

HP ProtectTools Security Manager - 2007



Introduction	2
The security dilemma	2
HP ProtectTools Security Manager	3
Security Software Modules for HP ProtectTools	4
Drive Encryption for HP ProtectTools	5
Encrypting the hard drive	5
Hard Drive Encryption Process	6
Full Enterprise Capability	6
Embedded Security for HP ProtectTools	7
Credential Manager for HP ProtectTools	9
BIOS Configuration for HP ProtectTools	10
Java Card Security for HP ProtectTools	13
Device Access Manager for HP ProtectTools	14
Simple Configuration	15
Advanced Configuration	15
Platform Support	16
Frequently Asked Questions	19
For more information	22

Introduction

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

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

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

The security dilemma

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

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

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

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

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

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

- Notebook and desktop computers can be configured to utilize smart card readers or biometric sensors, which are standard on many HP business notebook models.
- The Trusted Platform Module (TPM), or embedded security chip designed to the Trusted Computing Group (TCG) standard, is available on a range of HP products.

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

- Pre-OS authentication – authenticates a user before allowing the operating system to boot
- Device configuration lock down – allows port control in BIOS that can be protected against modification by users without administrative access
- Remote management capabilities – allows administrators to remotely set BIOS security policies.

HP ProtectTools Security Manager

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



Figure 1 - HP ProtectTools Security Manager Console

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

Features of HP ProtectTools Security Manager include support for broad multifactor user authentication where a number of different security technologies, such as smart cards, biometric fingerprint sensors and embedded security chips, can be used to authenticate users. This solution provides users with a more secure and convenient alternative to passwords when logging into a PC using the Microsoft® Windows® operating system. HP ProtectTools Security Manager also includes single sign-on capability that conveniently stores and protects many of the credentials users need daily to access websites, network resources and applications.

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

- Provide better protection against unauthorized access to the PC, while making access to the PC and network resources simple and convenient for authorized users.
- Deliver a higher degree of data protection while the PC is turned off
- Enable better protection against unauthorized access even before the operating system is loaded by leveraging underlying security technologies such as the TPM embedded security chip.

Security Software Modules for HP ProtectTools

This section provides more details on specific add-on security software modules available for use with the HP ProtectTools Security Manager. The modular architecture of the HP ProtectTools Security Manager enables add-on modules to be selectively installed by the end-user or IT administrator, providing a high degree of flexibility to customize HP ProtectTools depending on security needs and the underlying hardware configuration. Each add-on module is a self contained security application providing targeted security functionality. Integrated into the HP ProtectTools Security Manager, these modules form a holistic security solution. They are specifically designed to work with and complement each other. With the addition of Drive Encryption for HP ProtectTools, the number of modules currently available for HP ProtectTools has grown to seven, and includes:

- Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools
- Credential Manager for HP ProtectTools
- BIOS Configuration Manager for HP ProtectTools
- Java Card Security for HP ProtectTools
- Device Access 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.

