HP ProtectTools Security Software 2010

Technical white paper

Table of contents

Introduction 2

HP ProtectTools security software overview 2

HP security setup wizard 4

User management 5

Backup and restore 5

Security software components for HP ProtectTools 6

- Credential Manager for HP ProtectTools 7
- Central management for HP ProtectTools 8
- Device Access Manager for HP ProtectTools 9
- Drive Encryption for HP ProtectTools 11
- HP Enhanced Pre-Boot Security 12
- Embedded Security for HP ProtectTools 14
- Face Recognition for HP ProtectTools 15
- File Sanitizer for HP ProtectTools 16
- Computrace® LoJack Pro for HP ProtectTools 17
- Privacy Manager for HP ProtectTools 17
- Smart Card Security for HP ProtectTools 19

Platform Support 20

Frequently Asked Questions 21

For more information 25

Introduction

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

HP has a rich heritage in enterprise security and started devoting resources to solving the mobile security problem as soon as the trend emerged. Taking a holistic approach to security, HP designed HP ProtectTools security software to provide protection for PCs, and to ensure that PCs do not become points of vulnerability that threaten the entire IT infrastructure. HP ProtectTools security software not only helps protect PCs and prevent them from becoming points of vulnerability, it is also extensible, easy to use, and centrally manageable.

HP ProtectTools security software overview

Security concerns are inherent with the trend towards mobility, but we cannot let security concerns slow mobility adoption. That is why HP decided to invest heavily in building a strong security portfolio. Our goal is to offer our customers the most comprehensive standard security features out of the box of any client PC manufacturer.

HP ProtectTools for Microsoft® Windows® includes a complete suite of features that work together to protect access to your notebook or desktop computer, protect the data on it, and protect the network you connect to. HP ProtectTools security software provides security features that help protect against unauthorized access to the computer, networks, and critical data. Enhanced security functionality is provided by several HP ProtectTools software modules.

Table 1 shows the three pillars of security and HP ProtectTools solutions for each.

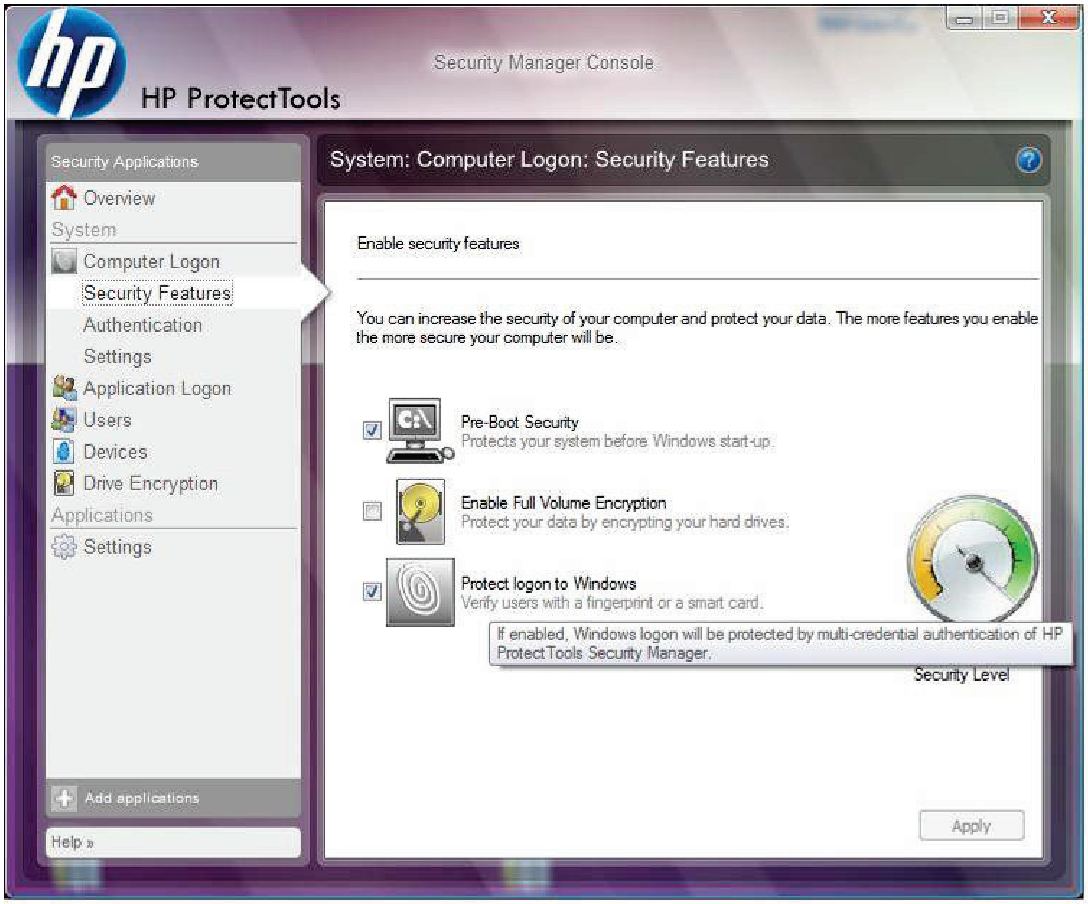
Table 1. Three pillars of security and HP ProtectTools integrated solutions for total information protection

Access protection (strong authentication)	Data protection (data at rest)	Communications protection (data in motion)
Integrated fingerprint sensor, facial recognition, and smartcard reader	Drive Encryption (full volume encryption standard with every business notebook)	Credential Manager single sign-on feature keeps passwords in a vault and automatically enters them when required
Enhanced pre-boot security (multiple users, multiple factors)	Device Access Manager prevents unauthorized copying of files to removable drives	Privacy Manager allows more secure communication via instant messaging (IM) and email
HP SpareKey can recover users from lost credentials after initial user setup	File Sanitizer allows you to securely delete files from hard drive so they cannot be recovered in accordance with the DOD 5220.22-M Supplement	

HP ProtectTools can be accessed from a single, easy-to-use software interface. It is easily accessible from the Windows® task bar, start menu, or desktop gadget. Each plug-in module provides a high level overview of its purpose. The desktop gadget also indicates the overall security status of your computer using an easy to understand color code. Detailed help files provide additional information.

