HP ProtectTools security software 2011

Technical white paper

Table of contents

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 for Microsoft Windows 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 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.

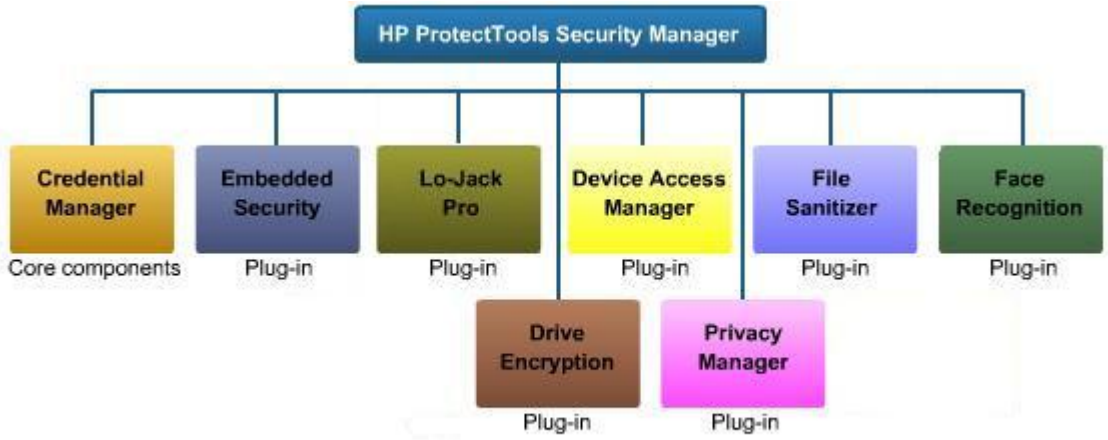
Table 1. Three pillars of security and HP ProtectTools integrated solutions for total information protection

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 protected communication via and email
HP SpareKey helps users recover lost credentials	File Sanitizer allows you to delete files from hard drive so they cannot easily be recovered	

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.

The core HP ProtectTools components are HP ProtectTools Security Manager and Credential Manager, which manages user authentication. You can select some or all of the additional plug-ins (depending on what is supported by the platform) to build a security solution that is right for your environment. Figure 1 shows the HP ProtectTools plug-ins.

Figure 1. HP ProtectTools plug-ins



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 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.

HP ProtectTools Security Manager

HP ProtectTools Security Manager provides two consoles: User and Administrative. Although somewhat similar, the two consoles provide different options. The Administrative Console makes changes to system wide parameters (Figure 2). For example, if the administrator wants to change the minimum and maximum number of enrolled fingerprints required for all users, she would use the Administrative Console. The HP ProtectTools Administrative Console is also designed to allow administrators to create and delete ProtectTools users system wide.

Figure 2. HP ProtectTools Administrative Console

The User Console is the HP ProtectTools Security Manager (Figure 3). This console makes changes to individual user profiles. For example, if a user wants to change his own password or register his fingerprints, he would use the User Console.