Drive Encryption for HP ProtectTools

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

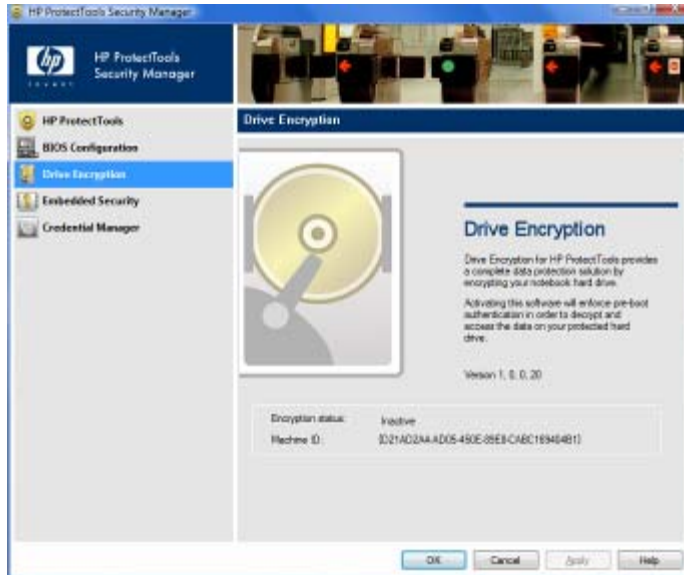


Figure 2: Drive Encryption for HP ProtectTools

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

Encrypting the hard drive

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

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

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

Hard Drive Encryption Process

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

Full Enterprise Capability

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

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

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

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

Embedded Security for HP ProtectTools

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



Figure 2 - 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 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 1 – 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 infrastructures 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) in version 4.0	Personal Secure Drive (PSD) is an encrypted mountable volume. In Embedded Security for HP ProtectTools version 4.0, 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 version 4.0 or later supports 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.

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. It is the glue that brings the different security technologies together to create a specified behavior.

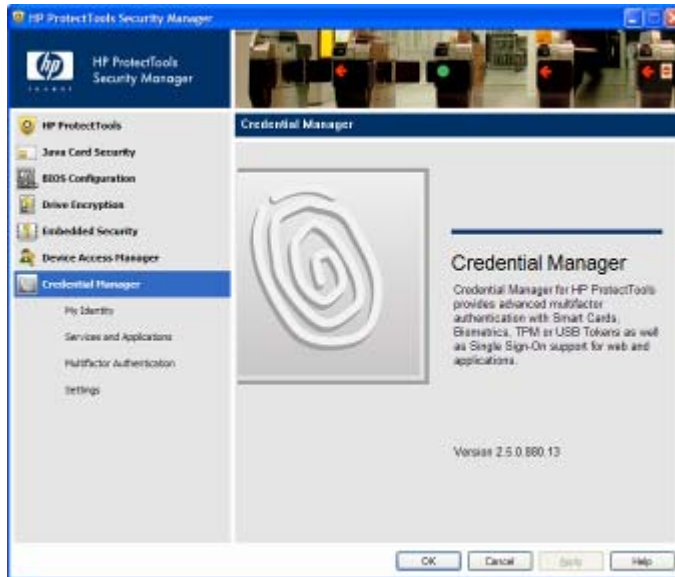


Figure 3 – Credential Manager for HP ProtectTools

Through the 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 a single sign-on capability that automatically remembers credentials for websites, applications, and protected network resources. Credential Manager effectively is 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
- 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 - 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	<p>Users no longer need to remember multiple passwords for protected websites, applications and network resources.</p> <p>Single sign-on works with multifactor authentication capabilities to add additional protection requiring users to re-authenticate when accessing particularly sensitive data.</p> <p>Registering new websites, applications or network logon dialogues is fully automated making it easy for users to begin taking advantage of the added convenience and security of the single sign-on feature.</p>

BIOS Configuration for HP ProtectTools

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



Figure 4 – BIOS configuration for HP ProtectTools

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

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

Using BIOS Configuration for HP ProtectTools, authorized users can:

- Manage power-on user and administrator passwords
- Configure pre-boot authentication features such as smart cards, Power-on Passwords, and TPM-enhanced DriveLock
- Enable/disable hardware features such as CD-ROM boot.
- Configure boot options including disabling the ability to boot to drives other than the primary hard drive.

Table 3 - BIOS Configuration for HP ProtectTools Features and Benefits

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

Enabling access to BIOS security configuration from within the HP ProtectTools Security Manager creates an integrated security solution and enables authorized users to control every aspect of security management from a single application with a common user interface. The following table describes the key BIOS security features¹ that become accessible from the HP ProtectTools Security Manager using the BIOS Configuration Module.

¹ Pre-boot authentication features are available on select platforms. Refer to platform specific specifications for more details.

