HP ProtectTools Security Manager - 2008

Introduction

As computers become more mobile and better connected, and theft and security breaches occur more frequently, threats to data security are increasing in magnitude as well as complexity. Data security can have a direct impact on the health of your business, and most businesses rank security among their top concerns.

HP has a rich heritage in enterprise security and started devoting resources to solving the mobile security problem as soon as the trend started emerging. Taking a holistic approach to security, HP designed the HP ProtectTools Security Manager to bring many technology areas together in a way that helps ensure not only protection for PCs, but also that the PCs themselves do not become points of vulnerability that could be used to threaten the entire IT infrastructure.

HP ProtectTools Security Manager not only helps protect and prevent PCs from becoming points of vulnerability, it is also extensible and easy to use.

The security dilemma

Businesses trying to implement security policies for personal computing devices face numerous choices that may not always work well together and that can be difficult to deploy and use. If a technology is difficult to use, most users will avoid using it which further complicates the task of making personal computing devices secure. In addition, security solutions should provide a clear and demonstrable value to the user.

While security features increasingly rely on established industry standards and are better integrated with other elements of IT security, there are still requirements that must be met before widespread deployment and utilization can take place. These requirements include:

- **Usability** – security features must be easy to use
- **Manageability** – technologies and features must be easy to manage, and scalable from small businesses to large enterprises
- **Awareness** – IT managers and users must be made aware of a feature, and help should be provided to assist them in understanding its purpose
- **Interoperability** – IT managers and users should be made aware of features or services that span multiple technologies
- **Extensibility** – solutions must adapt as security needs grow and newer technologies and features become available

The HP ProtectTools security software suite addresses these requirements using a modular architecture that uses add-on software modules for functionality. As your business grows and security needs change, new security features can easily be added by installing new modules. HP ProtectTools Security Manager gives users access to all HP ProtectTools functionality from a single, easy-to-use software interface. HP ProtectTools is easily accessible from the Microsoft® Windows® task bar, and each plug-in module provides a high level overview of its purpose. Detailed help files provide additional information.

HP ProtectTools modules have corresponding manageable components (available separately) that were designed specifically with enterprise requirements in mind.

Basics of notebook and desktop security

HP ProtectTools features a number of capabilities based on a variety of standards-based technologies:

- Notebook and desktop computers can be configured to use passwords, smart cards or biometrics individually or in any combination to achieve multifactor authentication. Smartcard readers and biometric devices are standard on many HP business notebook models.
- The Trusted Platform Module (TPM), or embedded security chip designed to the Trusted Computing Group (TCG) standard, is available on a range of HP products.

In addition, HP Business notebooks and desktops include security features within the device BIOS, such as:

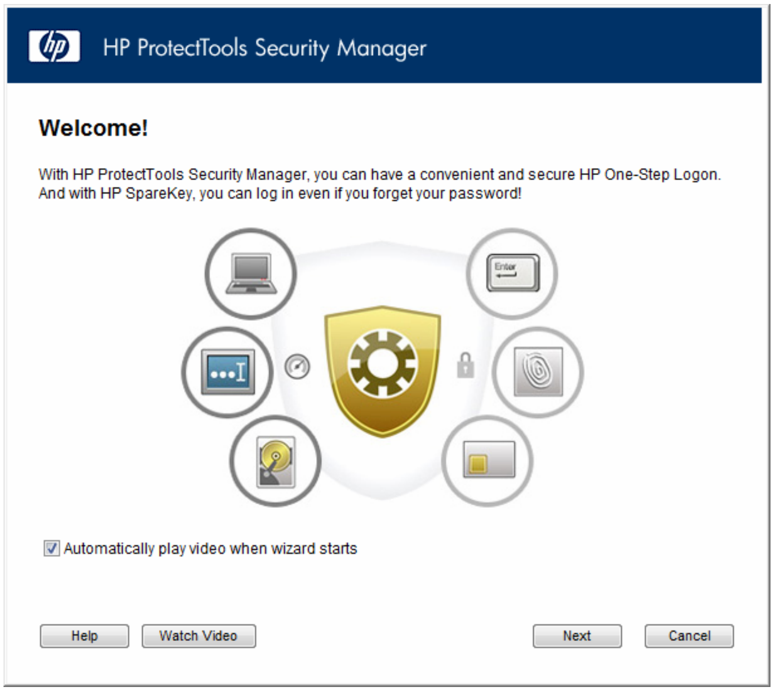
- Pre-Boot security – authenticates a user before allowing the operating system to boot.
- Enhanced Pre-Boot Security – *new* in business notebooks for 2008. Just type in only one password and that will log you directly into Windows. Enhanced pre-boot security that doesn't require you to remember and enter two different logon passwords every time you logon to your system. This feature synchronizes users with Microsoft Windows to allow multiple users as well as custom login policies for each user in the pre-boot environment. Advanced pre-boot authentication supports passwords, smartcards and biometrics individually or in combination to achieve multifactor authentication. The **One-Step logon** feature allows users to authenticate themselves once, and then logs the users all the way into Windows.
- HP SpareKey – *new* in business notebooks for 2008. HP SpareKey allows users to more securely log into their account even if they forget their password or lose their credentials[1]. HP SpareKey works by associating the users credential to three personal questions. In case of a forgotten password or a lost credential, the user can answer the three questions in order to gain access to the Windows account.
- Device configuration lock down – allows port control in BIOS that can be protected against modification by users without administrative access
- Remote management capabilities – allows administrators to remotely set BIOS security policies.

Setup Wizard for HP ProtectTools

Setting up security should be fast and easy. Getting started with HP ProtectTools is as easy as swiping your finger on the HP Fingerprint Sensor. This launches the Setup Wizard for HP ProtectTools and guides you through a short list of simple questions after which your notebook is protected.

Setup Wizard is designed to help you secure access to your computer via a password, smartcard or fingerprint sensor, and to safeguard the information on your hard drive using data encryption, securing both access and data for total information protection.

[1] Requires initial user setup.



Welcome!

With HP ProtectTools Security Manager, you can have a convenient and secure HP One-Step Logon. And with HP SpareKey, you can log in even if you forget your password!

☑ Automatically play video when wizard starts

Figure 1: HP ProtectTools Security Setup Wizard

The HP ProtectTools Security Setup Wizard is designed to setup notebook security in three easy steps.

1. Select the security level
    a. Windows level security
    b. Pre-Boot Security
    c. Drive Encryption
2. Select Login Method
    a. Windows Password
    b. Fingerprint
    c. HP ProtectTools Java Card
3. Review and commit your selections

HP ProtectTools Security Setup Wizard then does the rest. The security levels can be selected individually or in combination. At a minimum, HP recommends accepting the default setting of Windows level and Pre-Boot Security. For total protection, Drive Encryption should also be selected.

Login methods can also be selected either individually, or in combination to achieve multifactor authentication. The HP ProtectTools Java Card is itself a two factor authentication method, requiring both possession and a PIN in order to authenticate. Passwords and Fingerprints on the other hand are single factor authentication methods. To achieve multifactor authentication with passwords and fingerprints, users should consider combining them into a single login policy that requires both a password and a fingerprint.

Enhanced Pre-Boot Security

Pre-Boot security is a feature that requires users to authenticate themselves upon turning on the computer. This authentication takes place before the operating system is allowed to load. During Pre-Boot software is not allowed to run, and neither is booting from external devices such as optical drives or USB storage. This means that software designed to bypass the operating system password protection cannot run if the computer is protected using Pre-Boot Security.

For 2008, HP is introducing Enhanced Pre-Boot Security in Business Notebooks. Enhanced Pre-Boot Security now makes it possible to setup multiple users as well as multifactor authentication policies using a password, fingerprint or HP ProtectTools Java Card.

One-Step Logon

The One-Step Logon feature of Enhanced Pre-Boot Security is designed to integrate seamlessly into Windows authentication in order to provide users with a seamless logon into the operating system.

In essence, the user authenticates only once. The logon process uses the provided credentials to authenticate to the Pre-Boot environment, drive encryption and then all the way into the operating system. From a users standpoint therefore, it's the same login process as before, just during Pre-Boot instead of the operating system login.

HP SpareKey

HP SpareKey allows users to more securely log into their operating system account if they forget their password, lose their Java card or for some reason cannot use their fingerprint to login.