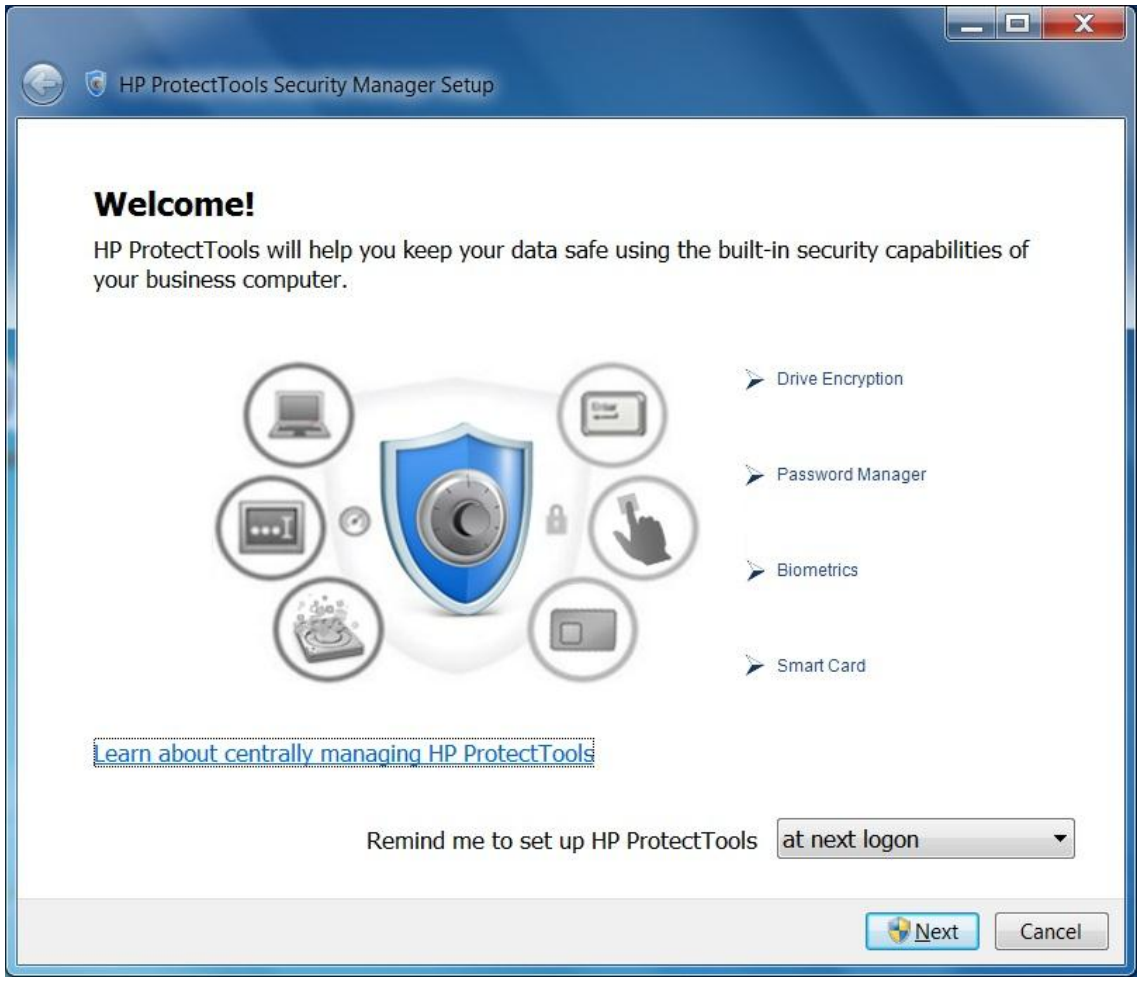
Figure 3. HP ProtectTools Security Manager home page

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 Manager Setup wizard

Setting up security should be fast and easy. Immediately after logging on to Windows on the user desktop, the administrator is guided through an easy setup of the HP ProtectTools Security Manager by a simple and straightforward Security Manager Setup wizard (Figure 4).

Figure 4. HP ProtectTools Security Setup wizard



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 Windows 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. 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 (Figure 5), 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.

Figure 5. HP ProtectTools Administrative Console Users application

Credential Manager for HP ProtectTools

Credential Manager is a core component of HP ProtectTools security software. It 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 6). It is the glue that brings the different security technologies together to create a specified behavior.

Figure 6. Credential Manager for HP ProtectTools

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 with DigitalPersona Pro central management applications
- Support for smart 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.

Feature	Benefit
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.

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 set up multiple users as well as multifactor authentication policies using a password, fingerprint or smart card. In addition to enabling pre-boot security, a BIOS admin password must be set to provide enhanced protection.

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 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 smart card, or for some reason cannot use their fingerprint to login. Users are asked to enroll in HP SpareKey when they first log in to the notebook. The enrollment process is easy and requires the user to answer any three questions from a predetermined list of ten and up to three custom questions. 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.