Table 4 - Key BIOS security features made accessible by the BIOS Configuration Module

Feature	Description	Benefit
TPM embedded security chip pre-boot authentication	Utilizes the embedded security chip for user authentication. Users need to input the basic user key pass phrase	Helps protect against unauthorized access to the PC by preventing access to the computer by booting from a device other than the primary hard drive. Provides security benefits similar to a power-on password; however, by allowing users to use their embedded security chip pass phrase, users are not required to remember an additional password.
TPM-enhanced DriveLock	Requires a user to authenticate to the embedded security chip before a DriveLock protected hard drive can be accessed. A separate DriveLock password is not required.	TPM-enhanced DriveLock helps protect a hard drive from unauthorized access even if it is physically removed from a system. Allows very strong, random DriveLock passwords to be automatically set in a way that is completely transparent to users (does not require the user to remember another password) Ties a hard drive to a specific system with a specific embedded security chip, preventing other systems from accessing the hard drive if it is physically removed from the original system.
Smart card pre-boot authentication	Requires a user to insert a smart card and, optionally, enter a PIN to authenticate prior to an operating system being allowed to load	Protects a system from unauthorized access by requiring users to insert their smart card to boot the system. The same smart card used to authenticate a user in the pre-boot environment can also be used with HP ProtectTools to login to Microsoft Windows XP or Windows 2000. Smart card pre-boot authentication requires the HP ProtectTools Smart Card, or the new HP ProtectTools Java Card.

BIOS Configuration for HP ProtectTools is supported on most HP business notebooks, desktops and workstations. See Table 6 of this white paper for more information on support by platform. Enhanced authentication features are supported on select business PCs including business notebooks with integrated TPM chips as well as the dc7600 and dc7700 desktop PC series.

All HP Notebooks also have a built in feature called Disk Sanitizer. Disk Sanitizer enables secure disposal or recycling of notebooks by erasing the hard drive using a method documented in the Dept. of Defense DOD 5220.22-M specification, Chapter 8 of the National Industry Security Program Operating Manual. Since the Disk Sanitizer erases the entire hard drive, it is not accessible from BIOS Configuration for HP ProtectTools, and instead has to be accessed directly from the BIOS. For more information on Disk Sanitizer, please refer to the whitepaper titled "HP ProtectTools: Firmware security features in HP business notebooks", available for download at www.hp.com/products/security.

Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools allows the HP ProtectTools Java Card to be utilized for user authentication in the pre-boot as well as the Microsoft Windows environment. Java Card Security enables access to Java Card configuration and security features on systems equipped with a smart card reader. Smart card readers can either be integrated into the system, or can be added using the PC card slot on notebooks or 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.



Figure 5 – Java Card Security for HP ProtectTools

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

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

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

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

Device Access Manager for HP ProtectTools

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

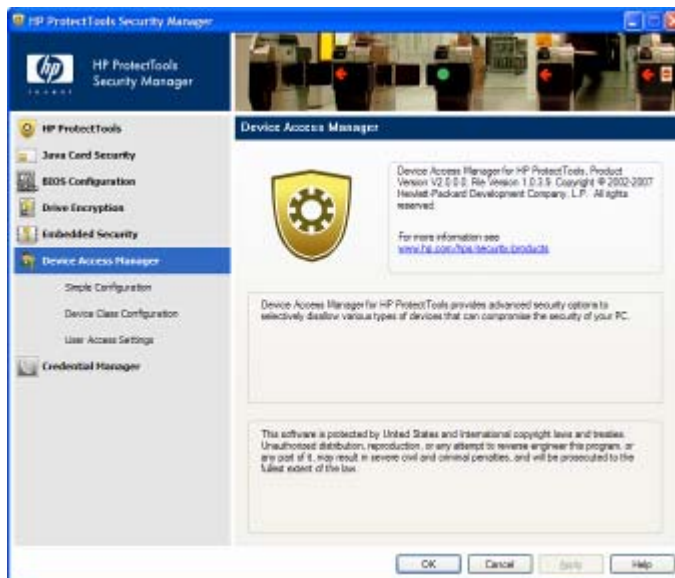


Figure 7 – Device Access Manager for HP ProtectTools

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

Simple Configuration

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

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

Advanced Configuration

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

By using Advanced 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, by default allows all devices for all users. 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 Advanced Configuration, Device Access Manager presents a device tree view derived from the Windows Device Manager. Individual devices or an entire class of devices from the device tree can be selected. Access to the selected device can then be restricted by applying the policy to selected users or class of users.