Users are asked to enroll in to HP SpareKey when they first login to the notebook. The enrollment process is easy and requires the user to answer any three questions out of a predetermined list of ten. These questions are designed to collect information that is unique to the user and does not change over time (i.e. Mother's maiden name, first school attended, etc.)

Answering the three questions completes the enrollment, and the user is now protected. In the case of a lost credential or forgotten password, the user can enter HP SpareKey and answer the previously selected questions. If the answers match, login continues. Upon completion of the login process, the user is asked to change the login credential with an option to accept or decline.

HP SpareKey security

Answers to HP SpareKey questions are encrypted and cannot be deciphered by an unauthorized person. The basic process for securing the questions is as follows

Step 1: Answers to the three questions are concatenated into a single text string, eliminating all spaces.
Step 2: The single text string is then used to derive an encryption key using a SHA1 hash function. This encryption key is mathematically unique to the three answers given by the user.
Step 3: The derived encryption key is then used to encrypt the login password, the encrypted password is then stored.

The answers to the three questions and the encryption key aren't stored in memory. The only way to access the encrypted password is to answer the same three questions with exactly the same responses used during initial enrollment.

What is enhanced about Enhanced Pre-Boot Security?

Pre-Boot security has been available for a number of years, and was designed for a single user environment. Enhanced Pre-Boot Security addresses the following issues with One-Step Logon and HP SpareKey:

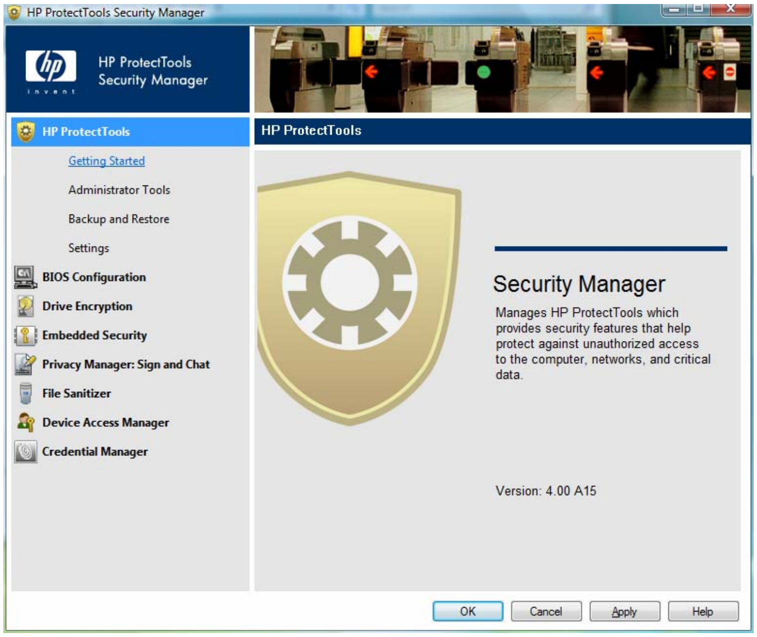
1. Multiple users, multiple factors. Previously, multiple users using the same machine had to use the same password for Pre-Boot access. Enhanced Pre-Boot synchronizes with the Windows operating system to let multiple users access the Pre-Boot environment with their unique credentials (username and password).

2. One-Step Logon ensures the user only has to authenticate once – and not multiple times as was previously required in Pre-Boot due to lack of operating system integration. (once in pre-boot and then again in the operating system).

3. HP Spare Key provides users with an easy to use means to recover passwords. Let's face it, people lose smartcards, and forget passwords. With standard Pre-Boot, there were two ways to recover. Some computers would allow password erase via access to the system board - this option was not secure. On other computers, the system board had to be replaced - this was usually not covered under warranty.

HP ProtectTools Security Manager

Your business requires protection against unauthorized PC access, as well as stronger protection for sensitive data that is stored locally or accessed over a network. At the heart of the security strategy for business notebooks, desktops and workstations is the HP ProtectTools Security Manager. This single client console application unifies the security capabilities of HP business notebooks, desktops and workstations under a common architecture and single user interface. Today, a range of features are being delivered that build on underlying hardware security building blocks such as embedded security chips designed to the TCG standard and smart card technology.



Security Manager

Manages HP ProtectTools which provides security features that help protect against unauthorized access to the computer, networks, and critical data.

Version: 4.00 A15

Figure 2 - HP ProtectTools Security Manager Console

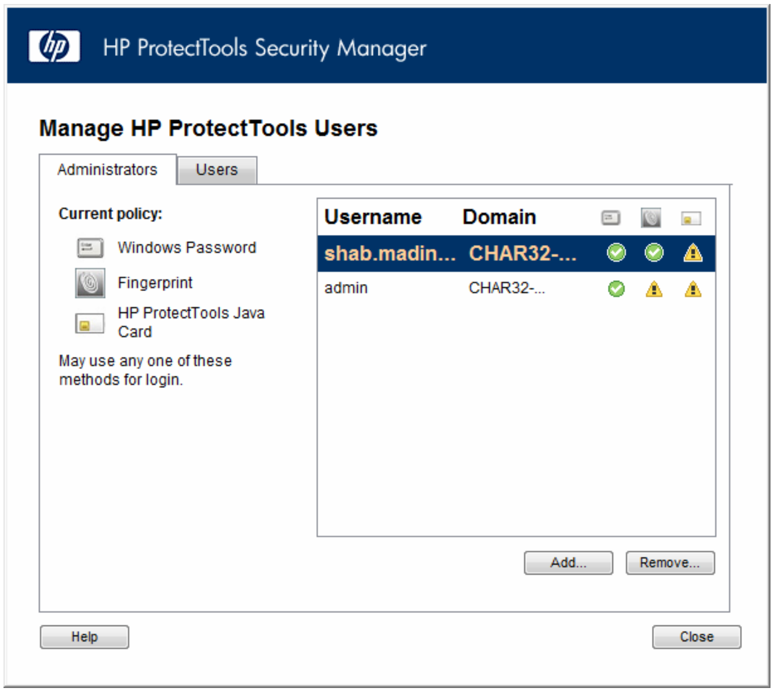
The HP ProtectTools Security Manager framework allows you to enhance security software functionality through add-on modules as your security needs change. This approach ensures that all new HP ProtectTools security modules introduced over time are highly integrated. Ultimately, you benefit from security features that are easier to use, manageable, and provide enhanced value by taking advantage of the multiple security hardware attributes of your HP business notebook, desktop or workstation.

HP ProtectTools Security Manager provides global functionality that is needed by the installed security modules, as well as security setup features such as the Setup Wizard, User Management and Security Backup and Restore.

User management

In an HP ProtectTools secured computer, security is built in from the ground up and completely integrated. There is no longer a separate pre-boot password, a separate drive encryption password and a separate operating system password as in previous security solutions. Security for the computer is holistic because all components work together to share users and credentials.

User Management, which is accessed from the Administrator Tools section of HP ProtectTools Security Manager, is designed to allow users to be created and deleted system wide.



HP ProtectTools Security Manager

Manage HP ProtectTools Users

Current policy:

- Windows Password
- Fingerprint
- HP ProtectTools Java Card

May use any one of these methods for login.

Username	Domain			
shab.madin...	CHAR32-...	✓	✓	⚠
admin	CHAR32-...	✓	⚠	⚠

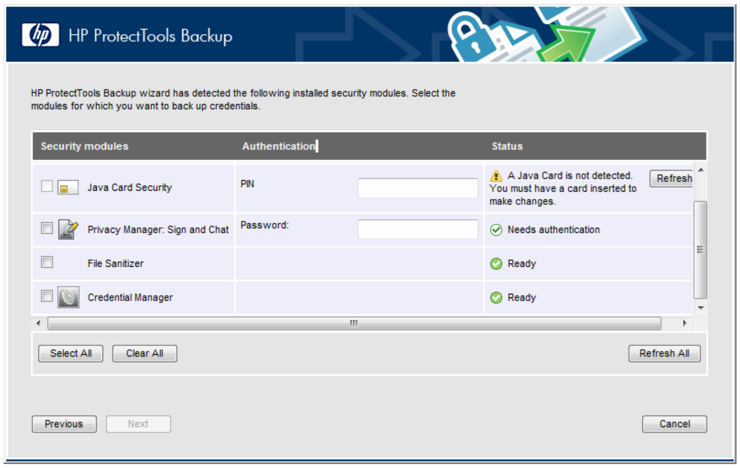
Figure 3 – HP ProtectTools User Management

In order to ensure that users and security policies are perfectly synchronized between the operating system and the pre-boot environment, users should always be added and deleted using the HP ProtectTools user management.

