HP ProtectTools Troubleshooting Guide

HP Compaq Business Desktops

Document Part Number: 413742-001

January 2006

This document contains information and recommendations for the ProtectTools administrator concerning questions that may arise in the administration and operation of HP ProtectTools.

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.

⚠ **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.

HP ProtectTools Troubleshooting Guide
HP Compaq Business Desktops

First Edition (January 2006)

Document Part Number: 413742-001

HP ProtectTools Troubleshooting Guide

Overview

HP ProtectTools Security is a new technology offered by HP on some Business PCs. This technology offers enhanced security support for file/folder encryption, user identity and protection, Single Sign On, multi-factor authentication, smart card, smart card preboot, token and biometric support and works natively with the operating system to enhance security aware applications, such as secure e-mail. The enhanced security is achieved through both hardware and software. Windows-based management of the BIOS is also incorporated through a BIOS Configuration module. All software is centrally managed through an HP Security Manager interface, which can be accessed from the task tray, start menu, or control panel. A properly enabled security system requires a TPM-enabled BIOS, versions 1.54 or greater, obtainable through www.hp.com support, and security software available via purchase.

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

Hardware

The hardware consists of a Trusted Platform Module (TPM) which meets the Trusted Computing Group requirements of TPM 1.2 standards. The card is integrated with the system board and is part of the NIC. The NIC and TPM solution contains 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.

Software

The software, HP ProtectTools, has two parts: HP ProtectTools Security Manager and HP plug-in modules. Security Manager is the interface (shell) that centralizes all security applications (plug-ins). The computer offers security in both configure-to-order and aftermarket configurations. Both offerings provide a CD which can be used in Microsoft Windows to install the HP ProtectTools security products. Customers using a non-HP corporate image are encouraged to use the provided CD to install security software. Some HP Web-based downloads (SoftPaqs) will not install unless previous versions of security software are already installed on the target PC.

HP ProtectTools security applications for the computer are:

- HP ProtectTools Security Manager: The software is preinstalled on the hard drive and can be accessed from the Start Menu or Control Panel applet. The Security Manager shell interface provides a central point for administering all security plug-in modules. Security plug-ins like the TPM, Smart Card, and future security products cannot be installed unless the Security Manager interface is present.
- HP ProtectTools Embedded Security: This supports the TPM 1.2 hardware directly and is preinstalled on the imaged drive for desktop. In Windows 2000 and Windows XP environments, this software supports enhanced security for secure e-mail with Microsoft

Outlook or Outlook Express, and it supports enhanced security for Microsoft EFS file/folder encryption. The software also provides a function called Personal Secure Drive (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. Additionally, the TPM also supports 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 Internet Explorer) and applications that use PKCS#11 (such as Netscape) for protected digital certificate operations when using the Embedded Security software.

- HP ProtectTools TPM Firmware Update Utility: This utility is a Web-based SoftPaq for updating your TPM firmware.
- HP Credential Manager for ProtectTools: This tool provides identity management and has security features that protect against unauthorized access to your computer. These features include the following:
    - ❏ Alternatives login capability as opposed to passwords when logging on to Windows, such as using a smart card or biometric reader to log on to Windows
    - ❏ Single Sign On feature that automatically remembers credentials for Web sites, applications, and protected network resources
    - ❏ Support for optional security devices, such as smart cards and biometric readers
    - ❏ Support for additional security settings, such as requiring authentication 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
- Smart Card Security for ProtectTools: This tool manages the smart card setup and configuration for computers equipped with an optional smart card reader. The smart card BIOS security mode is available on some models. When enabled, this mode requires you to use a smart card to log on to the computer.
- BIOS Configuration for ProtectTools: This configuration provides access to the Computer Setup Utility security and configuration settings. This allows users to access system security features managed by Computer Setup through Windows.

Please consult the HP ProtectTools Security Manager Guide that shipped with the computer or access this online at http://www.hp.com along with the latest software, firmware, driver, and support materials. Help files provided with the installed product contain a variety of troubleshooting, configuration, and functional product data, and they are considered the first direct source of information.

