryption or decryption occurs due to the file being used by another process, even though that file or folder is not being processed by the operating system or other applications.	To resolve the failure: <ol style="list-style-type: none"> <li>1. Restart the system.</li> <li>2. Log off.</li> <li>3. Log back in.</li> </ol>
Data loss in removable storage occurs if storage is removed prior to new data generation or transfer.	Removing storage mediums such as a MultiBay hard drive still shows PSD availability and does not generate errors while adding/modifying data to the PSD. After system restart, the PSD does not reflect file changes that occurred while the removable storage was not available.	The 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 <b>the device is not ready</b> .
During uninstall, if user has not initialized the Basic User and opens the Administration tool, the <b>Disable</b> 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 Admin. tool), then uninstalling. Accessing the Admin 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 Admin tool (by clicking <b>Yes</b> in the dialog box prompting <b>Click Yes to open Embedded Security Administration tool</b> ), uninstall waits	The Admin 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, then select <b>OK</b> or <b>Cancel</b> in order to continue with the uninstallation process.

Short description	Details	Solution
	until the Admin tool is closed. If user clicks <b>No</b> in that dialog box, then the Admin tool does not open at all and uninstall proceeds.	
Intermittent system lockup occurs after creating PSD on 2 users accounts and using fast-user-switching in 128-MB system configurations.	System may lock up with a black screen and non-responding keyboard and mouse instead of showing welcome (logon) screen when using fast-switching with minimal RAM.	<p>Root Cause suspicion is a timing issue in low memory configurations.</p> <p>Integrated graphics uses UMA architecture taking 8 MB of memory, leaving only 120 available to user. This 120 MB is shared by both users who are logged in and are fast-user-switching when error is generated.</p> <p>Workaround is to reboot system and customer is encouraged to increase memory configuration (HP does not ship 128-MB configurations by default with security modules).</p>
EFS User Authentication (password request) times out with <b>access denied</b> .	The EFS User Authentication password reopens after clicking <b>OK</b> or returning from standby state after timeout.	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 description	Functional descriptions during custom setup option during installation wizard are truncated.	HP will correct this in a future release.
EFS Encryption works without entering password in the prompt.	By allowing prompt for User password to time out, encryption is still capable on a file or folder.	The ability to encrypt does not require password authentication, since this is a feature of the Microsoft EFS encryption. The decryption will require the user password to be supplied.
Secure e-mail is supported, even if unchecked in User Initialization Wizard or if 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 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 will render 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 not functioning during user restore in Embedded Security.	<p>The error occurs after user</p> <ul style="list-style-type: none"> <li>• Initializes owner and user in Embedded Security (using the default locations—<b>My Documents</b>).</li> <li>• Resets the chip to factory settings in the BIOS.</li> <li>• Reboots the computer.</li> <li>• Begins to restore Embedded Security. During the restore process, Credential Manager asks</li> </ul>	Click the <b>Browse</b> button on the screen to select the location, and the restore process proceeds.

Short description	Details	Solution
	<p>user if the system can automate the logon to Infineon TPM User Authentication. If user selects <b>Yes</b>, then the location of SPEmRecToken automatically appears in the text box.</p> <p>Even though this location is correct, the following error message is displayed: <b>No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.</b></p>	
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 will be unavailable.	The second user's PSD will only be available if it is reconfigured to use another drive letter or if the first user is logged off.
PSD is disabled and cannot be deleted after formatting the hard drive on which the PSD was generated	<p>The PSD is disabled and cannot be deleted after formatting the secondary hard drive on which the PSD was generated. The PSD icon is still visible, but the error message <b>drive is not accessible</b> appears when the user attempts to access the PSD.</p> <p>User is not able to delete the PSD and a message appears that states: <b>your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process.</b> User must reboot the system in order to delete the PSD and it is not loaded after reboot.</p>	<p>As designed: If a customer force-deletes or disconnects from the storage location of the PSD data, the Embedded Security PSD drive emulation continues to function and will produce errors based on lack of communication with the missing data.</p> <p>Resolution: After the next reboot, the emulations fail to load and user can delete the old PSD emulation and create a new PSD.</p>
An internal error has been detected restoring from Automatic Backup Archive.	<p>If the user</p> <ul style="list-style-type: none"> <li>clicks <b>Restore under Backup</b> option of Embedded Security in HPPTSM to restore from the automatic backup Archive</li> <li>selects <b>SPSystemBackup .xml</b></li> </ul> <p>the Restore Wizard fails and the following error message is displayed: <b>The selected Backup Archive does not match the restore reason. Please select another archive and continue.</b></p>	<p>If the user selects <b>SpSystemBackup.xml</b> when the SpBackupArchive.xml is required, Embedded Security Wizard fails with: <b>An internal Embedded Security error has been detected.</b></p> <p>User must select the correct .xml file to match the required reason.</p> <p>The processes are working as designed and function properly; however, the internal Embedded Security error message is not clear and should state a more appropriate message. HP is working to enhance this in future products.</p>
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 <b>decryption process failed</b> error message is displayed.	<p>The non-selected users can be restored by resetting the TPM, running the restore process, and selecting all users before the next default daily back 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 non-selected users cannot be restored.</p> <p>Also, user must restore the entire system backup. An Archive Backup can be restored individually.</p>

