

# HP ProtectTools Security Manager - v2.0



Introduction .....	3
The security dilemma .....	3
HP ProtectTools Security Manager .....	4
Security Software Modules for HP ProtectTools .....	5
Device Access Manager for HP ProtectTools .....	5
Simple configuration .....	6
Advanced Configuration .....	6
Embedded Security for HP ProtectTools .....	6
BIOS Configuration for HP ProtectTools .....	8
Java Card Security for HP ProtectTools .....	10
Smart Card Security for HP ProtectTools .....	11
Credential Manager for HP ProtectTools .....	12
Platform Support .....	14
Frequently Asked Questions .....	15
Additional Resources .....	17

# Introduction

As computers get increasingly mobile and better connected, threats to data security are increasing in magnitude as well as complexity. Correspondingly business customers, for whom data security can have a direct impact on the health of their business, are becoming increasingly concerned about this problem. Gartner, in the IT focused polled titled "top ten business trends, 2005" ranked security and privacy as a top five concern.

HP saw the need for a better security solution very early, and started devoting resources to solving this problem. Knowing that security needed to be addressed holistically, HP required the solution to bring many technology areas together in a way that helps ensure not only protection for client devices, but also helps ensure that client devices themselves do not become points of vulnerability that could be used to threaten the entire IT infrastructure.

As a result of this proactive effort, HP has developed a solution, the HP ProtectTools Security Manager, which meets the above requirements, and builds on them by being extensible, and easy to use.

## The security dilemma

Businesses trying to implement client device security face a dizzying number of choices that may not always work well together. In addition, security solutions can be difficult to deploy and use. If a technology is difficult to use, most users will avoid using it, and this further complicates the task of making client devices secure.

Client device security options feature a number of capabilities based on a variety of technologies:

- Notebook and desktop computers can be configured with Smart Card readers or Biometric sensors.
- 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
- RFID (Radio Frequency Identification) is expected to become more important as the technology matures and becomes more suitable for enterprise deployment

In addition, many client devices include security features that exist within the device BIOS. These include features such as:

- Pre-OS authentication – ability to authenticate a user before allowing the operating system to boot
- Device configuration lock down
- Remote management capabilities

While these security features increasingly rely on established industry standards, and therefore better integrate with other elements of IT security, there are still challenges that are keeping these features from being widely deployed and used. These challenges include:

- Usability: technologies and features that are difficult to use
- Manageability: technologies and features that are difficult to manage, particularly on a large scale
- Awareness: IT managers and users are not aware of a feature, or do not understand its purpose
- Interoperability: features or services that span multiple technologies
- Extensibility: solutions that adapt as security needs grow and newer technologies and features become available

The HP ProtectTools Security Manager is a security platform that addresses these challenges by using add-on software modules, which provide important client security features. New features can easily be added by installing new modules. This architecture gives users an easy to use all in one security solution.

# HP ProtectTools Security Manager

At the heart of the security strategy for business notebooks, desktops and workstations is the HP ProtectTools Security Manager – this single client console application unifies security capabilities of HP client PCs under a common architecture and single user interface. Today, a range of features is being delivered that build on underlying hardware security building blocks such as embedded security chips designed to the Trusted Computing Group (TCG) standard and Smart Card technology. Collectively these features are addressing business customer needs for better protection against unauthorized PC access, as well as stronger protection for sensitive data stored locally or accessed over a network.