Table A Glossary of HP ProtectTools Embedded Security Related Terminology

Acronym	Term	Detail
AES	Advanced Encryption Standard	A symmetric 128-bit block data encryption technique
API	Application Programming Interface	A series of internal operating system functions that applications can use to perform various tasks
CSP	Cryptographic Service Provider	A software component that interfaces with the MSCAPI

Acronym	Term	Detail
EFS	Encryption File System	A transparent file encryption service provided by Microsoft for Windows 2000 or later
LPC	Low Pin Count	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.
MSCAPI:	Microsoft Cryptographic API, or CryptoAPI	An API from Microsoft that provides an interface to the Windows operating system for cryptographic applications
PKCS	Public Key Cryptographic Standards	Standards generated that govern definition and use of Public Key/Private Key means of encryption and decryption.
PKI	Public Key Infrastructure	A general term defining the implementation of security systems that use Public Key/Private Key encryption and decryption
PSD	Personal Secure Drive	A feature that is provided by HP ProtectTools Embedded Security. This application creates a virtual drive on the user's machine that automatically encrypts files/folders that are moved into the virtual drive.
S/MIME	Secure Multipurpose Internet Mail Extensions	A specification for secure electronic messaging using PKCS. S/MIME offers authentication via digital signatures and privacy via encryption
TCG	Trusted Computing Group	Industry association set up to promote the concept of a “Trusted PC.” TCG supersedes TCPA
TCPA	Trusted Computing Platform Alliance	Trusted computing alliance; now superseded by TCG
TPM	Trusted Platform Module	TPM hardware and software enhances 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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Encrypting folders, sub folders, and files on PSD cause 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 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.
HP ProtectTools Embedded Security—Cannot Take Ownership With Another OS In Multi-Boot 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, the Embedded Security is designed to work with only one OS per system.
HP ProtectTools Embedded Security—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.
HP ProtectTools Embedded Security—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.
HP ProtectTools Embedded Security—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 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.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Initialization fails for TPM module after system restore.	If the user restores the hard drive from the restore CD, initialization of the TPM fails.	This is as designed. The TPM must be reset and enabled again in Computer Setup (F10) Utility prior to initialization.
HP ProtectTools Embedded Security—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 W2K only. HP recommends always having the built-in Administrator account password-protected.
HP ProtectTools Embedded Security—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—HP ProtectTools Embedded Security EFS interaction with Norton Antivirus produces longer encryption/decryption and scan times	Encrypted files interfere with Norton Anti Virus 2005 virus scan. During the scan process, the Basic User Key password prompt asks the user for a password every 10 files or so. If the user does not enter a password, the Basic User Key password prompt times out, allowing NAV2005 to continue with the scan. Encrypting files using HP ProtectTools Embedded Security EFS takes longer when Norton Antivirus is running.	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. To reduce the time required to encrypt/decrypt data using HP ProtectTools Embedded Security EFS, the user should disable Auto-Protect on Norton Antivirus.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Cannot encrypt any data in the Windows 2000 French (France) environment.	There is no Encrypt 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 **Encrypt** selection will appear. To work around the problem, encrypt the file as follows: right-click the file icon and select **Property > Advanced > Encrypt Contents**.
HP ProtectTools Embedded Security—Errors occur after experiencing a power loss while taking ownership during the Embedded Security Initialization	If there is a power loss while initializing the Embedded Security chip, the following issues will occur: • When attempting to launch the Embedded Security Initialization Wizard, the following error is displayed: **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.** • When attempting to launch the User Initialization Wizard, the following error 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: ✎ 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 screen (or as soon as the monitor LED turns green). 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 F10 Setup utility.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—The PSD password box is no longer displayed when the system becomes active after Standby status	When a user logs on the system after creating a PSD, the TPM asks for the 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.	This is by design. The user has to log off and back on to view the PSD password box again.