Backup and Restore

Good information security is not simply about the best technologies, it also requires best practices. Regular backup of security policies, encryption keys, credentials and certificates is a best practice that imposes a small administrative overhead in the short term, but can result in significant cost savings in the long run should a security instance occur. Therefore, Administrators should create policies where users are required to use this Backup and Restore feature on a regular basis.

HP ProtectTools Backup and Restore is not a user data backup solution. It is designed to simply backup security related data such as login credentials and encryption keys. The backup and restore process therefore only takes a few minutes.



HP ProtectTools Backup wizard has detected the following installed security modules. Select the modules for which you want to back up credentials.

Security modules	Authentication	Status
□ Java Card Security	PIN	A Java Card is not detected. You must have a card inserted to make changes.
□ Privacy Manager: Sign and Chat	Password:	✓ Needs authentication
□ File Sanitizer		✓ Ready
□ Credential Manager		✓ Ready

Figure 4 – HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore is accessed from the “Backup and Restore” section of HP ProtectTools Security Manager. HP ProtectTools Backup and Restore allows you to backup all security related data such as credentials and encryption keys.

Using HP ProtectTools Backup and Restore, users have the flexibility to:

- Perform a full HP ProtectTools backup, which backups data from all installed modules
- Perform a selective backup which allows selected modules to be backed up
- Backup on demand
- Scheduled backup
- Selective restore
- Full restore

Security Software Modules for HP ProtectTools

HP ProtectTools Security Manager is only the first step, the base security platform that gets its functionality through independent plug-in software modules. The following sections include more information about modules that:

- Provide better protection against unauthorized access to the PC, while making access to the PC and network resources simple and convenient for authorized users.
- Deliver a higher degree of data protection while the PC is turned off
- Protect communications such as emails and instant messaging
- Enable better protection against unauthorized access even before the operating system is loaded by leveraging underlying security technologies such as the TPM embedded security chip.
- Provide the ability to more securely delete files and personal information

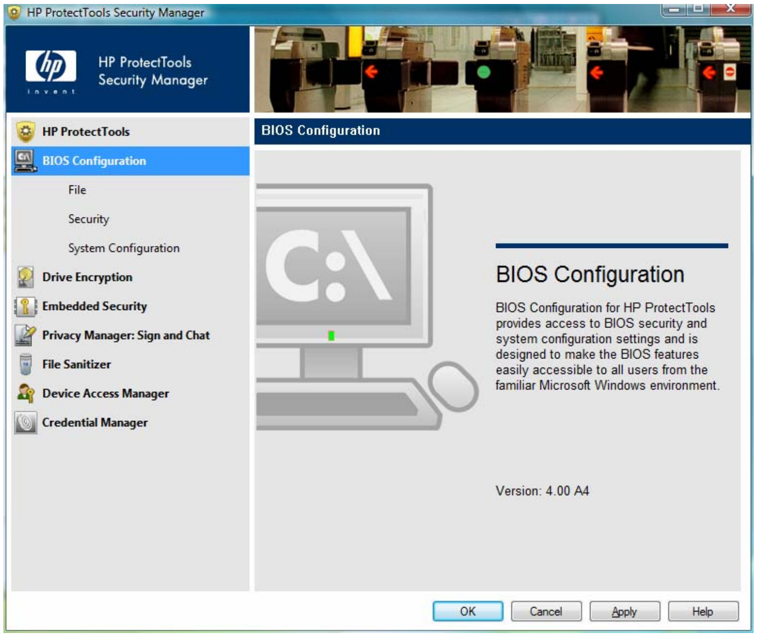
The modular architecture of the HP ProtectTools Security Manager enables additional modules to be selectively installed by the end-user or IT administrator, providing a high degree of flexibility to customize HP ProtectTools depending on security needs of the business and the underlying hardware configuration. Each additional module is a self contained security application providing targeted security functionality. Integrated into the HP ProtectTools Security Manager, these modules are specifically designed to work with and complement each other and form a holistic security solution.

- BIOS Configuration Manager for HP ProtectTools
- Credential Manager for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- File Sanitizer for HP ProtectTools *new* for 2008
- Privacy Manager: Chat and Sign *new* for 2008
- Java Card Security for HP ProtectTools

Going forward, as new security risks are identified, HP plans to continue to expand its PC security offerings with additional modules for the HP ProtectTools Security Manager.

BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools provides access to the BIOS security and configuration settings from within the HP ProtectTools Security Manager application. The BIOS on an HP client plays an important role in enhancing overall security. Some users may not be comfortable modifying BIOS settings through standard F10 access. The BIOS Configuration for HP ProtectTools module is designed to make these features easily accessible to all users from the familiar Microsoft Windows environment.



BIOS Configuration

BIOS Configuration for HP ProtectTools provides access to BIOS security and system configuration settings and is designed to make the BIOS features easily accessible to all users from the familiar Microsoft Windows environment.

Version: 4.00 A4

Figure 5 – BIOS configuration for HP ProtectTools

With BIOS Configuration for HP ProtectTools, authorized users can get access to power-on user and administrator password management, and they can configure pre-boot authentication features, such as smart card, power-on password and the TPM embedded security chip.

BIOS Configuration for HP ProtectTools also allows access to system configuration options such as port configuration, boot order options and built in device options.

Using BIOS Configuration for HP ProtectTools, authorized users can:

- Manage power-on administrator passwords
- Configure pre-boot authentication features such as automatic DriveLock and TPM Power-On authentication

- Enable/disable features such as HP SpareKey, CD-ROM boot.
- Configure boot options including disabling the ability to boot to drives other than the primary hard drive.

Table 1 - BIOS Configuration for HP ProtectTools Features and Benefits

Feature	Benefit
Works with HP ProtectTools Security Manager	User interface is fully integrated into the HP ProtectTools Security Manager.
Provides access to BIOS security and configuration features from within the operating system	Provides an easier to use alternative to the pre-boot BIOS configuration utility known as F10 Setup.
Protected Access	Requires the BIOS administrator password for settings modification if the administrator password has been set.
Enhanced security feature set that takes advantage of other HP ProtectTools supported security technologies such as smart cards and embedded security chips	Provides better protection against unauthorized access to the PC through features that help protect the system from the moment power is turned on. Embedded security chip pre-boot authentication requires that users securely authenticate to the chip prior to allowing the system to boot, which helps protect against attacks that exploit the ability to boot to alternative operating system environments. TPM-enhanced DriveLock protects a hard drive from unauthorized access even if removed from a system without requiring the user to remember any additional passwords beyond the embedded security chip user pass phrase. Working with Java Card Security for HP ProtectTools, pre-boot smart card authentication requires users to present their smart card prior to allowing the system to boot.

Enabling access to BIOS security configuration from within the HP ProtectTools Security Manager creates an integrated security solution and enables authorized users to control every aspect of security management from a single application with a common user interface. The following table describes the key BIOS security features[2] that become accessible from the HP ProtectTools Security Manager using the BIOS Configuration Module.

Table 2 - Key BIOS security features made accessible by the BIOS Configuration Module

Feature	Description	Benefit
TPM embedded security chip pre-boot authentication	Utilizes the embedded security chip for user authentication. Users need to input the basic user key pass phrase	Helps protect against unauthorized access to the PC by preventing access to the computer by booting from a device other than the primary hard drive. Provides security benefits similar to a power-on password; however, by allowing users to use their embedded security chip pass phrase, users are not required to remember an additional password.

[2] Pre-boot authentication features are available on select platforms. Refer to platform specific specifications for more details.