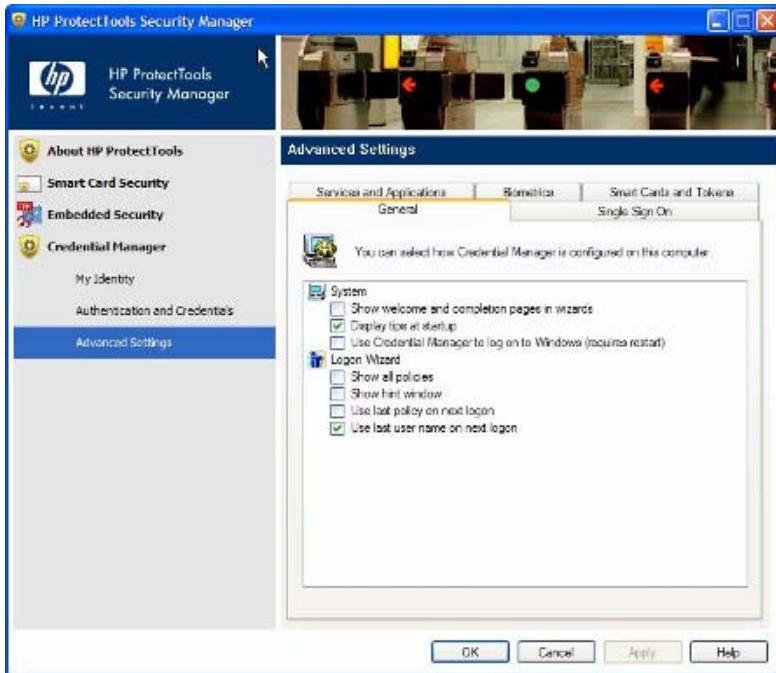


Figure 1 - HP ProtectTools Security Manager Console

HP ProtectTools Security Manager embodies an extensible framework that is designed to allow security software functionality to be added through add-on modules. This approach supports longer term client device security strategy by enabling HP to introduce new functionality over time, but in a highly integrated manner. Ultimately, customers benefit from security features that are easier to use, manage, and provide enhanced value through features that play off of multiple security hardware attributes of the client device.

HP ProtectTools Security Manager is only the first step. The application is a security platform that gets its functionality via plug in software modules. A number of software modules are also being introduced 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.

Features include support for broad multifactor user authentication where a number of different security technologies, such as Smart Cards, biometric fingerprint readers or embedded security chips, can be used to authenticate users. Users are provided with more secure as well as convenient alternatives to passwords when logging into a Microsoft Windows PC. HP is also extending the HP ProtectTools Security Manager feature set to include a client-centric single sign-on capability that conveniently stores and protects many of the credentials users need daily to access websites, network resources and applications.

Additional modules are also available that deliver a higher degree of client device security from the moment power is turned on. By leveraging underlying security technologies such as the TPM embedded security module, HP is enabling better protection against unauthorized access even prior to allowing the operating system to load.

# 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 platform, these modules form a holistic security solution. They are designed to work with and compliment the features provided by other modules. The number of modules currently available for HP ProtectTools has grown to five. Going forward, as new needs are identified, HP expects to continue to expand its client security offerings with additional modules for the HP ProtectTools Security Manager.

## Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools is a new module that speaks to HP's commitment to security and HP's ability to listen to customers and to solve their problems. A common assumption with today's client usage model is that if a User is authorized to log on to a client and access sensitive information, that that information can be viewed, copied or printed. In reality, this is not always that case. Companies may want 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.

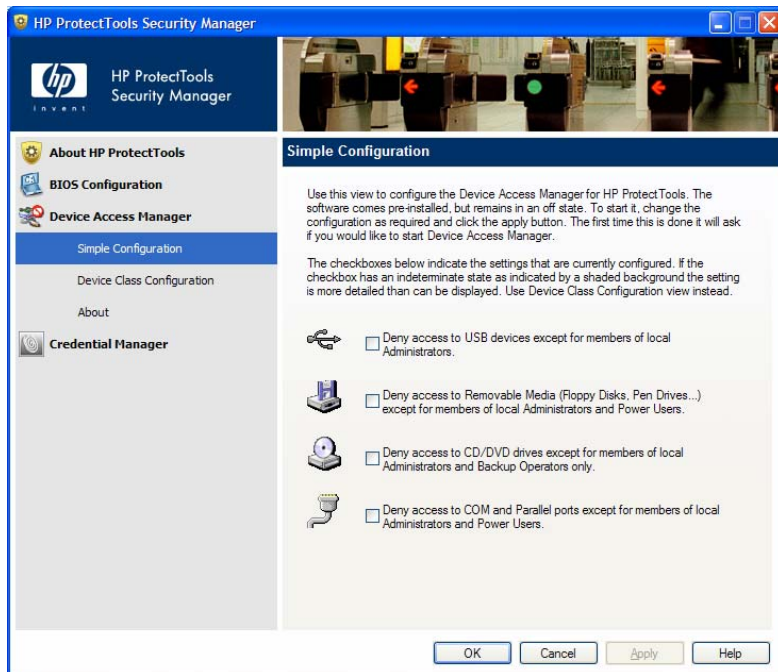


Figure 2 – Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools has two configuration options:

- Simple Configuration
- Advanced Configuration

### Simple configuration

Is a collection of common options that can be configured with a single selection. These options include:

- Limit access to All USB devices to administrators only

- Limit access to removable media to administrators and power users only
- Limit access to optical drives to administrators and backup operators
- Limit access to Serial and Parallel ports to administrators and power users only

### 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. Device Access Manager enables new client usage models

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 works on a white list basis. By default, all users have access to all devices. Advanced Configuration presents the user with a device tree view derived from the Windows Device Manager. Individual Devices from the device tree or an entire class of devices can be selected. Access to the selected device can then be controlled by adding users or class of users for whom access is denied.

This level of configurability enables new client usage models, such as:

- 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 configured for unauthorized users.
- In another scenario, a company is making sensitive financial information available on a notebook PC to an Auditor, and wants to protect this information from being copied and remove from the laptop. Device Access Manager can allow a policy where this user is denied access to any removable storage devices.

Device Access Manager for HP ProtectTools is a single user client version. However an enterprise version of Device Access Manager (HP ProtectTools Device Manager) is also available 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/](http://www.hp.com/hps/security/products/)

### Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools is an add-on module for the HP ProtectTools security manager that allows users to configure how they would like to use the TPM embedded security chip. This add-on module is intended for client devices 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.