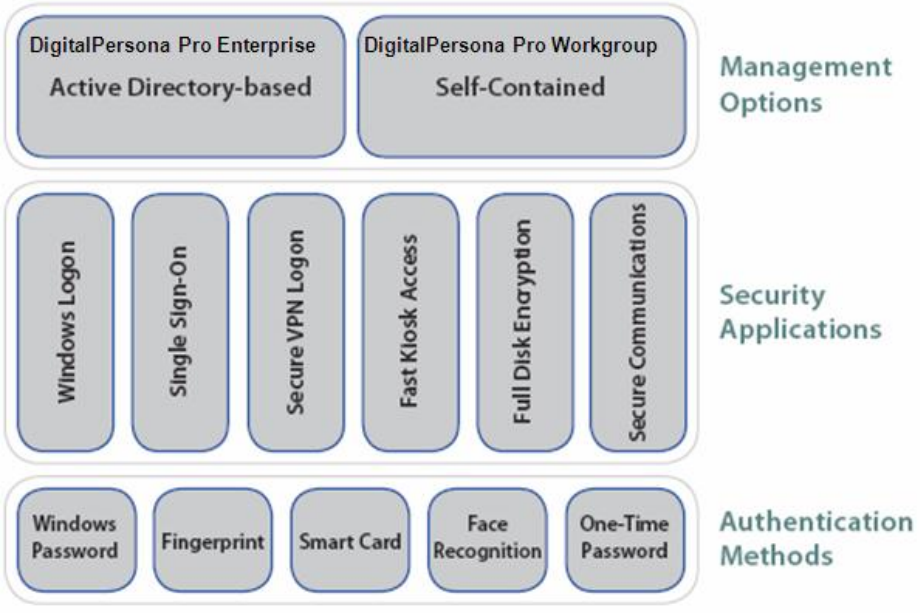
On centrally managed systems, HP Enhanced Pre-Boot Security supports One Time Password (OTP) access, allowing IT support to recover remote users even if they are not connected.

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.

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 7 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 7. 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

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 back up 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 8 shows the HP ProtectTools Security Manager Backup and Restore menu.

Figure 8. HP ProtectTools Security Manager Backup and Restore menu

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:

- Face Recognition for HP ProtectTools
- Device Access Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- File Sanitizer for HP ProtectTools[1]
- Computrace® LoJack Pro for HP ProtectTools[2]
- 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.

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 notebook pc 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 recommends protecting face scenes with a PIN or with Bluetooth phone pairing, which can be combined with Face Recognition to provide exceptional security.

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

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 several configuration options:

- Simple Configuration
- Device Class Configuration
- Just-in-time authentication (JITA) Configuration

---

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

[2] Tracking and recovery is supported by an embedded BIOS agent on HP business notebooks, which is shipped turned off, and must be activated by the purchase of a subscription for terms ranging from one to five years via LoJack Pro. Service is limited, check with Absolute Software for availability outside the U.S., certain conditions apply. For full details visit:http://www.absolute.com/products/lojackforlaptops.

- Advanced Settings

Device Administrators Group

When Device Access Manager is installed, a Device Administrators group is created. This group is used to exclude trusted users from the restrictions imposed by a Device Access Manager policy. Trusted users usually include system administrators.

Simple Configuration

Simple Configuration enables or denies access to certain major categories of devices to users that are not part of the Device Administrators group. The Simple Configuration option is a collection of common options that can be configure with a single selection (Figure 9).

Figure 9. Device Access Manager for HP ProtectTools Administrative Console

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, 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, 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 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.

JITA Configuration

JITA Configuration allows the administrator to view and modify lists of users and groups that are allowed to access devices using just-in-time authentication. JITA-enabled users will be able to access some devices for which policies created in the Device Class Configuration or Simple Configuration view have been restricted.