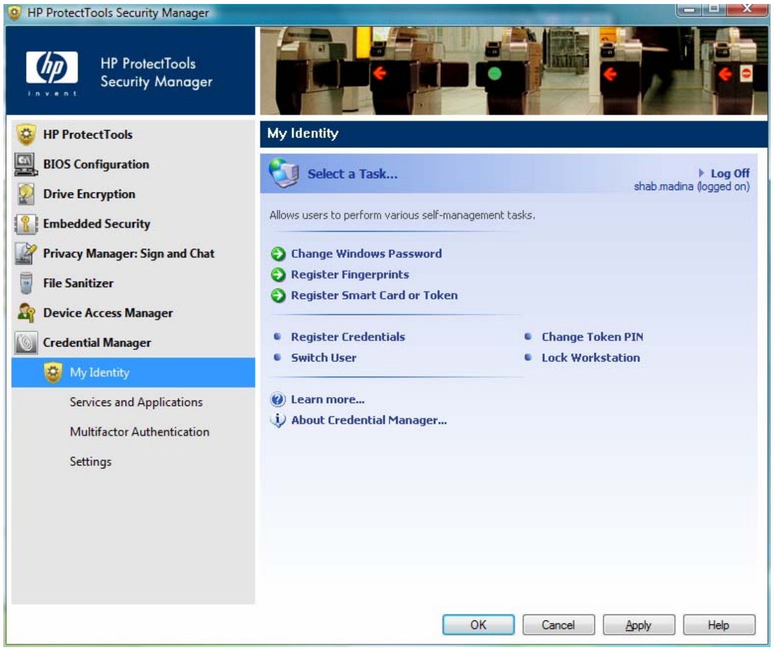
Feature	Description	Benefit
Automatic DriveLock	Requires a user to authenticate to the embedded security chip before a DriveLock protected hard drive can be accessed. A separate DriveLock password is not required.	Automatic DriveLock helps protect a hard drive from unauthorized access even if it is physically removed from a system. Allows very strong, random DriveLock passwords to be automatically set in a way that is completely transparent to users (does not require the user to remember another password) Ties a hard drive to a specific system with a specific embedded security chip, preventing other systems from accessing the hard drive if it is physically removed from the original system.

BIOS Configuration for HP ProtectTools is supported on most HP business notebooks, desktops and workstations. See Table 6 of this white paper for more information on support by platform.

Most HP Notebooks also have a built in feature called Disk Sanitizer. Disk Sanitizer enables more secure disposal or recycling of notebooks completely empting your hard drive of all sensitive information before you reassign or replace your PC. Both of these features meet government standards for data security, developed in accordance with the DOD 5220.22-M Supplement[3]. Since the Disk Sanitizer erases the entire hard drive, it is not accessible from BIOS Configuration for HP ProtectTools, and instead has to be accessed directly from the BIOS. For more information on Disk Sanitizer, please refer to the whitepaper titled "HP ProtectTools: Firmware security features in HP business notebooks", available for download at www.hp.com/products/security.

Credential Manager for HP ProtectTools

Credential Manager gives users the ability to specify how the different available security authentication methods will work together to provide increased protection against unauthorized access to the personal computer. It is the glue that brings the different security technologies together to create a specified behavior. In addition, Credential Manager also provides a single sign-on capability that automatically remembers credentials for websites, applications, and protected network resources, effectively serving as a personal password vault that makes accessing protected information more secure and convenient.



Allows users to perform various self-management tasks.

[3] For the use cases outlined in the DOD 5220.22-M Supplement.

Figure 6 – Credential Manager for HP ProtectTools

Key features of Credential Manager include:

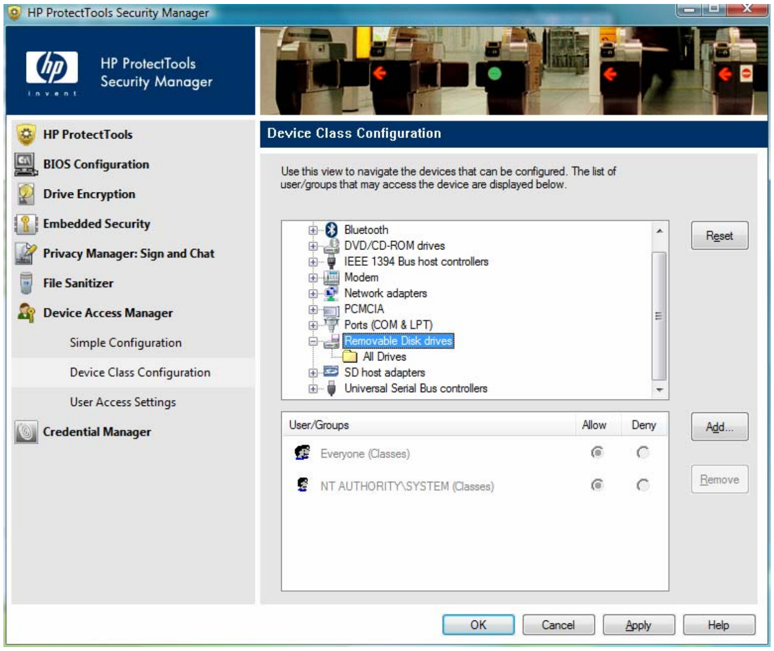
- Full integration into HP ProtectTools Security Manager
- Support for smart cards (including HP ProtectTools Java Cards), biometric fingerprint security, TPM embedded security chips, USB tokens, virtual tokens and passwords
- Single sign-on capability manages and protects passwords for websites, applications and network resources
- Application Protection allows administrators to manage applications. This includes giving users or user groups permission to run an application or to block it. Application access can also be controlled based on times and dates, as well as requiring user authentication before an application can be run. This feature is ideal for computers in shared environments.

Table 3 - Credential Manager for HP ProtectTools Features and Benefits

Feature	**Benefit**
Multifactor authentication support	Brings together the available (integrated and add-on) security technologies on a PC into a cohesive and unique behavior that utilizes these technologies to authenticate users based on user preferences.
Microsoft Windows logon capability	Enables the use of any supported security technology to logon to Windows providing a more secure and convenient alternative to password authentication.
Single sign-on manages user credentials for websites, applications and protected network resources	Users no longer need to remember multiple passwords for protected websites, applications and network resources. Single sign-on works with multifactor authentication capabilities to add additional protection requiring users to re-authenticate when accessing particularly sensitive data. Registering new websites, applications or network logon dialogues is fully automated making it easy for users to begin taking advantage of the added convenience and security of the single sign-on feature.
Application Protection	Allows the control and management of applications. This includes giving users or user groups' permission to run an application or to block it. Application access can also be controlled based on times and date, as well as requiring user authentication before an application can be run. This feature is ideal for computers in shared environments.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools speaks to HP's strong commitment to security and its ability to respond to customer needs with innovative solutions. A common assumption with today's PC usage model is that users who are authorized to log on to a personal computer and access sensitive data are also able to copy or print that information. In reality, this is not always the case. Companies may need to allow users to view sensitive data, but restrict their ability to copy or print that data. Device Access Manager for HP ProtectTools solves that problem and in doing so, enables a new usage model for personal computing devices.



Use this view to navigate the devices that can be configured. The list of user/groups that may access the device are displayed below.

User/Groups	Allow	Deny
Everyone (Classes)	●	○
NT AUTHORITY\SYSTEM (Classes)	●	○

Figure 7 – Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools has two configuration options: Simple Configuration and Advanced Configuration

Simple Configuration

The Simple Configuration option is a collection of common options that can be configured with a single selection. These options include:

- Limit access to all Removable Media
- Limit access to all DVD/CD-ROM Drives
- Limit access to all Bluetooth devices
- Limit access to all 1394 devices

Advanced Configuration

By default Device Access Manager allows all devices for all users. This ensures a normal experience for users operating without the need for administrative oversight.

The Advanced Configuration option demonstrates the true power of Device Access Manager. By using these settings, policies can easily be created to implement security requirements to meet complex business processes and policies. IT Managers can also create device and peripheral usage profiles based upon the individual user, such as - user type, individual device or even establish a black list of devices for individual users, or a class of users.

If Device Control is needed however, Device Access Manager creates a “black list” of devices for individual users, or a class of users. Through Advanced Configuration, Device Access Manager presents a device tree view derived from the Windows Device Manager. Individual devices or an entire class of devices from the device tree can be selected. Access to the selected device can then be restricted by applying the policy to selected users or class of users.