Short description	Details	Solution
Resetting System ROM to default hides 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 <b>Security &gt; Device security</b> , modify the field from <b>Hidden to Available</b> .
Automatic backup does not work with mapped drive.	<p>When an administrator sets up Automatic Backup in Embedded Security, it creates an entry in <b>Windows &gt; Tasks &gt; Scheduled Task</b>. This Windows Scheduled Task is set to use NT AUTHORITY\SYSTEM for rights to execute the backup. This works properly to any local drive.</p> <p>When the administrator instead configures the Automatic Backup to save to a mapped drive, the process fails because the NT AUTHORITY\SYSTEM does not have the rights to use the mapped drive.</p> <p>If the Automatic Backup is scheduled to occur upon login, Embedded Security TNA Icon displays the following message: <b>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.</b> If the Automatic Backup is scheduled for a specific time, however, the backup fails without displaying notice of the failure.</p>	<p>The workaround is to change the NT AUTHORITY\SYSTEM to (computer name)\(admin name). This is the default setting if the Scheduled Task is created manually.</p> <p>HP is working to provide future product releases with default settings that include computer name\admin name.</p>
Unable to disable Embedded Security State temporarily in Embedded Security GUI.	<p>The current 4.0 software was designed for HP Notebook 1.1B implementations, as well as supporting HP Desktop 1.2 implementations.</p> <p>This option to disable is still supported in the software interface for TPM 1.1 platforms.</p>	HP will address this issue in future releases.

# Miscellaneous

Software Impacted— Short description	Details	Solution
<p>HP ProtectTools Security Manager—Warning received: <b>The security application can not be installed until the HP Protect Tools Security Manager is installed.</b></p>	<p>All security applications such as Embedded Security, Java Card, and biometrics are extendable plug-ins for the HP Security Manager interface. Security Manager must be installed before an HP-approved security plug-in can be loaded.</p>	<p>HP ProtectTools Security Manager software must be installed before installing any security plug-in.</p>
<p>HP ProtectTools TPM Firmware Update Utility for dc7600 and models containing Broadcom-enabled TPMs—The tool provided through HP support Web site reports <b>ownership required.</b></p>	<p>This is the expected behavior of TPM firmware utility for dc7600 and models containing Broadcom-enabled TPMs</p> <p>The firmware upgrade tool allows the user to upgrade the firmware, with or without an endorsement key (EK). When there is no EK, no authorization is required to complete the firmware upgrade.</p> <p>When there is an EK, a TPM owner must exist, since the upgrade requires owner authorization. After the successful upgrade, the platform must be restarted for the new firmware to take effect.</p> <p>If the BIOS TPM is factory-reset, ownership is removed and firmware update capability is prevented until the Embedded Security Software platform and User Initialization Wizard have been configured.</p> <p>*A reboot is always recommended after performing a firmware update. The firmware version is not identified correctly until after the reboot.</p>	<ol style="list-style-type: none"> <li>1. Reinstall HP ProtectTools Embedded Security Software.</li> <li>2. Run the Platform and User configuration wizard.</li> <li>3. Ensure that the system contains Microsoft .NET framework 1.1 installation:             <ol style="list-style-type: none"> <li>a. Click <b>Start</b>.</li> <li>b. Click <b>Control Panel</b>.</li> <li>c. Click <b>Add or remove programs</b>.</li> <li>d. Ensure <b>Microsoft .NET Framework 1.1</b> is listed.</li> </ol> </li> <li>4. Check the hardware and software configuration:             <ol style="list-style-type: none"> <li>a. Click <b>Start</b>.</li> <li>b. Click <b>All Programs</b>.</li> <li>c. Click <b>HP ProtectTools Security Manager</b>.</li> <li>d. Select <b>Embedded Security</b> from tree menu.</li> <li>e. Click <b>More Details</b>. The system should have the following configuration:                 <ul style="list-style-type: none"> <li>• Product version = V4.0.1</li> <li>• Embedded Security State: Chip State = Enabled, Owner State = Initialized, User State = Initialized</li> <li>• Component Info: TCG Spec. Version = 1.2</li> <li>• Vendor = Broadcom Corporation</li> <li>• FW Version = 2.18 (or greater)</li> <li>• TPM Device driver library version 2.0.0.9 (or greater)</li> </ul> </li> </ol> </li> <li>5. If the FW version does not match 2.18, download and update the TPM firmware. The TPM Firmware SoftPak is a support download available at <a href="http://www.hp.com">http://www.hp.com</a>.</li> </ol>
<p>HP ProtectTools Security Manager—Intermittently,</p>	<p>Intermittently (1 in 12 instances), an error is created by using the close button in the</p>	<p>This is related to a timing dependency on plug-in services load time when closing and restarting Security</p>