HP ProtectTools Embedded Security—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.
HP ProtectTools Embedded Security—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.	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 for more information. The documents cannot be opened by a non-administrator user.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Intermittent encrypt and decrypt error occurs: **The process cannot access the file because it is being used by another process.**	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, the user can log off and back on to the system. Restart, log off, and log back in to resolve the issue.
HP ProtectTools Embedded Security—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 **the device is not ready**.
HP ProtectTools Embedded Security—During uninstall, if user has not initialized the Basic User Key and opens the Administration tool, the **Disable** option is not available and Uninstaller will not continue until the Administration tool is closed.	During uninstallation, 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 **Yes** in the dialog box prompting **Click Yes to open Embedded Security Administration tool**), uninstall waits until the Admin tool is closed. If user clicks **No** in that dialog box, then the Admin tool does not open at all and uninstall proceeds.	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 **Ok** or **Cancel** in order to continue with the uninstallation process.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—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.	Root Cause suspicion is a timing issue in low memory configurations. 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. 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).
HP ProtectTools 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, smart 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.	HP ProtectTools Security Manager software must be installed before installing any security plug-in.
HP ProtectTools Embedded Security—EFS User Authentication (password request) times out with **access denied**	The EFS User Authentication password reopens after clicking **OK** or returning from standby state after timeout.	This is by design—to avoid issues with Microsoft EFS, a 30-second timer watchdog timer was created to generate the error message).
HP ProtectTools Embedded Security—Minor truncation during setup of Japanese is observed in functional description	Functional descriptions during custom setup option during installation wizard are truncated.	HP is aware of translation issues and will be translating in future Web release.
HP ProtectTools Embedded Security—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.
HP ProtectTools Embedded Security—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)	In future releases, the wizard and user policies descriptions will be modified for better clarity. This behavior is as designed. Encrypted mail is configured after Embedded Security is initialized.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Application lock-ups occur when the connection with a TPM Module is lost	When the TPM module is damaged or the connection is lost, the Security Manager locks up. Attempting to close the Security Manager causes Windows error messages.	If system appears not to function properly or the TPM is not found, perform the following manual inspections to ensure the system is properly configured: • Check in the Computer Setup (F10) Utility to ensure that the TPM is unhidden. • Check the Device Manager reports to ensure that the TPM Device Driver is installed: 1. Click **Start**. 2. Click **Control Panel**. 3. Click **System**. 4. Click **System Devices**. 5. Click **Broadcom TPM**. (The device status should indicate **This device is working properly.**) A 3-minute delay occurs as applications and Windows services time out after attempting connection to the damaged TPM. The Security Manager recovers and the user can run the self test and confirm damaged module.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	**Details**	**Solution / Workaround**
HP ProtectTools TPM Firmware Update Utility—The tool provided through HP support Web site reports **ownership required**	Expected Behavior of TPM firmware Utility The firmware upgrade tool allows the user to upgrade the firmware, both when there is and when there is not an endorsement key (EK) present. 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. *A reboot is always recommended after performing a firmware update. The firmware version is not identified correctly until after the reboot.	1. Reinstall HP ProtectTools Embedded Security Software 2. Run the Platform and User configuration wizard. 3. Ensure that the system contains Microsoft .NET framework 1.1 installation: • Click **Start**. • Click **Control Panel**. • Click **Add or remove programs**. • Ensure **Microsoft .NET Framework 1.1** is listed. 4. Check the hardware and software configuration: • Click **Start**. • Click **All Programs**. • Click **HP ProtectTools Security Manager**. • Select **Embedded Security** from tree menu. • 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) If the FW version does not match 2.18, download and update the TPM firmware. The TPM Firmware SoftPaq is a support download available at www.hp.com.