HP ProtectTools Security Manager is at the heart of the security strategy for business notebooks, desktops and workstations. This single client console application unifies the security capabilities of HP business notebooks, desktops and workstations under a common architecture and single user interface (Figure 1).

Figure 1. HP ProtectTools Security Manager Console



System: Computer Logon: Security Features

Enable security features

You can increase the security of your computer and protect your data. The more features you enable the more secure your computer will be.

☑ Pre-Boot Security
Protects your system before Windows start-up.

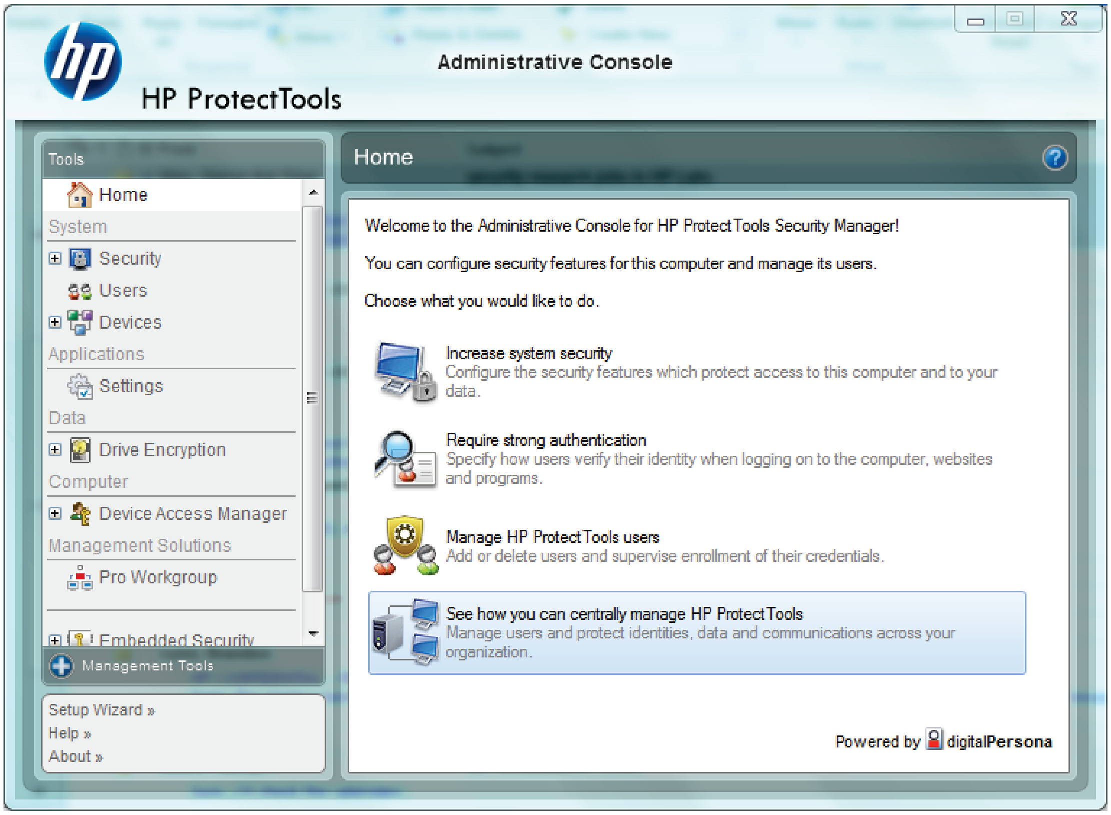
☐ Enable Full Volume Encryption
Protect your data by encrypting your hard drives.

☑ Protect logon to Windows
Verify users with a fingerprint or a smart card.

If enabled, Windows logon will be protected by multi-credential authentication of HP ProtectTools Security Manager.

HP ProtectTools is also centrally manageable at the workgroup or enterprise level using either DigitalPersona Pro Workgroup or DigitalPersona Pro Enterprise management solutions. Organizations have many security needs, which can create a management challenge. Central management allows administrators to create role based security policies, decide how users log on, remotely recover users who have lost their credentials, or revoke user credentials, all from a single control point. HP ProtectTools with DigitalPersona Pro provides a single management platform for multiple security applications. Client software for legacy computers allows deployment throughout the entire organization. Mixed deployments of HP ProtectTools and DigitalPersona Pro client software can be managed through a single management tool (Figure 2).

Figure 2. HP ProtectTools Administrative Console



Welcome to the Administrative Console for HP ProtectTools Security Manager!

You can configure security features for this computer and manage its users.

Choose what you would like to do.

Increase system security
Configure the security features which protect access to this computer and to your data.

Require strong authentication
Specify how users verify their identity when logging on to the computer, websites and programs.

Manage HP ProtectTools users
Add or delete users and supervise enrollment of their credentials.

See how you can centrally manage HP ProtectTools
Manage users and protect identities, data and communications across your organization.

Powered by digitalPersona

The HP ProtectTools Security Manager framework allows you to adapt HP ProtectTools 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 the personal computing device.

HP ProtectTools Security Manager provides global functionality needed by the installed security modules, as well as security setup features such as the setup wizard, user management and security backup and restore.

HP security setup wizard

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 or clicking the desktop gadget. This launches the setup wizard for HP ProtectTools and guides you through a short list of simple questions after which your notebook is setup protected. The setup wizard is designed to help you secure access to your computer via a password, smartcard, fingerprint sensor, or face recognition. It allows you to safeguard the information on your hard drive using data encryption, securing both access and data for total information protection.

Security levels can be selected individually or in combination. At a minimum, HP recommends accepting the default setting of W indows level and Pre-Boot Security. For total protection, Drive Encryption can also be selected. The setup wizard then does the rest.