This level of configurability enables new client usage models, such as described in the scenarios below:

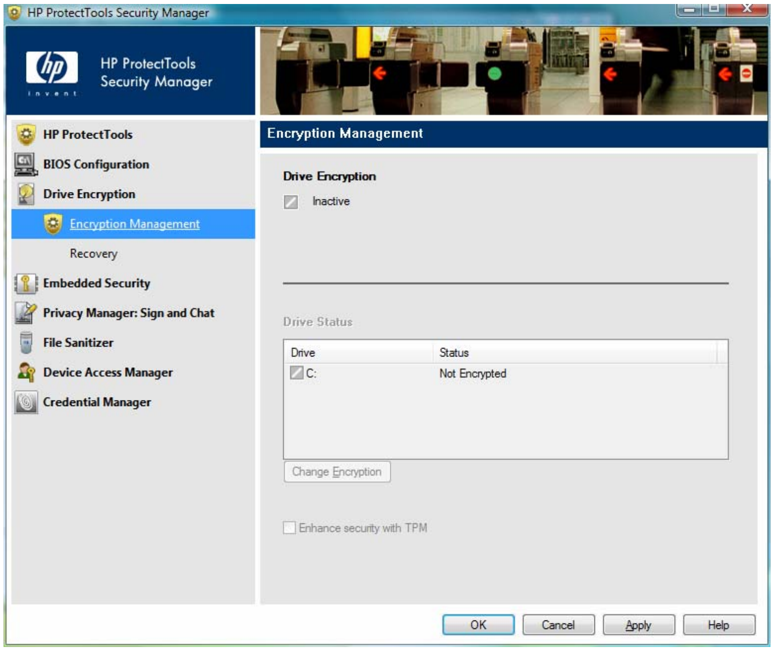
- Scenario 1: In a call center environment, call takers have full access to sensitive product and pricing information. The company however wants to protect this data and ensure that it is not removed from the premises. This can be accomplished by creating a Device Access Manager policy that prevents removable storage devices such as USB keys and writeable optical drives from being used by unauthorized users.

- Scenario 2: A company is making sensitive financial information available to an auditor and wants to protect this information from being copied or removed from the notebook. Device Access Manager can allow a policy where this user is denied access to any removable storage devices or printers.

Device Access Manager for HP ProtectTools is offered on business notebooks and desktops as a single user client version. However, an enterprise version of Device Access Manager (HP ProtectTools Device Manager) is also available that allows the same policies to be configured and deployed remotely. For information on HP ProtectTools Device Manager, please refer to www.hp.com/hps/security/products/

Drive Encryption for HP ProtectTools

Drive Encryption is a full volume encryption (FVE) solution that encodes all information on the hard drive volume so it becomes unreadable to an unauthorized person. FVE is currently the preferred way to protect data on a hard drive. With Drive Encryption, you can select which drives to encrypt and add, remove and set various access levels for different users.



Drive Encryption

▨ Inactive

Drive Status

Drive	Status
▨ C:	Not Encrypted

☐ Enhance security with TPM

Figure 8: Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools is based on SafeBoot FVE technology. SafeBoot (McAfee) is a leading provider of powerful encryption and strong access control software that seamlessly integrates with existing standards-based enterprise systems.

Encrypting the hard drive

The hard drive on a new HP business notebook or desktop is unencrypted. The encryption process can be activated by launching HP ProtectTools Security Manager and selecting Drive Encryption for HP ProtectTools. If HP ProtectTools is not installed on your notebook or desktop, it can be downloaded free of charge from the business notebook and desktop sections of www.hp.com. For a list of supported notebooks and desktops, refer to Table 6 of this white paper.

Before a hard drive can be encrypted, Drive Encryption for HP ProtectTools requires that the encryption key is backed up. This is a simple and fast process, and only requires access to a USB flash drive. The key backup ensures that if the password is ever forgotten, it can be reset using the backed-up key on the USB flash drive.

HP has collaborated with SafeBoot to create the Drive Encryption Key Recovery Service. This service allows users to back up their encryption keys to a remote location managed by SafeBoot. If the password is lost or forgotten, users worldwide can call the service in order to recover their password. Users are prompted to subscribe to this service when they activate the Drive Encryption for ProtectTools module. If they choose to subscribe, they will be automatically guided through the subscription process. Successful registration results in an email to users with a confirmation of the subscription and a telephone number to call in case of a lost password.

Hard drive encryption process

The hard drive encryption process is transparent and continues in the background. The time it takes to encrypt the entire drive will depend on the size of the partition, and how the notebook is being used (i.e. number and type of applications open). However, while the drive is being encrypted, the user can continue to work normally. If the notebook is shutdown during encryption, encryption will continue upon system restart.

Full enterprise capability

The Drive Encryption for HP ProtectTools module is designed with enterprise extensibility in mind. HP has collaborated with SafeBoot to make their enterprise FVE solution available for enterprise customers to be deployed in a managed IT environment. SafeBoot has accumulated years of experience in the FVE market, and has applied this knowledge to their enterprise software, which has advanced management and helpdesk capability.

The SafeBoot enterprise solution provides vital auditing and compliance reporting to meet legislation/compliance requirements to prove that the personal computing device has been encrypted and that data was encrypted should the PC be lost or stolen. The auditing and reporting capabilities provide an up-to-date status of every device, user and security policy.

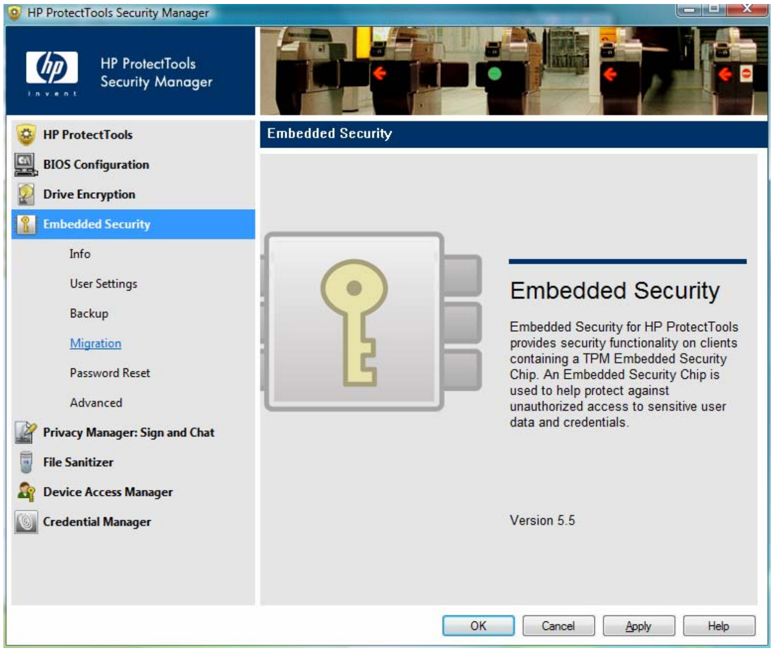
Customers demand that their data security solution integrate unobtrusively into their existing enterprise infrastructure. The SafeBoot enterprise solution is designed for minimal impact on daily operations and to be non-intrusive to the network, especially in large-scale implementations. It delivers a small, 3MB file to the PC, while the core functionality remains in the Management Center. SafeBoot provides connectors to infrastructures based on PKIs, such as Microsoft and Entrust, and directories including Active Directory and Novell NDS.

The SafeBoot enterprise solution synchronizes password changes to all machines assigned to each user. SafeBoot includes a scripting engine to allow support for any login system, including Windows smart card login. Additionally, the SafeBoot suite of encryption and access control solutions integrate seamlessly with ActivIdentity's authentication technology to secure enterprise-wide data on hard drives and in files and folders. ActivIdentity is a member of the SafeBoot Certified Token Partners Program and collaborated with HP on the development of the Java Card Security for HP ProtectTools module and the HP ProtectTools Java Card.

For additional details on SafeBoot's enterprise solutions please visit: http://mcaffe-safeboot-enteprise.com

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools is an add-on software module that allows users to configure how they would like to use the TPM embedded security chip. This add-on module is intended for HP business notebooks, desktops and workstations configured with a TPM embedded security chip designed to the TCG standard. Embedded Security for HP ProtectTools version 4.0 or later supports the latest TPM v1.2 as well as the previous TPM v1.1.



Embedded Security

Embedded Security for HP ProtectTools provides security functionality on clients containing a TPM Embedded Security Chip. An Embedded Security Chip is used to help protect against unauthorized access to sensitive user data and credentials.