Software Impacted-Short description	**Details**	**Solution / Workaround**
HP ProtectTools Credential Manager—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 machine.	Using Credential Manager Single Sign On tools allows user to authenticate other accounts.
HP ProtectTools Embedded Security—Automated logon scripts not functioning during user restore in Embedded Security	The error occurs after user 1. Initializes owner and user in Embedded Security (using the default locations—**My Documents**). 2. Resets the chip to factory settings in the BIOS. 3. Reboots the machine. 4. Begins to restore Embedded Security. During the restore process, Credential Manager 1.5.0.631.35 asks user if the system can automate the logon to Infineon TPM User Authentication. If user selects **Yes**, then the location of SPEmRecToken automatically appears 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.**	Use the **Browse** button to select the location, and the restore process proceeds.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Credential Manager—USB token credential is not available with login to Windows XP SP1	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. 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.	This only occurs with Windows XP SP1; update Windows version to SP2 via Windows Update to correct. To work around if retaining SP1, re-log back into Windows using another credential (Windows password) in order to log off and re-log back into Credential Manager.
HP ProtectTools Credential Manager—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.	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. If a specific Single Sign On cannot be disabled for a given application. Call 3rd level support for HP direct assistance.
HP ProtectTools Credential Manager—System intermittently locks up and goes into hibernation when an APC biometric fingerprint reader is configured as an authentication tool for Credential Manager	System intermittently locks up and displays the **going into hibernation** screen when APC Personal biometric USB Pod (BIOPOD) is configured as an authentication tool for Credential Manager.	Press the power button for 3 seconds to force the system to reboot. HP is working on a resolution. The resolution will be made available in future Credential Manager product development.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Security Manager—Intermittently, an error is returned when closing the Security Manager interface	Intermittently (1 in 12 instances), an error is created by using the close button in the upper right of the screen to close Security Manager before all plug-in applications have finished loading.	This is related to a timing dependency on plug-in services load time when closing and restarting Security 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. To resolve, 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. No corrective action is planned by HP for the Security Manager product.
HP ProtectTools Embedded Security—Guest User account can violate policy through the PSD interface	Using the Embedded Security Task Notification Area (task tray) icon, a guest user can bypass Security Manager and initialize a basic user. During the basic user initialization, the guest could create a PSD that monopolizes the hard drive.	The system administrator can resolve this by deleting the guest-user-created PSD. HP is working with plug-in suppliers to be aware of limited/guest user capabilities for future product enhancements.
HP ProtectTools Embedded Security—Guest User receives message that **PTHOST.exe** has not been approved by Hewlett-Packard Company	The following error message appears when a guest user opens HP ProtectTools Security Manager: **this module 'C:\Program Files\HPQ\HP Protect Tools Security\PTHOST.EXE' has not been approved by Hewlett-Packard Company. Do you want to continue?**	Guest user support is not provided by HP, HP recommends limited user support by the administrator. Future improvements are planned to prevent Security Manager runtime in Guest mode.
HP ProtectTools Embedded Security—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—PSD is disabled and cannot be deleted after formatting the hard drive on which the PSD was generated	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 **drive is not accessible** appears when the user attempts to access the PSD. User is not able to delete the PSD and a message appears that states: **your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process**. User must reboot the system in order to delete the PSD and it is not loaded after reboot.	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.
HP ProtectTools * General—Unrestricted access or uncontrolled administrator privileges pose security risk	Numerous risks are possible with unrestricted access to the client PC: • 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.
HP ProtectTools Embedded Security—Hiding the Broadcom TPM in the BIOS causes the Embedded Security Software to stop functioning and produce error messages	Hiding the TPM chip in the BIOS with Embedded Security software loaded stops functioning if Security Manager is launched in Windows. User will eventually see two errors indicating inability to connect to the TPM three minutes after the application hangs up.	Hiding the TPM in BIOS makes the TPM invisible to the ACPI table and Windows, and installed software cannot recognize the device. This behavior is as designed, as the Security Manager requires the TPM hardware. Customers wishing to avoid this behavior should re-enable their TPM or remove the HP Embedded Security software through **Add/remove programs**.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—An internal error has been detected restoring from Automatic Backup Archive	If the user 1. clicks **Restore under Backup** option of Embedded Security in HPPTSM to restore from the automatic backup Archive 2. 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 the SpSystemBackup.xml when the SpBackupArchive.xml is required, Embedded Security Wizard fails with: **An internal Embedded Security error has been detected**. 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. We are working to enhance this in future products.
HP ProtectTools Embedded Security—Security System 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. An error that a **decryption process failed** 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 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. Also, user must restore the entire system backup. An Archive Backup can be restored individually.
HP ProtectTools Embedded Security—After reinstalling Embedded Security, user sees general driver error	After reinstalling Embedded Security, either by setup.bat or through supplemental CD autorun, a general driver error is displayed when opening Security Manager, Embedded Security, user settings, configure, check PSD.	A reboot is not requested, but it is required. The reinstallation of Embedded Security produces this error if it is used before the computer is rebooted. HP is working on an enhancement to be made available in future product versions.