Login methods can also be selected either individually or in combination to achieve multifactor authentication. The HP ProtectTools Java Card is a two factor authentication method, requiring both possession and a PIN to authenticate. Passwords, fingerprints, and face recognition are single factor authentication methods. To achieve multifactor authentication with these methods, users can use them in combinations such as fingerprint with password.

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. Security is global to the computer and users exist in Windows as well as in the pre-boot environment.

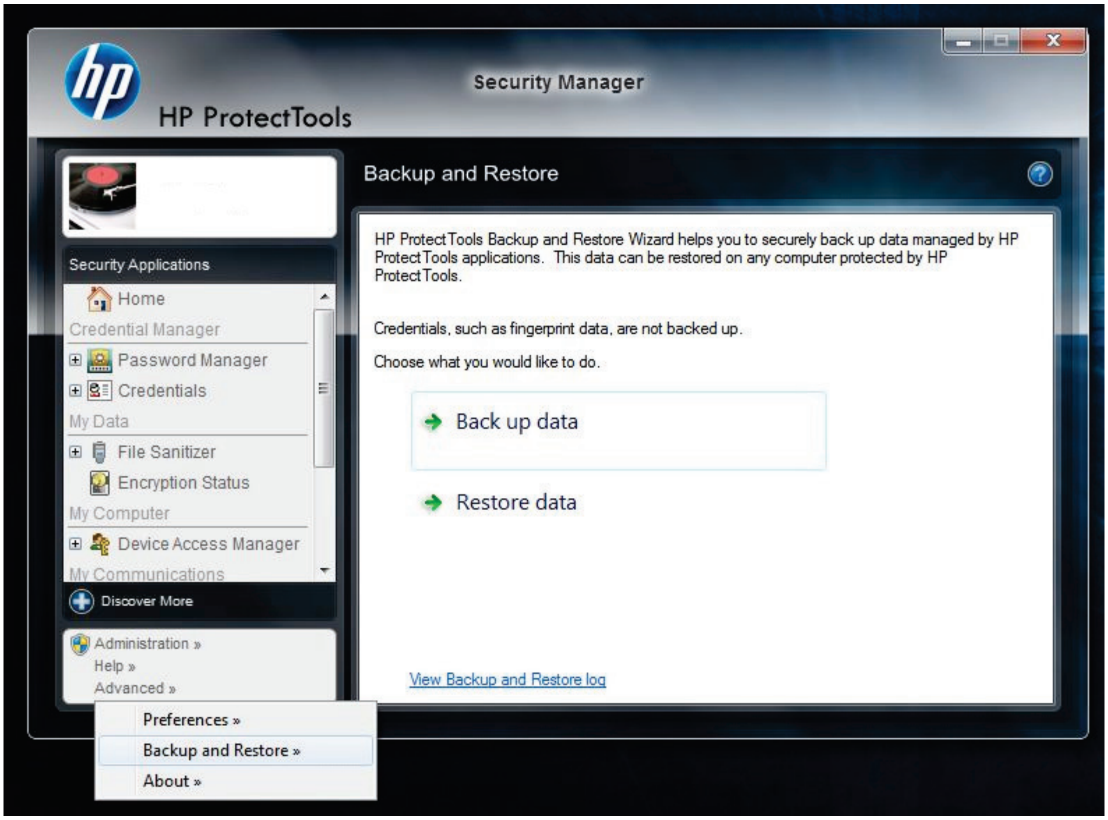
User management, accessed from HP ProtectTools Administrative Console, is designed to allow you to create and delete ProtectTools users system wide. To ensure that users and security policies are synchronized between the operating system and the pre-boot environment, users should always be added and deleted using 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 small administrative overhead in the short term, but can result in significant cost savings in the long run.

HP ProtectTools Backup and Restore is not a user data backup solution. It is designed to backup security related data such as login credentials and encryption keys. Therefore, the backup and restore process only takes a few minutes. Backup and Restore is available from the Security Manager by clicking on the Advanced link (Figure 3).

Figure 3. HP ProtectTools Security Manager Backup and Restore menu



HP ProtectTools Backup and Restore Wizard helps you to securely back up data managed by HP ProtectTools applications. This data can be restored on any computer protected by HP ProtectTools.

Credentials, such as fingerprint data, are not backed up.

Choose what you would like to do.

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
- Selective Restore
- Full Restore

Security software components for HP ProtectTools

The modular architecture of the HP ProtectTools Security Manager enables add-on components to be selectively installed by the end user or IT administrator. This provides a high degree of flexibility to customize HP ProtectTools depending on security needs and the underlying hardware configuration. Each add-on element is a self contained security application providing targeted security functionality. Integrated into HP ProtectTools Security Manager, these applications form a holistic security solution. They are specifically designed to work with and complement each other. These elements include:

- Credential Manager for HP ProtectTools
- Central Management for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- Face Recognition for HP ProtectTools