Version 5.5

Figure 9 - Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools uses the TPM embedded security chip to help protect against unauthorized access to sensitive user data and credentials. Features that can be accessed through Embedded Security for HP ProtectTools include:

- Administrative functions such as taking ownership and managing the owner pass phrase
- User functions such as user enrollment and management of user pass phrases
- Configuration options including setting up enhanced Microsoft Encrypted File System (EFS) and Personal Secure Drive for helping to protect user data as well as functions such as backing up and restoring the key hierarchy as well as key migration.

Embedded Security for HP ProtectTools is supported on all HP business notebooks, desktops and workstations configured with a qualified TPM embedded security chip. See Table 6 of this white paper for more information on support by platform.

Table 4 – Embedded Security for HP ProtectTools Features and Benefits

Feature	**Benefit**
Works with HP ProtectTools Security Manager	User interface is fully integrated into the HP ProtectTools Security Manager. Increases the functionality of the entire security solution. For example, if the embedded security chip is present, Credential Manager for HP ProtectTools can use it to further secure the encryption keys that encrypts sensitive user credentials.
Designed to the Trusted Computing Group (TCG) standard	As a standards-based technology, embedded security chips are designed to work with a growing number of third party software solutions while providing a platform to support future hardware and operating system architectures.
Supports Microsoft CAPI and PKCS#11 cryptographic software interfaces	Enables the embedded security chip to enhance a broad range of existing applications and solutions that take advantage of these interfaces (for example, Microsoft Outlook®, Netscape Navigator, RSA SecurID and public key infrastructures solutions from leaders like Microsoft, Verisign and Entrust.)

Feature	Benefit
Enhanced Microsoft EFS	Helps protect sensitive user data stored locally on a PC, where access to Microsoft EFS encrypted files are protected by the embedded security chip providing a higher degree of hardware-based protection.
Enhanced Personal Secure Drive (PSD)	Personal Secure Drive (PSD) is an encrypted mountable volume. In Embedded Security for HP ProtectTools version 4.0 and later, PSD has been enhanced with a significantly larger size limit. The PSD can now occupy the entire hard drive (minus 5GB for system files). PSD can now also be created on removable storage devices such as USB hard drives, and USB flash drives.
Password Reset	Allows administrators to reset a lost user password.
Automatic Backup	Allows automatic backups of TPM Embedded Security Credentials, Settings and Personal Secure Drive (PSD). Backups can be created on local drives as well as network drives. This ensures that TPM protected user data can be recovered in case of a service event.

For more information on trusted computing solutions from HP, including more information on the embedded security chip solution for HP business desktop, notebook and workstation PCs, visit www.hp.com/go/security.

File Sanitizer for HP ProtectTools

Files dropped into the recycle bin on your Windows desktop can easily be recovered by simply opening the recycle bin and restoring the files. Even once the recycle bin is emptied, the files remain on the hard drive and can be recovered using disk utilities available online.

File deletion process

When you delete a file, it is removed from the hard drive directory. The process is quick, and requires the same amount of time regardless of the size of the file. Removing the link to the file from the directory makes the space occupied by the file available to new files. The deleted file however, continues to reside on the hard drive and can be recovered until it is overwritten by another file. Normal file deletion process, while fast and convenient, also poses a security threat as deleted information could be recovered by an unauthorized person.

File sanitization

File sanitization (also referred to as shredding) is a process where the data designated to be erased is overwritten multiple times with meaningless bits in order to help ensure that it cannot be recovered. File sanitization is a more intensive process and helps ensure the deleted data can not be recovered.

Free space bleaching

Free space bleaching is a process where previously used space on a hard drive is overwritten to help ensure no deleted data can be recovered.

File Sanitizer for HP ProtectTools starts by placing an icon on the desktop. You can then shred files by simply dragging and dropping onto the File Sanitizer icon. You can also define files and folders that you want shredded automatically, and define the schedules.

Using File Sanitizer for HP ProtectTools

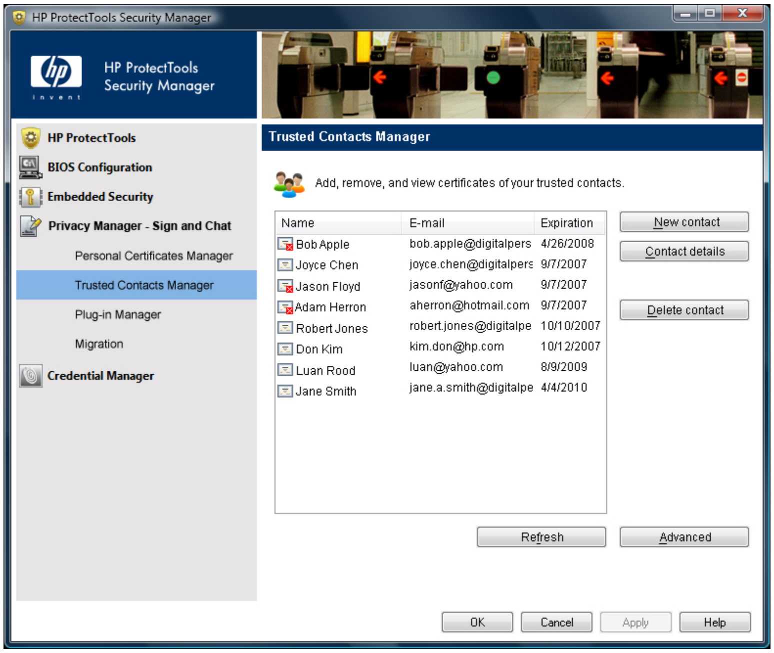
File sanitization is more intensive process than simple file deletion. The amount of time it takes to delete a file or a group of files is in direct relation to their size. File Sanitizer is therefore not a replacement for simple file deletion, it is instead meant to complement it.

While you can use the file sanitizer to drag and drop files, certain types of information can be marked for automatic shredding. This level of control is available in File Sanitizer settings, where security levels can be selected as well custom control over types of information to erase (i.e. cookies, temporary files etc.). File Sanitizer can then be setup to erase the predefined files based on events such as Windows shutdown.

Free Space Bleaching can also be setup to bleach the hard drive at a predetermined schedule.

Privacy Manager for HP ProtectTools

When it comes to information security, concerns typically revolve around lost or stolen notebooks, or unauthorized access to the network. However, information can easily fall into the wrong hands through seemingly harmless, normal everyday communications tools such as instant messaging and email. Privacy Manager for HP ProtectTools enables you to secure the documents and emails you create within Microsoft Office applications, and also provides stronger privacy control of Instant Messaging (IM) chats when communicating via Microsoft Live Messenger. Privacy Manager assures you that only those friends, clients or colleagues you select will be able to open and read a given document, email or IM. Conversely, recipients can be certain that messages and documents they receive have been created by you and have not been tampered with. Privacy Manager accomplishes all of this by leveraging the strong, multifactor user-authentication features provided by HP ProtectTools . The result is that you can now take a much more proactive approach to ensure the privacy, security and integrity of the information you create and communicate regardless of where it may ultimately be transmitted or stored.



Trusted Contacts Manager

Add, remove, and view certificates of your trusted contacts.

Name	E-mail	Expiration
Bob Apple	bob.apple@digitalpers	4/26/2008
Joyce Chen	joyce.chen@digitalpers	9/7/2007
Jason Floyd	jasonf@yahoo.com	9/7/2007
Adam Herron	aherron@hotmail.com	9/7/2007
Robert Jones	robert.jones@digitalpe	10/10/2007
Don Kim	kim.don@hp.com	10/12/2007
Luan Rood	luan@yahoo.com	8/9/2009
Jane Smith	jane.a.smith@digitalpe	4/4/2010

Figure 11 – Privacy Manager for HP ProtectTools

How Privacy Manager works

Privacy Manager is an HP ProtectTools plug-in, and can be accessed directly from within Microsoft Office 2007 and Microsoft Live Messenger. Upon first use, a wizard will guide you through the process of obtaining a digital certificate. HP has collaborated with Comodo, a leading issuer of digital certificates, to provide HP Privacy Manager users with a certificate at no cost, valid for one year. The certificate will be issued and sent to the email address you provide, thus certifying you have access to that email account.