Software Impacted— Short description	Details	Solution
an error is returned when closing the Security Manager interface.	upper right of the screen to close Security Manager before all plug-in applications have finished loading.	<p>Manager. Since PTHOST.exe is the shell housing the other applications (plug-ins), it depends on the ability of the plug-in to complete its load time (services). Closing the shell before the plug-in has had time to complete loading is the root cause.</p> <p>Allow Security Manager to complete services loading message (seen at top of Security Manager window) and all plug-ins listed in left column. To avoid failure, allow a reasonable time for these plug-ins to load.</p>
HP ProtectTools * General—Unrestricted access or uncontrolled administrator privileges pose security risk.	<p>Numerous risks are possible with unrestricted access to the client PC:</p> <ul style="list-style-type: none"> <li>• deletion of PSD</li> <li>• malicious modification of user settings</li> <li>• disabling of security policies and functions</li> </ul>	<p>Administrators are encouraged to follow “best practices” in restricting end-user privileges and restricting user access.</p> <p>Unauthorized users should not be granted administrative privileges.</p>
BIOS and OS Embedded Security password are out of synch.	If 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 initialize 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 in.	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.
User has to change PIN to make TPM preboot work after a TPM factory reset.	User has to change PIN or create another user to initialize his 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.
<b>Power-on authentication support</b> not set to default using Embedded Security <b>Reset to Factory Settings</b>	In Computer Setup, the <b>Power-on authentication support</b> option is not being reset to factory settings when using the Embedded Security Device option <b>Reset to Factory Settings</b> . By default, <b>Power-on authentication support</b> is set to <b>Disable</b> .	<p>The <b>Reset to Factory Settings</b> option disables Embedded Security Device, which hides the other Embedded Security options (including <b>Power-on authentication support</b>). However, after re-enabling Embedded Security Device, <b>Power-on authentication support</b> remained enabled.</p> <p>HP is working on a resolution, which will be provided in future Web-based ROM SoftPaq offerings.</p>
Security Power-On Authentication overlaps BIOS Password during boot sequence.	Power-On Authentication prompts the user to log on to system using the TPM password, but, if the user presses F10 to access the BIOS, Read rights access only is granted.	To be able to write to BIOS, the user must enter 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 BIOS asks for both the old and new passwords through Computer Setup after changing the Owner password in Embedded Security Windows software.	This is as designed. This is due to the inability of the BIOS to communicate with the TPM, once the operating system is up and running, and to verify the TPM pass phrase against the TPM key blob.



---

<b>Software Impacted— Short description</b>	<b>Details</b>	<b>Solution</b>
changing the Owner password in Embedded Security Windows software.		

---



# Glossary

**Advanced Encryption Standard (AES)** A symmetric 128-bit block data encryption technique

**Application Programming Interface (API)** A series of internal operating system functions that applications can use to perform various tasks

**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.

**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 for ProtectTools 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. A software component that interfaces with the MSCAPI

**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.

**Emergency recovery archive** Protected storage area that allows the re-encryption of Basic User Keys from one platform owner key to another.

**Encrypting File System (EFS)** System that encrypts all files and subfolders within the selected folder. A transparent file encryption service provided by Microsoft for Windows 2000 or later

**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.

**Identity** In the 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.

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

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

**Low Pin Count (LPC)** Defines an interface used by the HP ProtectTools Embedded Security device to connect with the platform chipset. The bus consists of 4 bits of Address/Data pins, along with a 33Mhz clock and several control/status pins.

**Microsoft Cryptographic API, or CryptoAPI (MSCAPI)** An API from Microsoft that provides an interface to the Windows operating system for cryptographic applications

**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 data. A feature that is provided by HP ProtectTools Embedded Security. This application creates a virtual drive on the user's computer that automatically encrypts files/folders that are moved into the virtual drive.

**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 Cryptographic Standards (PKCS)** Standards generated that govern definition and use of Public Key/Private Key means of encryption and decryption.