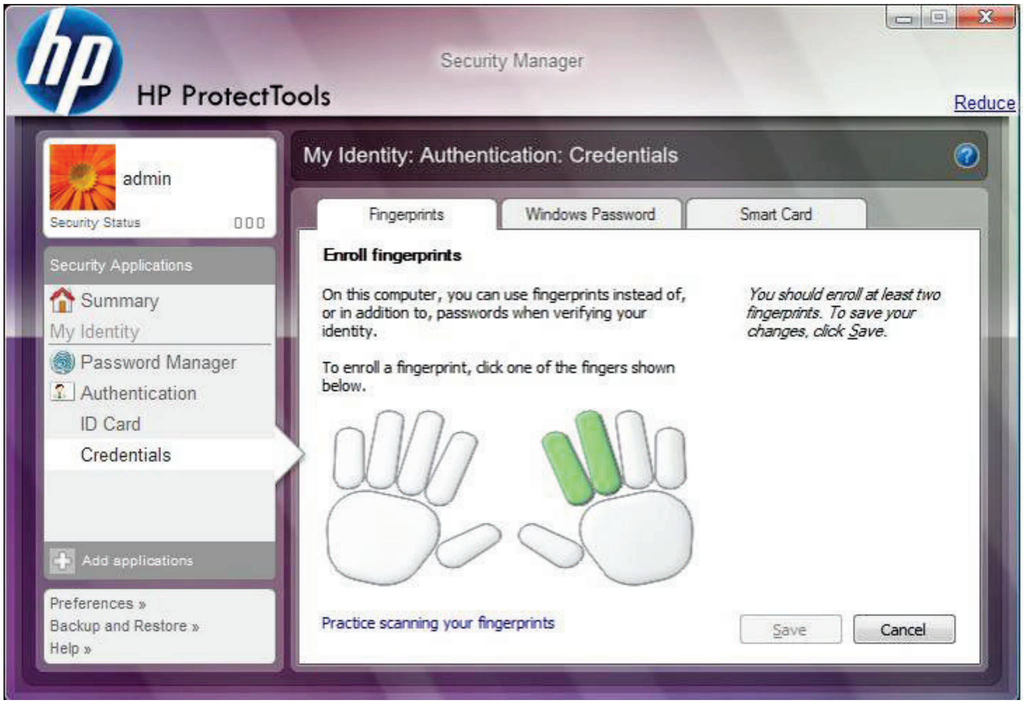
- File Sanitizer for HP ProtectTools
- Computrace® LoJack Pro for HP ProtectTools
    - Tracking and recovery requires a fee based subscription and setup. For details and country availability, please visit www.absolute.com/products/lojackforlaptops.
- Privacy Manager for HP ProtectTools

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

Credential Manager for HP ProtectTools

Credential Manager gives users the ability to specify how the different available security technologies will work together to provide increased protection against unauthorized access to the personal computer (Figure 4). It is the glue that brings the different security technologies together to create a specified behavior.

Figure 4. Credential Manager for HP ProtectTools



Enroll fingerprints

On this computer, you can use fingerprints instead of, or in addition to, passwords when verifying your identity.

To enroll a fingerprint, click one of the fingers shown below.

You should enroll at least two fingerprints. To save your changes, click Save.

Through Credential Manager, users can create a unique security behavior that requires their chosen authentication method, including alternatives to passwords when logging on to Microsoft® Windows. Credential Manager also provides single sign-on capability that automatically remembers credentials for websites, applications, and protected network resources. Credential Manager includes a personal password vault that makes accessing protected information more secure and convenient.

Key features of Credential Manager include:

- Full integration into HP ProtectTools Security Manager
- Centrally manageable

- 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

Table 2 shows the features and benefits of Credential Manager for HP ProtectTools.

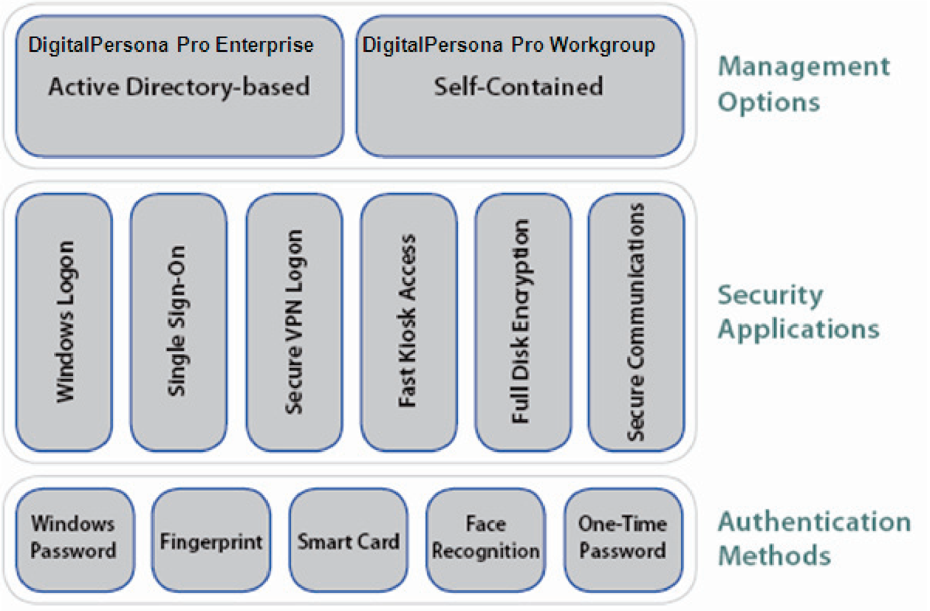
Table 2. Credential Manager for HP ProtectTools features and benefits

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 simple, making it easy for users to begin taking advantage of the added convenience and security.

Central management for HP ProtectTools

Central Management for HP ProtectTools is developed in partnership with DigitalPersona, and is available in two configurations: DigitalPersona Pro Enterprise and DigitalPersona Pro Workgroup. Central Management allows administrators to create and deploy role based policies, revoke access and recover users with lost credentials. DigitalPersona Pro Enterprise is designed for small to medium businesses and enterprises that use Active Directory. It allows administrators to leverage Active Directory for maximum scalability. Figure 5 shows the key features of HP ProtectTools with DigitalPersona Pro. DigitalPersona Pro Workgroup makes central management accessible to smaller organizations without Active Directory through simplicity of design and deployment, and attractive per seat cost. DigitalPersona Pro Workgroup is a self-contained solution with no special server hardware requirements. It makes security easy to deploy by allowing administrators to create role based policies and implement them within the workgroup. Security keys are managed centrally and allow the administrator to recover users with lost credentials. DigitalPersona Pro Workgroup can be accessed directly from HP ProtectTools and can be deployed for up to five users with no per seat cost.

Figure 5. Key features of HP ProtectTools with DigitalPersona Pro



DigitalPersona Pro protects applications and data by simplifying security controls for multiple applications. It provides for strong authentication to boost accountability and deter fraud. It simplifies auditing with comprehensive logging. By consolidating point management tools into one console, organizations are able to automate processes and reduce costs from passwords and provisioning. Table 3 shows the major features of HP ProtectTools with DigitalPersona Pro.