HP ProtectTools Embedded Security—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 **Security > Device security**, modify the field from **Hidden** to **Available**.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Numerous end-task errors during reboot after uninstalling	If the user uninstalls HP ProtectTools Embedded Security and waits a few minutes after the uninstall completes, when the user selects **Yes** to reboot, numerous end-task errors appear with Japanese (JP), Taiwanese (TW), Traditional Chinese (TZ). These end tasks include: • persistWnd • hkem.exe • conime.exe • ccapp • PSD • HP ProtectTools Embedded Security Icon tray	This occurs only on first uninstall attempt. Allow more time and the stalled process will successfully complete.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Embedded Security—Automatic backup does not work with 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 login, 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.
HP ProtectTools Embedded Security—Unable to disable Embedded Security State temporarily in 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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Credential Manager—No option to **Browse for Virtual Token** 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.
HP ProtectTools Credential Manager—Login with TPM authentication does not give the **Network Accounts** option	Using the **Network Accounts** 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.
HP ProtectTools Credential Manager—Credential Manager creates long account names that are truncated.	When registering a password in Credential Manager, the user can click **Options** and select **Prompt to select account for this application.** User must then enter a unique name for each document so Credential Manager can tell which password to apply. When creating these unique names, Credential Manager fills in the application name and the user enters the document name. In this window, the user can scroll to view the document name. When reopening the password-protected document, the document names cannot scroll. Credential Manager automatically fills in the application name; only 9 characters can be viewed when selecting the unique name.	HP is researching workaround for future product enhancements.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Credential Manager—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: **User account restriction**.	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 **Windows security > Change password** 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.
HP ProtectTools Credential Manager—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.
HP ProtectTools Credential Manager—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.
HP ProtectTools Credential Manager—Credential Manager does not recognize the **Connect** button	If the Single Sign On credentials for Remote Desktop Connection (RDP) are set to **Connect**, Single Sign On, upon relaunch, always enters **Save As** instead of **Connect**.	HP is researching a workaround for future product enhancements.
HP ProtectTools Credential Manager—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.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Credential Manager— When logging in using TPM authentication, the **Back** button skips the option to choose another authentication method	If user using TPM login authentication for Credential Manager enters his/her password, the **Back** button does not work properly, but instead immediately displays the Windows login screen.	HP is researching a workaround for future product enhancements.
HP ProtectTools Credential Manager—Credential Manager opens out of standby when it is configured not to	When **use Credential Manager log on to Windows** 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.	With no administrator password set, user cannot logon to Windows through Credential Manager because of account restrictions invoked by the Credential Manager. Without smart card/token: User can cancel the Credential Manager login and user will see the Microsoft Windows login. User can log in at this point. With smart card/token: The following workaround allows the user to enable/disable opening of Credential Manager upon smart card insertion. 1. Click **Advanced Settings**. 2. Click **Service & Applications**. 3. Click **Smart Cards and Tokens**. 4. Click when smart card/token is inserted. 5. Select the **Advise to log-on** checkbox.
HP ProtectTools Smart Card Manager—The option to **Require PIN at Boot** does not work	The **Settings** button, at **HP ProtectTools Security Manager > Smart Card Security > BIOS > Smart Card BIOS Password Properties**, is a function of the card properties, as the name states. This button is functional for any supported card placed in the reader. The button becomes grayed out if there is no smart card administrator or user password on the card and it is available if there is a password on the card. This allows the card owner to change the card PIN at boot properties at any time.	The message box that asks the operator for a PIN at boot time is then determined by the data on the card. This method requires the operator to have a card and optionally, determined by the card owner, know a PIN to gain access of the computer. For the computer power-on authentication to work, the **BIOS Security Mode**, at the top of the **Smart Card Security > BIOS** page must be enabled. If not enabled, the PIN at boot time will not have any functionality. HP is researching a resolution for next product offering.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Smart Card Manager—Smart card software displaying incorrect USB status	After unplugging the USB cable of the Smart Card terminal, the status remains ´blue.´ To get the correct status, ProtectTools Security Manager must be reopened.	Refresh the graphical user interface by closing and reopening the smart card software.
HP ProtectTools Smart Card Manager—Smart Card Security Manager allows user to enter Japanese characters for the name of the card owner, but Japanese name will be in garbage characters in authentication	If the customer set up the system to request PIN input, the BIOS screen stays on with garbage admin name and prompts for corresponding password, so the customer impact is not minimal. It may lead customer to type wrong password and lock up the system.	There is a BIOS limitation of available fonts/characters. Multi-byte characters stored on smart card are not correctly displayed. At this point, there is no real solution for this. HP is working to add information in product help files to further clarify this limitation in future product offerings.
HP ProtectTools Credential Manager—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.	This is as designed. 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.
HP ProtectTools Credential Manager—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.	This is as designed. If user wishes to modify operating system level settings for auto admin logon values for bypassing the edit path is: HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon ⚠ Use Registry Editor at your own risk! Using the Registry Editor (regedit) incorrectly can cause serious problems that may require you to reinstall your operating system. There is no guarantee that problems resulting from the incorrect use of Registry Editor can be solved.
HP ProtectTools Credential Manager— 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: **You can place your finger on the fingerprint reader to log on to Credential Manager**.	The purpose of the desktop alert is to notify the user that fingerprint authentication is available, if it is configured.