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

- Scenario 1: In a call center environment, call takers have full access to sensitive product and pricing information. The company however wants to protect this data and ensure that it is not removed from the premises. This can be accomplished by creating a Device Access Manager policy that prevents removable storage devices such as USB keys and writeable optical drives from being used by unauthorized users.
- Scenario 2: A company is making sensitive financial information available to an auditor and wants to protect this information from being copied or removed from the notebook. Device Access Manager can allow a policy where this user is denied access to any removable storage devices or printers.

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

Platform Support

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

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

Business Notebooks													
	2510p	2710p	6510b	6515b	6710s	6710b	6715s	6715b	6910p	8510p	8510w	8710b	8710p
Hardware Support													
TPM Embedded Security Chip v.1.2	S	S	S	S	N	S	N	S	S	S	S	S	S
Integrated Fingerprint Sensor	S	S	S	S	N	S	N	S	O	S	S	S	S
Integrated Smartcard Reader	O	O	O	O	N	O	N	O	S	O	O	O	O
S = Standard / O = Optional / N = Not Available													
HP ProtectTools Support													
HP ProtectTools Security Manager	P	P	P	P	N	P	N	P	P	P	P	P	P
Credential Manager for HP ProtectTools	P	P	P	P	N	P	N	P	P	P	P	P	P
Drive Encryption for HP ProtectTools	P	P	P	P	N	P	N	P	P	P	P	P	P
BIOS Configuration for HP ProtectTools	P	P	P	P	N	P	N	P	P	P	P	P	P
Embedded Security for HP ProtectTools	P	P	P	P	N	P	N	P	P	P	P	P	P
Java Card Security for HP ProtectTools	W	W	W	W	N	W	N	W	W	W	W	W	W
Device Access Manager for HP ProtectTools	W	W	W	W	N	W	N	W	W	W	W	W	W
HP Disk Sanitizer	S	S	S	S	S	S	S	S	S	S	S	S	S
Computrace / LoJack for Laptops	S	S	S	S	S	S	S	S	S	S	S	S	S
P = Pre-installed / W = Web Release / S = Supported / N = Not Supported													

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
BIOS Configuration for HP ProtectTools	A	A	A	P
Embedded Security for HP ProtectTools	A	A	A	P
Java Card Security for HP ProtectTools	A	A	A	W
Computrace / Lojack for Laptops – for Desktops	S	S	S	S

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
BIOS Configuration for HP ProtectTools	A	A	A	P,W

Workstation Platforms	xw4400	xw6400	xw8400	xw9400
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 six modules are available. More modules will be developed and released in the future.

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

Q. What authentication technologies are supported by HP ProtectTools?

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

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

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

A. HP 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 XP and Microsoft Windows 2000. Microsoft Windows Vista will be supported when available.

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. Where can I get smartcards for HP ProtectTools?

A. The HP ProtectTools Java cards are available for purchase on hp.com.
http://h30143.www3.hp.com/configure2.cfm?sid=18562#m_84

Q. What is the minimum order quantity for HP ProtectTools Java Cards?

A. HP ProtectTools Java smart cards are sold in packages of 10.

Q. If the HP ProtectTools Java Card is locked due to the incorrect PIN retries exceeding maximum, (5 incorrect entries). Is there a way to reactivate it?

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

Q. What is the process for uninstalling HP ProtectTools?

A. The process is the same as uninstalling any windows application:

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

- Remove the following ProtectTools components if they exist
 - Credential Manager for HP ProtectTools
 - Java Card Security for HP ProtectTools
 - Drive Encryption for HP ProtectTools
 - Smartcard security for HP ProtectTools
 - Embedded Security for HP ProtectTools
 - BIOS Security for HP ProtectTools
 - HP ProtectTools Security Manager

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... There is a whitepaper that will give you details on the feature...

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

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

For more information

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

www.hp.com

www.hp.com/products/security

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

5982-9847EN, Rev 4, 04/2007