Table 3. HP ProtectTools with DigitalPersona Pro central management features and benefits

Feature	Benefit
Support for other PCs	Deploy HP ProtectTools-compatible client on legacy or non-HP PCs
Security policy synchronization	Keep security policies and settings the same across PCs
Strong authentication	Combine passwords, smart cards, fingerprints, face recognition
Access recovery	Unlock pre-boot, disk encryption and PCs for forgotten passwords or smart cards
Single Sign-on (SSO)	Enable stronger security for password-based enterprise and web applications
Secure communications	Sign or encrypt email and documents quickly and easily
Audit login	Simplify forensics and compliance

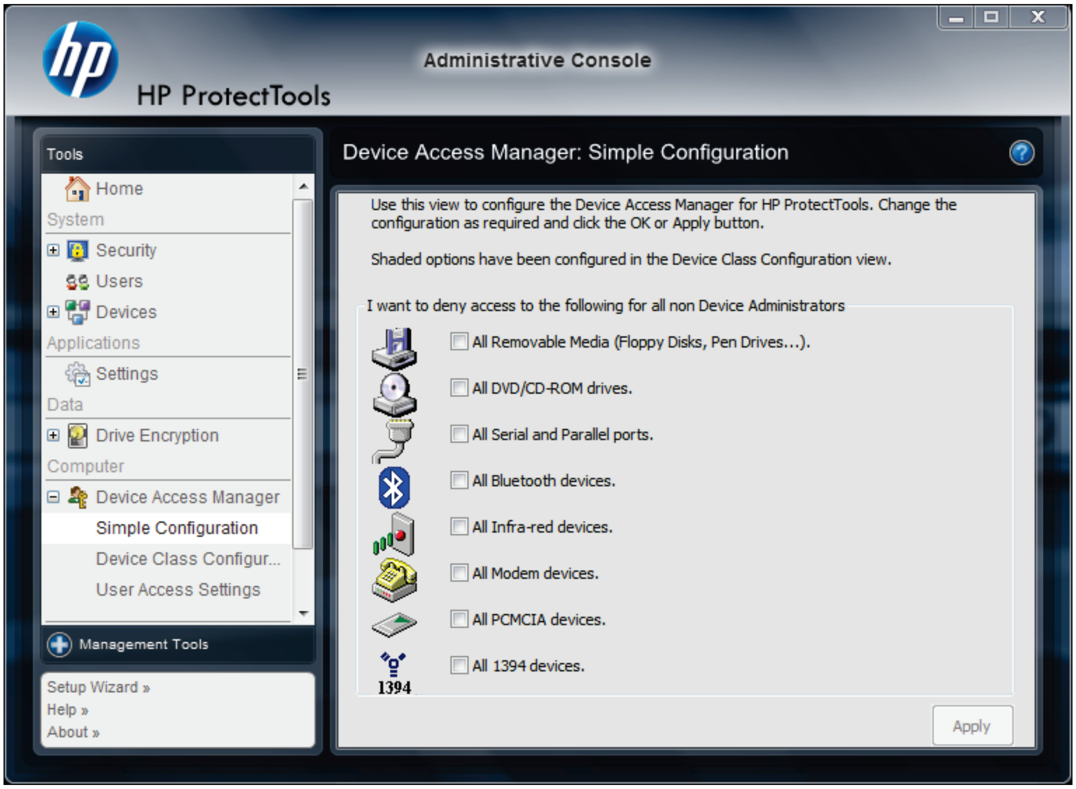
Device Access Manager for HP ProtectTools

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 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 that data. Device Access

Manager for HP ProtectTools solves that problem. In doing so, it enables a new usage model for personal computing devices.

Device Access Manager for HP ProtectTools has two configuration options: Simple Configuration (Figure 6) and Advanced Configuration.

Figure 6. Device Access Manager for HP ProtectTools Administrative Console



Device Access Manager: Simple Configuration

Use this view to configure the Device Access Manager for HP ProtectTools. Change the configuration as required and click the OK or Apply button.

Shaded options have been configured in the Device Class Configuration view.

I want to deny access to the following for all non Device Administrators

- □ All Removable Media (Floppy Disks, Pen Drives...).
- □ All DVD/CD-ROM drives.
- □ All Serial and Parallel ports.
- □ All Bluetooth devices.
- □ All Infra-red devices.
- □ All Modem devices.
- □ All PCMCIA devices.
- □ All 1394 devices.

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

Device Class Configuration

The Device Class Configuration option is where the true power of Device Access Manager lies. Using Device Class Configuration, policies can easily be created to implement complex security requirements as well as complex business processes.

Using Device Class Configuration, IT Managers can create device and peripheral usage profiles based on the individual user, user type, individual device or device class. Device Access Manager for HP ProtectTools allows all devices for all users by default. This ensures a normal experience for users who don't require device control. If Device Control is needed however, Device Access Manager creates a black list of devices for individual users, or a class of users. Through Device Class

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:

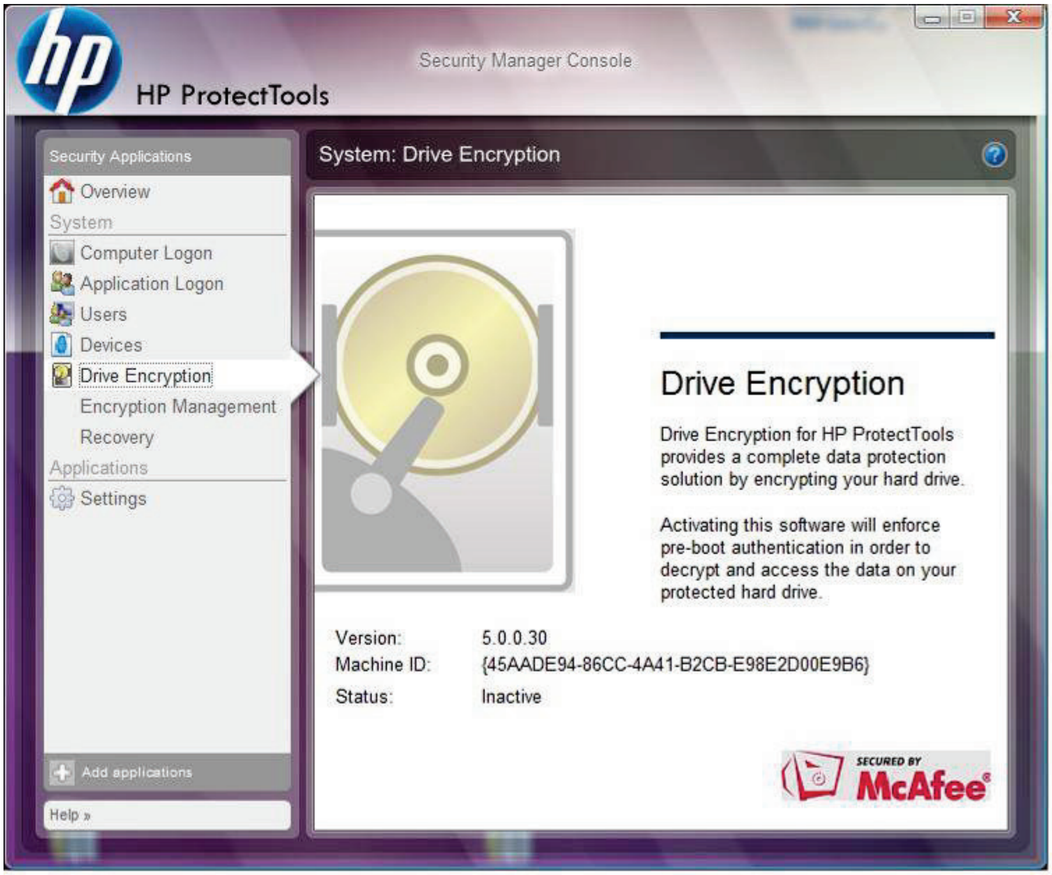
- Scenario 1: In a call center environment, call takers have full access to sensitive product and pricing information. The company however wants to protect this data and ensure that it is not removed from the premises. This can be accomplished by creating a Device Access Manager policy that prevents 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.

Device Access Manager for HP ProtectTools is a single user client version. However, an enterprise version of Device Access Manager (HP ProtectTools Device Manager) is also available and 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 encrypt or decrypt individual drives, create backup keys, and perform a recovery (Figure 7).

Figure 7. Drive Encryption for HP ProtectTools



Drive Encryption

Drive Encryption for HP ProtectTools provides a complete data protection solution by encrypting your hard drive.

Activating this software will enforce pre-boot authentication in order to decrypt and access the data on your protected hard drive.

Version: 5.0.0.30
Machine ID: {45AADE94-86CC-4A41-B2CB-E98E2D00E9B6}
Status: Inactive

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

The hard drive on a new HP Business notebook is unencrypted. The encryption process can be activated by launching HP ProtectTools Security Manager and selecting Drive Encryption for HP ProtectTools. Drive encryption is supported on SATA disk drives in the internal drive bay or docking station.

Before a hard drive can be encrypted, Drive Encryption for HP ProtectTools requires that the encryption key be backed up. This is a quick and simple 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.

The hard drive encryption process is transparent and works 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. 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.

HP 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 no software is allowed to run, and even booting from external devices such as optical drives or USB storage is disallowed. This means that software designed to bypass the operating system password protection cannot run if the computer is protected using Pre-Boot Security. Enhanced Pre-Boot Security makes it possible to setup multiple users as well as multifactor authentication policies using a password, fingerprint or HP ProtectTools Java Card.

While Pre-Boot security has been available for a number of years, it was never designed for multiuser environments. In addition, the following factors were commonly cited as the primary reasons for not using Pre-Boot security:

- Lack of Operating System integration. This meant that users wanting to use pre-boot security would have to authenticate themselves twice. Once in pre-boot and then again in the operating system
- No secure recovery options. Let's face it, people lose smartcards and forget passwords. Until now, there were two ways to recover, and neither option was very appealing. Some computers would allow password erase via access to the system board, which was not secure. On other computers, the system board had to be replaced, and this was usually not covered under warranty.

HP Enhanced Pre-Boot security addresses both these concerns with One-Step Logon and HP SpareKey. Additionally, HP Enhanced Pre-Boot security is centrally manageable with DigitalPersona Pro Workgroup and DigitalPersona Pro Enterprise, allowing IT managers to remotely recover users even if unconnected.

One-Step Logon

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. 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 user's standpoint it's the same login process as before, just during Pre-Boot instead of the operating system login.

HP SpareKey

HP SpareKey is designed allow users to 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 into HP SpareKey when they first log in 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.

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 used to encrypt the login password. The encrypted password is then stored.