**Public Key Infrastructure (PKI)** A general term defining the implementation of security systems that use Public Key/Private Key encryption and decryption

**Reboot** Process of restarting the computer.

**Secure Multipurpose Internet Mail Extensions (S/MIME)** A specification for secure electronic messaging using PKCS. S/MIME offers authentication via digital signatures and privacy via encryption

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

**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.

**TCG Software Stack (TSS)** Provides services to take full advantage of the TPM, but does not require the same protections. Provides standard software interface for accessing TPM functions. To make full use of TPM capabilities, such as key backup, key migration, platform authentication and attestation, applications write directly to the TSS.

**Trusted Computing Group (TCG)** Industry association set up to promote the concept of a "Trusted PC." TCG supersedes T CPA

**Trusted Computing Platform Alliance (TCPA)** Trusted computing alliance; now superseded by TCG

**Trusted Platform Module (TPM) embedded security chip (some 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 meet the Trusted Computing Group (TCG) specifications. TPM hardware and software enhance the security of EFS and the Personal Secure Drive by protecting the keys used by EFS and the Personal Secure Drive. In systems without the TPM, the keys used for EFS and the PSD are normally stored on the hard drive. This makes the keys potentially vulnerable. In systems with the TPM card, the TPM's private Storage Root Keys, which never leave the TPM chip, are used to “wrap” or protect the keys used by EFS and by the PSD. Breaking into the TPM to extract the private keys is much more difficult than hacking onto the system's hard drive to obtain the keys. The TPM also enhances the security of secure e-mail via S/MIME in Microsoft Outlook and Outlook Express. The TPM functions as a Cryptographic Service Provider (CSP). Keys and certificates are generated and/or supported by the TPM hardware, providing significantly greater security than software-only implementations.

**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 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

advanced tasks 6

## B

Backup Identity wizard  
password 4

Backup scheduler password 4

Basic User password, definition 3

## BIOS

administrator card password,  
definition 3

administrator password,  
definition 2

changing settings 11

user card password,  
definition 3

BIOS Configuration for  
ProtectTools 11

## C

Client Manager 21

## Computer Setup

administrator password,  
changing 9

administrator password,  
definition 2

passwords, managing 7

setting administrator  
password 9

## Credential Manager

installation 15

logging on 16

logon 5

logon password 3

recovery file password 3

troubleshooting 23

## D

Dictionary Attack 10

## E

Embedded Security for  
ProtectTools

password 3

Power-On Authentication 6

setup 14

troubleshooting 27

emergency recovery token

password, definition 3

## F

F10 Setup password 2

fingerprint logon 4

## I

installation, Credential  
Manager 15

## J

## Java Card

administrator password,  
definition 3

PIN, definition 3

Power-On Authentication 6

recovery file password,  
definition 3

Security for ProtectTools 17

user password, definition 3

## M

## Multifactor Authentication

Credential Manager Logon 5

## O

owner password, definition 3

## P

Password Reset Token 4

## passwords

Backup Identity wizard 4

Backup scheduler 4

Basic User 3

## Computer Setup

administrator 2

Computer Setup administrator,  
changing 9

Computer Setup administrator,  
setting 9

Computer Setup, managing 7

Credential Manager logon 3

Credential Manager recovery  
file 3

definitions 2

## Emergency Recovery

Token 3

Fingerprint logon 4

guidelines 5

Java Card administrator 3

Java Card PIN 3

Java Card recovery file 3

Java Card user 3

Owner 3

Password Reset Token 4

PKCS #12 Import 4

power-on 2

power-on, changing 7

power-on, setting 7

ProtectTools, management 2

Security Recovery Agent 4

TPM authentication alias 4

USB Token authentication 4

Virtual Token Authentication 4

Virtual Token Master PIN 4

Virtual Token User PIN 4

Windows logon 4

PKCS #12 Import password 4

## power-on

changing password 7

Dictionary Attack 10

- password definition 2
- setting password 7
- Power-On Authentication
  - embedded security 6
  - Java Card 6
- ProtectTools
  - Credential Manager 15
  - embedded security for 13
  - Java Card Security 17
  - managing settings 6
  - password management 2
  - Security Manager access 1
  - Security Manager modules 1

Virtual Token User PIN 4

## W

Windows

- logon password 4

## R

remote deployment, Client Manager 21

## S

security

- embedded for
  - ProtectTools 13
  - Java Card 17
- roles 2
- setup password 2

Security Manager, ProtectTools 1

Security Recovery Agent

- password 4

software

- ProtectTools Security Manager 1

## T

TCG Software Stack (TSS) 1, 19

third-party solutions 19

TPM authentication alias 4

TPM Preboot password 3

troubleshooting

- Credential Manager for ProtectTools 23
- Embedded Security for ProtectTools 27
- Miscellaneous 33

## U

USB Token authentication 4

## V

Virtual Token Authentication

- password 4

Virtual Token Master PIN 4