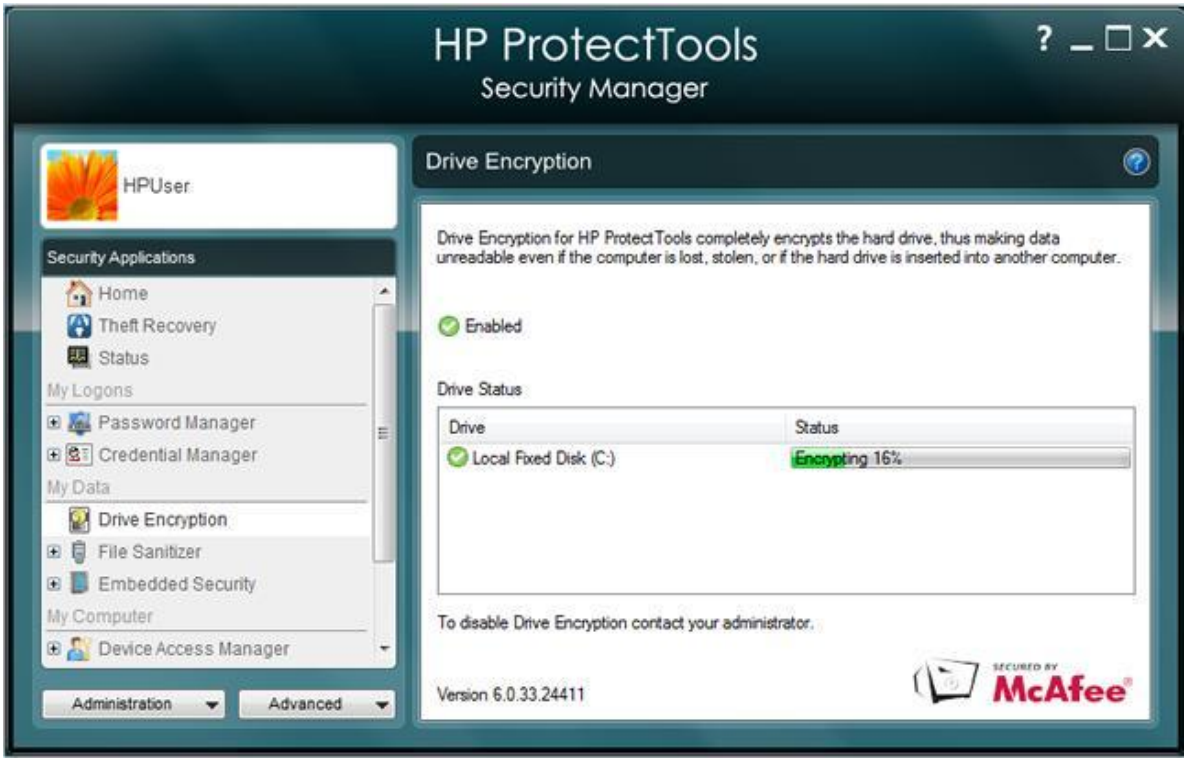
The JITA period can be authorized for a set number of minutes or 0 minutes. A JITA period of 0 minutes will not expire. Users will have access to the device from the time they authenticate until the time they log off the system. The JITA period can also be extended, if configured to do so. In this scenario, 1 minute before the JITA period is about to expire, users can click the prompt to extend their access without having to re-authenticate. Whether the user is given a limited or unlimited JITA period, as soon as the user logs off the system or another user logs in, the JITA period expires. The next time the user logs in and attempts to access a JITA-enabled device, a prompt to enter credentials is displayed.

JITA is available for DVD/CD-ROM drives and removable media.

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 10).

Figure 10. Drive Encryption for HP ProtectTools



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. Drive encryption is also supported on external SATA and eSATA drives. Self-encrypting drives (SEDs) meeting Trusted Computing Group's (TCG) OPAL specification for self-encrypting drive management can be encrypted using either software encryption with HP Drive Encryption, or hardware encryption using the SED self-encryption function. Only one encryption method can be selected for the drive.

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.

Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools is an add-on module that allows users to configure the Trusted Platform Module (TPM) embedded security chip (Figure 11). This add-on module is intended for HP business notebooks, desktops and workstations configured with a TPM embedded security chip designed to the Trusted Computing Group (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 11. 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 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, backing up and restoring the key hierarchy, and 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. 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

Feature	Benefit
	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 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.

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 12), 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 12. HP ProtectTools File Sanitizer setup menu

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 directly related 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

Privacy Manager for HP ProtectTools allows you to secure the documents and emails you create within Microsoft Office applications. 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 or email. 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 to comply with regulations in finance, law and healthcare applications.

Privacy Manager is an HP ProtectTools plug-in, and can be accessed directly from within Microsoft Office 2010. 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 six months, at no cost. The certificate identifies the originator of the communication to the recipient. Non-Comodo certificates are also supported. You can also invite your contacts to acquire their own Privacy Manager certificates to become Trusted Contacts. Trusted Contacts are listed in Privacy Manager.

Privacy Manager is designed to integrate seamlessly into Microsoft Office applications. Content created in Microsoft Office can be digitally signed and encrypted to ensure that only Trusted Contacts can view the content. It also ensures 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.

HP DigitalPass One Time Password

HP DigitalPass One Time Password (OTP) technology helps prevent access to a user's computer by providing a second level of authentication that helps validate online transactions. This elevated level of security and protection for online transactions is accomplished by validating the user's online identity with participating websites.

HP DigitalPass OTP is an HP ProtectTools plug-in that works with VeriSign Identity Protection (VIP) service to create secure connection to VIP-enabled websites. DigitalPass OTP allows you to enable VeriSign VIP and create VIP access tokens for supported sites. Once you have registered and created the access token, HP DigitalPass will log you into the site automatically.

HP DigitalPass requires the following hardware/firmware components:

- Intel Core i3, i5, or i7 processor and chipset
- Intel Management Engine Interface (MEI) driver version 7.x.x.x.x
- Host Embedded Controller Interface (HECI)
- BIOS containing management engine firmware ME FW 7.1.x.x

Or

- HP fingerprint sensor
- Fingerprint sensor driver version 4.3.117.0

HP DigitalPass uses a fingerprint or a hardware generated passcode that is used only once for a short period of time and is supplied invisibly to participating websites. This passcode provides a second factor of authentication to the traditional user name and password. It provides something the user knows (user ID and password) plus something the user has (HP DigitalPass). The passcode is protected in the PC hardware and cannot be accessed from the hard drive or the BIOS.

Platform Support

HP ProtectTools Security Manager is supported across a range of HP business notebooks, desktops, and workstations. Table 5 provides details of support for HP business notebooks.

Table 5. 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 (optional)		●	●
• 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	●	●	●
Smart 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		●	●

Frequently Asked Questions

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
- 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. 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. Smart cards are not supported in BIOS pre-boot; however, FVE supports specific ActivIdentity smart cards. 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 system 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. The email program may encrypt the data across the internet if that option is selected, but the TPM is no longer protecting the data. This is true of any data on your system encrypted by MSFT EFS (Microsoft's Encrypting File System where TPM can be used to protect the file/folder encryption keys) and also for files encrypted within PSD (ProtectTools Personal Secure Drive). It is possible for a file to remain encrypted no matter where it resides, but typically in those types of applications the file name is changed. For instance, *hello.doc* becomes *hello.doc.enc* to show that the 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 I 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 in a single, easy to use security solution. As an HP ProtectTools core component, 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. 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 administrator 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 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 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 smart card that comes with a PKCS#11 component.

Q. What is the process for uninstalling HP ProtectTools?

A. HP ProtectTools plug-ins and the Security Manager can be removed using the Windows Uninstall Program utility in the Windows Control Panel. The process is the same as uninstalling any Windows application. Select the HP ProtectTools application to be removed and then click the Uninstall button.

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 HP Business Notebook BIOS, 2006 and later.

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.

641527-001 Rev. B, Created May 2011