Remote recovery via central management

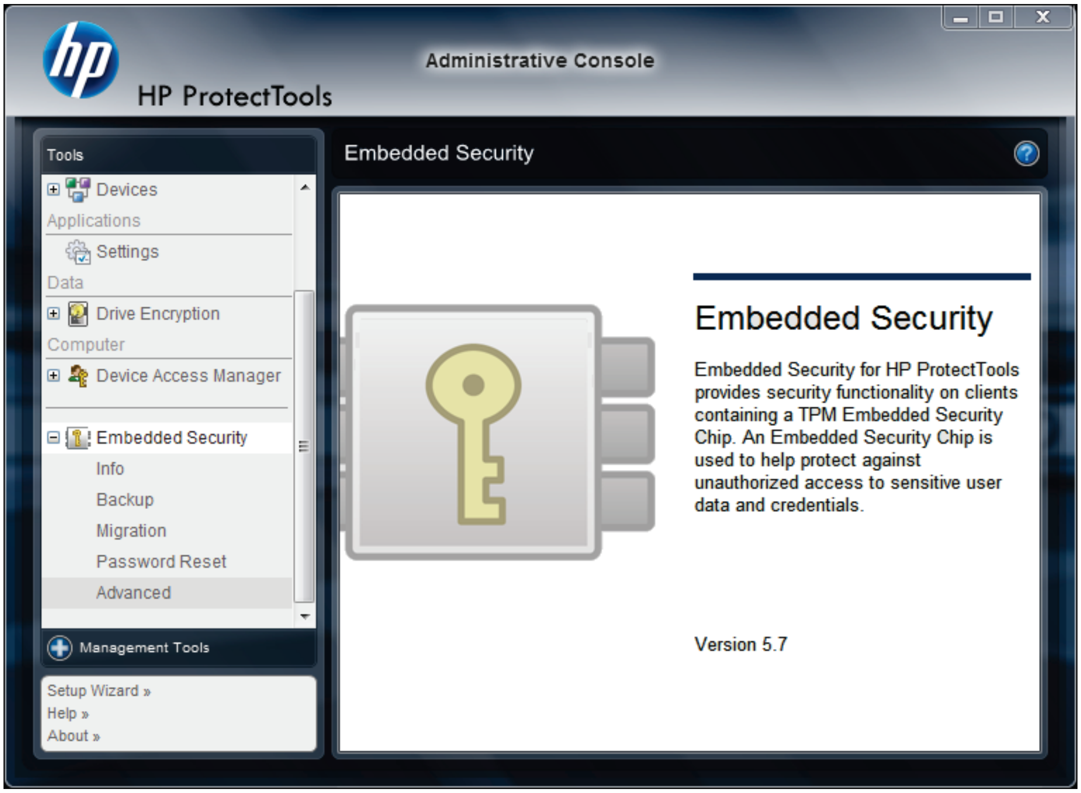
On centrally managed systems, HP Enhanced Pre-Boot security supports One Time Password (OTP) access, allowing IT support to recover remote users even if they are not connected.

Neither the answers to the three questions nor the encryption key are 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.

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools is an add-on module that allows users to configure the TPM embedded security chip (Figure 8). 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.

Figure 8. Embedded Security for HP ProtectTools



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 5.7

Embedded Security for HP ProtectTools uses the TPM embedded security chip to help protect against unauthorized access to sensitive user data and credentials. Features 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 shows Embedded Security for HP ProtectTools features and benefits.

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 by allowing access to the embedded security chip. For example, if the embedded security chip is present, Credential Manager for HP ProtectTools uses it to further secure the encryption keys that encrypt sensitive user credentials such as website passwords or network logon 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 infrastructure solutions from leaders like Microsoft, Verisign and Entrust)
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 size therefore is now only limited by the hard drive size. PSD can now also be created on removable storage devices such as USB hard drives, and USB flash drives.
Support for TPM v.1.2	Embedded Security for HP ProtectTools versions 4.0 or later support the latest TPM v1.2 as well as the previous TPM v1.1.
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.

Face Recognition for HP ProtectTools

Face Recognition for HP ProtectTools provides a new level of convenience for a high level of protection. This feature is easy to set up and use, provides multifactor authentication into Windows, and is integrated with Single Sign-on capability. Face Recognition is an innovative technology that allows you to log in to your laptop and all your favorite websites using a single sign-on. You can login simply by looking at the webcam on the PC, so there is no need to recall dozens of user names and passwords. At most sites that require a password, a window pops up over your browser and gives you the option to log in using Face Recognition.

HP recommends that a minimum of two factors be used to create a more secure environment. HP ProtectTools has additional authentication options, such as fingerprint authentication, which can be combined with Face Recognition to provide exceptional security.

Face Recognition for HP ProtectTools was developed in conjunction with Cogent, a leading biometric solutions provider.

File Sanitizer for HP ProtectTools

Files dropped into the recycle bin can easily be recovered. The recovery process is as simple as 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.

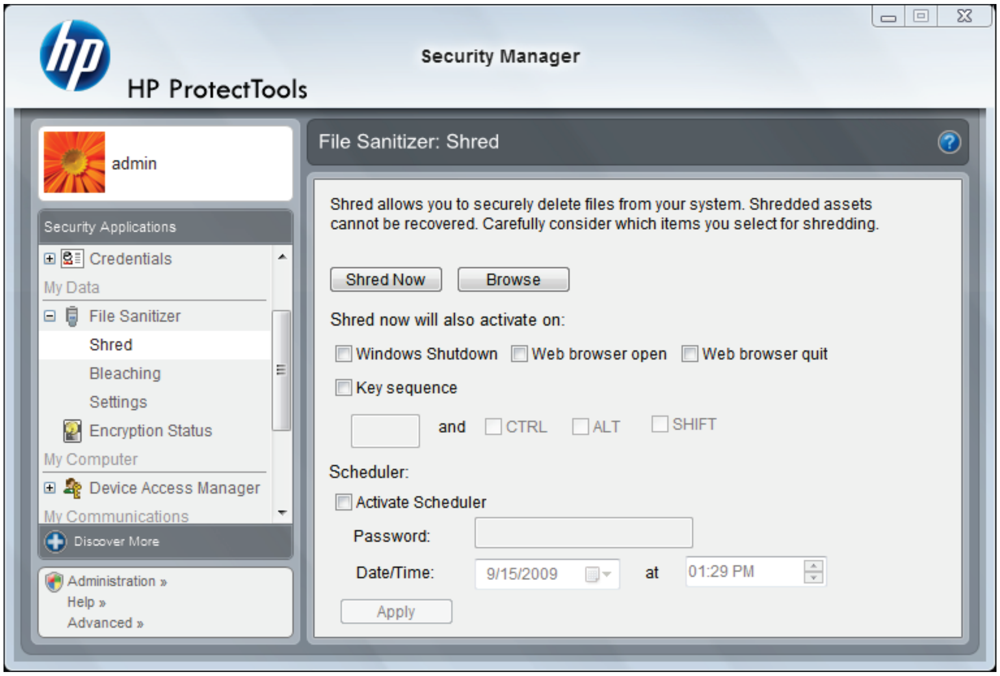
When you delete a file, it is removed from the hard drive directory. The process is quick and requires the same amount of time regardless of the size of the file. Removing the link to the file from the directory makes the space occupied by the file available to new files. The deleted file however, continues 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 because deleted information could be recovered by an unauthorized person.