Next, you will be prompted to invite your friends, colleagues or clients to be a Trusted Contact. Once the invitation is sent, they will get an email from you which will direct them to download the Privacy Manager software for free from DigitalPersona. They will then also be able to obtain a certificate at no charge. You are now setup to more securely communicate with each other:

- You can digitally sign emails and documents using passwords, fingerprints or smartcards. The digital signature is proof that the content was created by you, and has not been modified since being signed.
- You can encrypt Microsoft Office documents, worksheets and email messages ensuring they can only be viewed by your trusted contacts.
- You can incorporate signature lines into your Microsoft Office documents and worksheets to indicate your request for a digital signature by your recipients. This provides a simple method for authorization workflow.
- You can verify the identity of a person before starting a conversation using Windows Live Messenger, so you can be certain that the person you intend to chat with is the one sitting at the other end.
- You can maintain privacy in your Live Messenger conversations. You can be certain that the only person reading your messages is who you intend.

Privacy Manager for business

Privacy Manager is designed to integrate seamlessly into Microsoft Office applications. Content created in Microsoft Office can be digitally signed and encrypted, in order to ensure that only trusted contacts can view the content, and to ensure that the document was not modified after being signed.

Privacy Manager has clear benefits for businesses of all sizes. In addition to basic certificates which certify just an email address, Comodo can issue certificates which certify the real name and identity of the user. When businesses purchase this service, Comodo will formally validate that the administrator making the request has the authority to issue user certificates on behalf of the domain. This administrator will be given access to a management console used to request certificates for any employees. These certificates will now certify the user's actual identity, such as their name, title and email, so that their use can serve as a strong part of audit and compliance requirements.

Enterprises may also consider the deployment of a server to centrally manage policies and enable users to easily use their certificates from any computer on the network. DigitalPersona offers DigitalPersona Pro, a client/server solution to better manage authentication credentials and Privacy Manager on Active Directory-based networks.

Privacy Manager – Chat

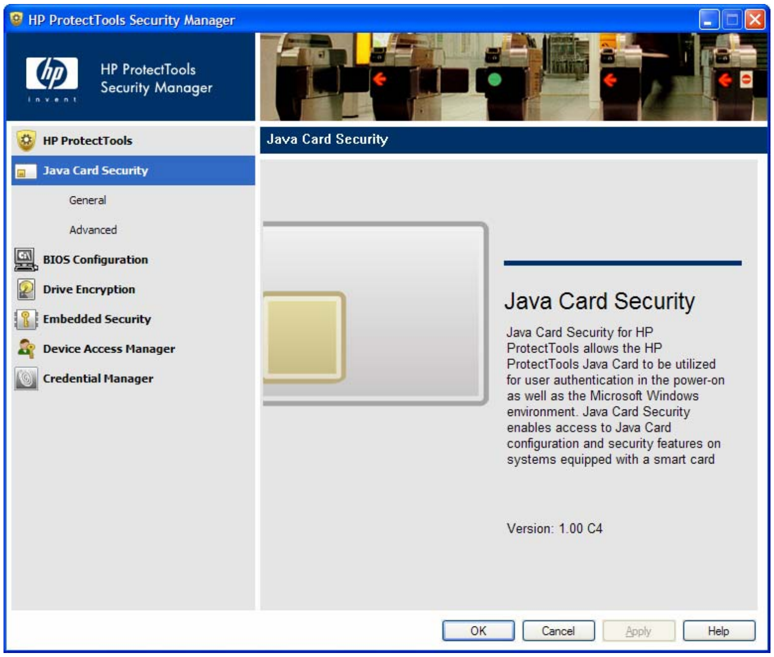
Think about using instant messaging to communicate. All messages are transferred unprotected and go through remote servers. Files transferred using instant messaging are also unprotected and go through remote servers. For this reason, many businesses disable instant messaging in their environments. While that takes care of the security exposure, it also prevents the benefits of a very useful communications tool.

Privacy Manager for HP ProtectTools adds extensions to MSN Live Messenger to allow for secure communications. With Privacy Manager – Chat, a user can continue using MSN Live Messenger, but with additional security. Privacy Manager – Chat uses the integrated fingerprint sensor to establish a person's identity. Even on systems without a fingerprint sensor, smartcards or passwords can be used to confirm identities. In an open office environment where you don't know if the person you are communicating with is who you think it is, Privacy Manager – Chat allows you to request identity confirmation.

Privacy Manager – Chat also adds a secure communications mode where all messaging and files are encrypted before they are transferred. Only the authorized recipient of these messages has the ability to decrypt and view them. If these messages are intercepted, they will be unreadable by the unauthorized person.

Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools allows the HP ProtectTools Java Card to be utilized for user authentication in the pre-boot as well as the Microsoft Windows environment. Java Card Security enables access to Java Card configuration and security features on systems equipped with a smart card reader. Smart card readers can either be integrated into the system, or can be added using the PC card slot on notebooks or connected via a USB port on any computing device equipped with one. For authentication, users are required to use the HP ProtectTools Java Card which can hold their passwords and PIN, and a supported reader, such as an integrated smart card reader, the HP PC Card Smart Card Reader, or the HP Smart Card Keyboard.



Java Card Security

Java Card Security for HP ProtectTools allows the HP ProtectTools Java Card to be utilized for user authentication in the power-on as well as the Microsoft Windows environment. Java Card Security enables access to Java Card configuration and security features on systems equipped with a smart card

Version: 1.00 C4

Figure 5 – Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools provides card management features such as:

- Separate administrator and user roles
- Ability to initialize and configure an HP ProtectTools Java Card, which enables the HP ProtectTools Java Card to be used for user authentication
- Interface with the BIOS to enable/disable Java Card pre-boot authentication
- Capability to configure separate Java Cards for administrators and users
- Set and change the Java Card PIN
- Backup and restore credentials stored on the Java Card

Table 5 - Java Card Security for HP ProtectTools Features and Benefits

Feature	**Benefit**
Compatible with many 3rd party applications	Uses the standard ActivIdentity profile with extensions for HP ProtectTools. This makes the HP ProtectTools Java Card compatible with many 3rd party enterprise security applications in addition to providing Pre-boot and Microsoft Windows authentication on HP notebooks and desktops. Standard ActivIdentity profile also makes the HP ProtectTools Java Card manageable using ActivIdentity's suite of enterprise solutions.
Initialize and configure Java Card security features such as pre-boot Java Card authentication.	Provides a complete Java Card security solution for pre-boot and Windows user authentication providing enhanced protection against unauthorized of the PC.
Backup and restore credentials stored on a user's Java Card.	Provides a mechanism to recover from a situation where a user or administrator loses the Java Card.
Provides the ability to configure an administrator Java Card that can be used on multiple systems to access BIOS configuration settings.	Allows an administrator to configure a single Java Card (or multiple cards) that can be used to securely access BIOS configuration settings without requiring the use of a BIOS administrator password.

Platform Support

HP ProtectTools Security Manager is supported across a range of HP business notebooks, desktops and workstations. The following tables provide details of support for HP business notebooks and desktops.

Table 6 – HP ProtectTools solution set support for business notebooks, desktops and workstations

Business Notebooks	**Standard Series (s)**	**Business Series (b)**	**Professional and Workstation Series (p, w)**
Hardware support			
• TPM Embedded Security Chip		●	●
• HP fingerprint sensor		●	●
• Integrated Smart Card reader (optional)		●	●
• HP Privacy Filter Support (optional)		●	●
HP ProtectTools support			
HP ProtectTools Security Suite	●	●	●
HP ProtectTools Security Setup Wizard	●	●	●
• Credential Manager for HP ProtectTools	●	●	●
• Drive Encryption for HP ProtectTools	●	●	●
• Java Card Security for HP ProtectTools	●	●	●
BIOS Configuration for HP ProtectTools		●	●
Privacy Manager (Chat and Sign)		●	●
File Sanitizer for HP ProtectTools		●	●
Embedded Security for HP ProtectTools		●	●
Device Access Manager for HP ProtectTools		●	●
Additional security support			
Enhanced Pre-Boot Authentication	●	●	●
Multiuser	●	●	●
Multifactor (password, fingerprint, smart card)		●	●
HP SpareKey	●	●	●
One-Step Logon	●	●	●
HP Disk Sanitizer	●	●	●
Computrace Support	●	●	●
Enhanced DriveLock		●	●

Business Desktops	**dc7600**	**dc5700**	**dc5750**	**dc7700**
Hardware support				
TPM Embedded Security Chip v.1.1	N	N	N	N
TPM Embedded Security Chip v.1.2	SF	SF	SF	SF
SF = Standard Feature / OF = Optional Feature / N = Not Available				
HP ProtectTools support				