Software Impacted-Short description	**Details**	**Solution / Workaround**
HP ProtectTools Credential Manager—Credential Manager logon window for Windows 2000 states **insert card** when no reader is attached	The Windows Credential Manager Welcome screen suggests the user can logon with **insert card** when no smart card reader is attached.	The purpose of the alert is to notify the user that smart card authentication is available, if it is configured.
HP ProtectTools Credential Manager—Unable to log into Credential Manager after transitioning from sleeping to hibernation on Windows XP SP1 only	After allowing system to transition into hibernation and sleeping, 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 smart card) is selected.	This issue appears to be resolved in SP2 from Microsoft. Refer to Microsoft knowledge base article 813301 for more information on the cause of the issue. Customer Workaround: In order to logon, 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. If user logs into Windows first, then user must manually log into Credential Manager.
HP ProtectTools Credential Manager—Restoring Embedded Security causes Credential Manager to fail	Credential Manager fails to register any credentials after the TPM Embedded Security Module is restored.	The HP Credential Manager for ProtectTools fails to access the TPM if the TPM was reset to factory settings or replaced after the Credential Manager installation. Workaround: 1. Back up the user identity before replacing or resetting the TPM. 2. Uninstall the Credential Manager. 3. Enable and initialize the TPM. 4. Install the Credential Manager. 5. Restore the user identity. HP is investigating resolution options for future customer software releases.

Software Impacted-Short description	Details	Solution / Workaround
HP ProtectTools Credential Manager—Credentials are lost from Credential Manager when Embedded Security is uninstalled	The Embedded Security device encrypts and protects the credentials. Removing the Embedded Security software causes a loss of all encrypted data.	Users should regularly back up their credentials, as referenced in help files. The Credential Manager Backup and Restore options are available on the Credential Manager menu. If the user does not back up credentials prior to removing the embedded Security Manager, his/her credentials are lost. Users who have backed up encrypted credentials should: 1. Reinstall HP ProtectTools Embedded Security software. 2. Perform the restore option for both their Embedded Security device and their Credential Manager backup files.
HP ProtectTools Credential Manager—Security cannot register smart card in Credential Manager through the **More** option	Cannot register Smart Card in Credential Manager through the **My Identity > More > Register Credentials** option. User must use **Register Smart Card or Token** option.	This functionality was not originally designed into the product. This is being implemented in future product revisions being designed by HP.
HP ProtectTools Credential Manager—Security **Restore Identity** process loses association with virtual token	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.	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 logon, even if the client part of the token is restored through identity restore. HP is investigating long-term options for resolution.