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 ensure that it cannot be recovered. File sanitization is an intensive process and makes the erased data unrecoverable.

Bleaching is a process where previously used space on a hard drive is overwritten to 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. This level of control is available in File Sanitizer settings (Figure 9), 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 set up to erase the predefined files based on events such as Windows shutdown.

Figure 9. HP ProtectTools File Sanitizer setup menu



File Sanitizer: Shred

Shred allows you to securely delete files from your system. Shredded assets cannot be recovered. Carefully consider which items you select for shredding.

Shred Now | Browse

Shred now will also activate on:

□ Windows Shutdown □ Web browser open □ Web browser quit

□ Key sequence

and □ CTRL □ ALT □ SHIFT

Scheduler:

□ Activate Scheduler

Password:

Date/Time: 9/15/2009 at 01:29 PM

Apply

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

Computrace® LoJack Pro for HP ProtectTools

Computrace LoJack Pro, powered by Absolute Software (purchased separately), addresses the growing problem of computers that are lost or stolen. Activating this software enables the Computrace agent, which remains active in your computer even if the hard drive is reformatted or replaced. LoJack Pro permits remote monitoring, management, and tracking of your computer. Absolute's recovery team will assist in your computer's recovery if it is lost or stolen, depending on geographic location.

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 easy fall into the wrong hands through normal everyday communications tools such as instant messaging and email.

Privacy Manager for HP ProtectTools allows you to secure the documents and emails you create within Microsoft Office applications and enables strong privacy of your IM chats when communicating via Microsoft Live Messenger. With Privacy Manager you can be sure that only those friends, clients or colleagues you select will be able to open and read a given document, email or instant message. Additionally, your recipients can be certain that such files were created by you, and never modified by anyone else, since Privacy Manager leverages the strong, multifactor user authentication provided by HP ProtectTools. The result is that you can now take control of the information you create and communicate to ensure its privacy, security, and integrity, not just on your local computer, but wherever it may ultimately be transmitted or stored.   Identity assurance and access control of electronic transactions and communications is increasingly required by regulations in finance, law and healthcare applications.

Privacy Manager is an HP ProtectTools plug-in, and can be accessed directly from within Microsoft Office 2007 and Microsoft Live Messenger. On first use, a wizard will guide you through the process of obtaining a digital certificate. HP has partnered with Comodo, a leading issuer of digital certificates, to provide HP Privacy Manager users with a certificate, valid for twelve months, at no cost. The certificate will be issued and sent to the email address you provide, certifying you have access to that email account. After this period ends, a subscription is required to renew the certificate. For additional information, please visit https://secure.comodo.com/buydpcert/.

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, an HP ProtectTools partner. They will then also be able to obtain a certificate at no charge. You are now set up to 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 at Work

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, an HP ProtectTools partner, offers a client/server solution, DigitalPersona Pro, to better manage authentication credentials and Privacy Manager on Active Directory-based networks.

Privacy Manager – Chat

Think about when using instant messaging to communicate. All messages are transferred in the clear and go through remote servers. Files transferred using instant messaging also transfer in the clear 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.

Smart Card Security for HP ProtectTools

Smart 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. Smart 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 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.

Smart 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 shows Smart Card Security for HP ProtectTools features and benefits.

Table 5. Smart 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 Smart Card security features such as pre-boot Java Card authentication	Provides a complete Java Card security solution for pre-boot, Drive Encryption, and Windows user authentication providing enhanced protection against unauthorized of the PC

Feature	Benefit
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

Platform Support

HP ProtectTools Security Manager is supported across a range of HP business notebooks, desktops and workstations. Table 6 provides details of support for HP business notebooks and desktops.

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

	Standard Series (s)	Business Series (b)	Professional and Workstation Series (p, w)
Hardware Features			
• TPM Embedded Security Chip		●	●
• HP fingerprint sensor		●	●
• Integrated Smart Card reader (optional)		●	●
• HP Privacy Filter Support (optional)		●	●
HP ProtectTools			
HP ProtectTools Security	●	●	●
HP ProtectTools Security Setup Wizard	●	●	●
• Credential Manager for HP ProtectTools	●	●	●
• Drive Encryption for HP ProtectTools	●	●	●
• Java Card Security for HP ProtectTools	●	●	●
Privacy Manager (Chat and Sign)		●	●
File Sanitizer for HP ProtectTools		●	●
Embedded Security for HP ProtectTools		●	●
Device Access Manager for HP ProtectTools		●	●
Enhanced Pre-Boot Authentication	●	●	●
Multiuser	●	●	●
Multifactor (password, fingerprint, smart card)		●	●
HP SpareKey	●	●	●
One-Step Login	●	●	●
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				
HP ProtectTools Security Manager	A	A	A	P
Credential Manager 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

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

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
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 components are available.

- HP ProtectTools Security
- Embedded Security for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Privacy Manager for HP ProtectTools

We also currently ship Face Recognition for HP ProtectTools on select models, and LoJack Pro for HP ProtectTools. More modules are planned to be developed and released in the future.

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
- Face recognition
- USB token
- Virtual token
- Password authentication

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

A. HP clients 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 7, Microsoft Windows XP, and Microsoft Windows Vista.

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.

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

  Embedded Security for HP ProtectTools

  File Sanitizer for HP ProtectTools

  Privacy Manager for HP ProtectTools

Q. Is 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... nothing to purchase or download...it's simply there. For more information, please refer to the "HP ProtectTools – Firmware Security Features" White Paper at www.hp.com/products/security.

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/products/security.

Product Number 641527-001

Created November 2010