Business Desktops	dc7600	dc5700	dc5750	dc7700
HP ProtectTools Security Manager	A	A	A	P
Credential Manager for HP ProtectTools	A	A	A	P
BIOS Configuration for HP ProtectTools	A	A	A	P
Embedded Security for HP ProtectTools	A	A	A	P
Java Card Security for HP ProtectTools	A	A	A	W
Computrace / Lojack for Laptops – for Desktops	S	S	S	S

Workstation Platforms	xw4400	xw6400	xw8400	xw9400
Hardware support				
TPM Embedded Security Chip v.1.1	N	N	N	N
TPM Embedded Security Chip v.1.2	S	S	S	S
HP ProtectTools support				
HP ProtectTools Security Manager	A	A	A	P,W
Credential Manager for HP ProtectTools	A	A	A	P,W
BIOS Configuration for HP ProtectTools	A	A	A	P,W
Embedded Security for HP ProtectTools	A	A	A	P,W
Smart Card Security for HP ProtectTools	A	A	A	N

A = After Market Option / P = Pre-install / N = Not Supported
S = Supported / W = Web Release

Frequently Asked Questions

Q. What add-on modules are currently available for HP ProtectTools Security Manager?

A. Currently the following modules are available. More modules will be developed and released in the future.

- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- Credential Manager for HP ProtectTools
- BIOS configuration for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Privacy Manager for HP ProtectTools
- Java Card Security for HP ProtectTools
- Device Access Manager for HP ProtectTools

Q. What authentication technologies are supported by HP ProtectTools?

A. HP ProtectTools Security Manager is a security platform that has been designed to easily grow with the user's needs. It supports the following authentication technologies currently, but can easily support additional technologies as they become available.

- Smart card authentication (HP ProtectTools Java Card)
- Biometric (fingerprint) authentication
- USB token
- Virtual token
- Password authentication

Q. How does smart card security compare to biometric security?

A. HP business PCs and software support both smart card authentication and biometric authentication. HP business notebooks offer both integrated smart card readers as well as integrated biometric sensors. Each has a specific applicability to task, and as a general guideline, HP recommends smart cards in high security or managed environments, and biometric security where convenient security is the objective.

Q. Which HP platforms support HP ProtectTools and the different add-on modules?

A. Please refer to the "Platform Support" section of this white paper.

Q. Is there is a cost associated with HP ProtectTools?

A. HP ProtectTools and security modules are available as standard security features on all business notebooks. On business desktops, some modules are available at additional cost. For details on ProtectTools availability on business desktops, please refer to the “Platform Support“ section of this white paper.

Q. Can smart cards be used for pre-boot authentication?

A. Yes, HP business notebooks support smart card pre-boot authentication. Supported cards include the HP ProtectTools Smart Card and the HP ProtectTools Java Card. Please refer to the user documentation that came with your computer for steps to configure the system for smart card pre-boot authentication.

Q. How can I tell if my PC contains a TPM embedded security chip?

A. If the PC contains a TPM embedded security chip, it will be listed in the Windows Device Manager, under the category "System Devices". On business notebooks, the TPM embedded security chip will be listed as "Infineon Trusted Platform Module"

Q. If a TPM encrypted file is copied moved to a second system which does not have the key to decrypt the file, what would happen to the file. Would it remain on the second as an unreadable file or would it be automatically deleted? Would the user of the second system be able to delete the file even if he does not have the decryption keys? Is there a solution to automatically delete such files?

A. This depends on the application being used to move data from one system to the other. If the application reads the data, repackages it and sends to another platform (say you email an encrypted file on your system), then the data/file is typically read/accessed by your email program, thereby unencrypting it. Now the email program may indeed encrypt the data across the internet if that option is selected, but the TPM is no longer in the picture protecting data. This is true of any data on your system encrypted by MSFT EFS (Microsoft's Encrypting Filesystem where TPM can be used to protect the file/folder encryption keys) and also same for files encrypted within PSD ("ProtectTools'" Personal Secure Drive). It is possible to have file remain encrypted no matter where it resides but typically in those types of applications the file is changed. For instance from "hello.doc" to hello.doc.enc" or some way of showing then that actual file is encrypted and a separate program must process the file before it's readable.

Q. Regarding the TPM chip itself, does it store any user specific information? If so, how can one clear it?
A. There is no user data in the TPM, however if required, the TPM can be cleared via F10 BIOS to return to factory default/cleared state.

Q. What is the Credential Manager module for HP ProtectTools?

A. Please refer to the "Credential Manager for HP ProtectTools" section of the white paper.

Q. How does Credential Manager differ from other single-sign-on solutions?

A. Most technologies and features provided by HP ProtectTools Security Manager are individually available. The value of HP ProtectTools is that it brings these technologies together into a single easy to use security solution. As an HP ProtectTools add-on, the features provided by Credential Manager are integrated into HP ProtectTools and work with the user authentication features of HP ProtectTools.

Q. Does Credential Manager for HP ProtectTools use the embedded security chip if available?

A. Yes, Credential Manager uses the embedded security chip, if available, to encrypt passwords stored in the password vault.

Q. Does Credential Manager for HP ProtectTools support multiple users on a single client device?

A. Yes, Credential Manager works on the concept of "identity". In order to log on to a computer, a user simply needs to create a Credential Manager ID.

Q. What if a user has multiple Microsoft Windows accounts?

A. This would function the same as multiple users on a single PC. The user would have to create a different identity for each account.

Q. What is the difference between user and administrator rights for Credential Manager for HP ProtectTools?

A. An administrator has full rights to all Credential Manager Configuration options. A user can use the Credential Manager for authentication and use the single sign-on features, but does not have access to the Authentication and Credential configuration or the Advanced Settings.

Q. If multiple PCs are used by the same user, can his or her identity be used on the different machines?

A. No, however a user's credential can be copied in order to be used on another PC.

Q. Is Credential Manager supported on non-HP computers?

A. Credential Manager for HP ProtectTools requires HP ProtectTools to be present on the system. If the client device is running HP ProtectTools, it will support Credential Manager.

Q. Is the HP ProtectTools security software suite available on a non-Microsoft Windows environment?

A. Currently HP ProtectTools is supported on Microsoft Windows Vista® and Microsoft Windows XP.

Q. What type of smart card is needed for HP ProtectTools?
A. Credential Manager for HP ProtectTools will support any smartcard card provide it comes with a PKCS#11 component. Most smartcards do, and before selecting a smartcard, this should be one of the questions that should be asked. Credential manager also has native support for the HP ProtectTools Java Card.

Q. If the HP ProtectTools Java Card is locked due to the incorrect PIN retries exceeding maximum, (5 incorrect entries). Is there a way to reactivate it?
A. The HP ProtectTools Java Card is blocked after the number of incorrect PIN entries exceeds 5, in order to protect against a dictionary attack in which someone enters different PINs systematically until a match is found. Once the Java Card is locked, there is no way to unlock it. It is therefore recommended that the Java Card be backed up, so a duplicate can be created is the original is locked.

Q. What is the process for uninstalling HP ProtectTools?
A. The process is the same as uninstalling any Windows application:

From the Windows Control Panel, select "Add Remove Programs"

- Remove the following ProtectTools components if they exist

- HP ProtectTools Security Suite
- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- Credential Manager for HP ProtectTools
- BIOS configuration for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Privacy Manager for HP ProtectTools
- Java Card Security for HP ProtectTools
- Device Access Manager for HP ProtectTools

Q. Is HP Disk Sanitizer available as a product, available standalone or only as part of HP ProtectTools? Where is the information about the hardware it might or might not work on?

A. HP Disk Sanitizer is a feature built into every business notebook BIOS, 2006 and later. There is nothing to purchase or download, it's simply there. The HP ProtectTools Embedded Security whitepaper provides additional details on this feature.

Q. Is the HP ProtectTools security software suite supported on iPAQ handheld devices?

A. iPAQ handheld devices also offer HP ProtectTools security, however HP ProtectTools for iPAQ is a separate application with features suited to handheld device security.

For more information

To learn more about HP ProtectTools, contact your local HP sales representative or visit our website at:
www.hp.com

www.hp.com/products/security

5982-9847EN, Rev 5, 07/2008