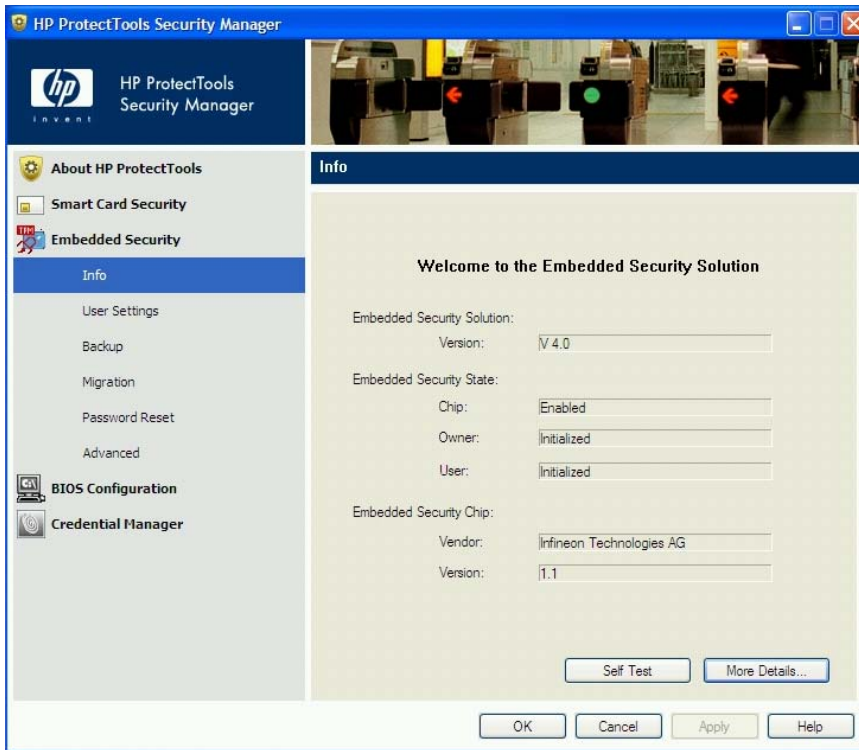


Figure 3 - Embedded Security for HP ProtectTools

Embedded Security for HP ProtectTools provides important client security functionality where an embedded security chip is used to help protect against unauthorized access to sensitive user data or 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 managing user pass phrases
- Feature configuration including setting up enhanced Microsoft EFS and Personal Secure Drive for helping to protect user data management 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 option. *See Table 7: HP ProtectTools solution set support by HP product* 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 standard 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 version 4.0, PSD has been enhanced with a significantly larger size limit. The PSD can now occupy the entire hard disk minus 5GB for system files. PSD size therefore is now only limited by the hard disk size.
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, refer to [www.hp.com/go/security](http://www.hp.com/go/security).

## 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. HP has invested heavily in developing BIOS security features, and therefore the BIOS on an HP client plays an important role in enhancing the overall security of the client. Non technical users however are not comfortable modifying BIOS settings. BIOS configuration for HP ProtectTools is designed to make the BIOS features easily accessible to all users from the familiar Microsoft Windows environment.

In keeping with the ProtectTools philosophy, BIOS configuration by enhancing ease of use, makes security features more accessible to every user.

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.

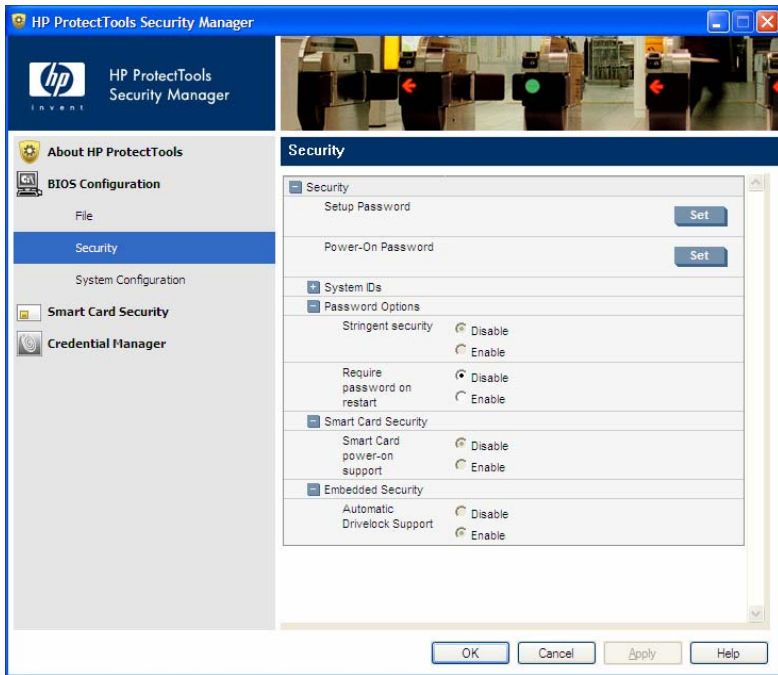


Figure 4 – BIOS configuration for HP ProtectTools

With 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.
- Configuring boot options including disabling the ability to boot to drives other than the primary hard drive

Table 2 – 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.
Enhanced security feature set that take 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>Embedded security chip 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 Smart 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 features<sup>1</sup> that become accessible from the HP ProtectTools Security Manager using the BIOS Configuration Module.

Table 3 – Key BIOS security features made accessible by the BIOS Configuration Module

Feature	Description	Benefit
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 the user 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.	DriveLock helps protect a hard drive from unauthorized access even if 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 a user 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 into Microsoft Windows XP or Windows 2000.  Smart Card pre boot authentication requires the HP ProtectTools smartcard, 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 - HP ProtectTools solution set support by HP product* for more information on support by platform. Enhanced authentication features are supported on select business PCs including business notebooks with integrated TPMs as well as the dc7100 desktop PC series.

## Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools allows the HP ProtectTools Java Card to be used 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, or can be added using the PC card slot. For authentication, users require the HP ProtectTools Java Card which can hold their passwords and PIN, and a supported reader, such as an integrated smart card reader, or the HP PC Card Smart Card Reader.

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

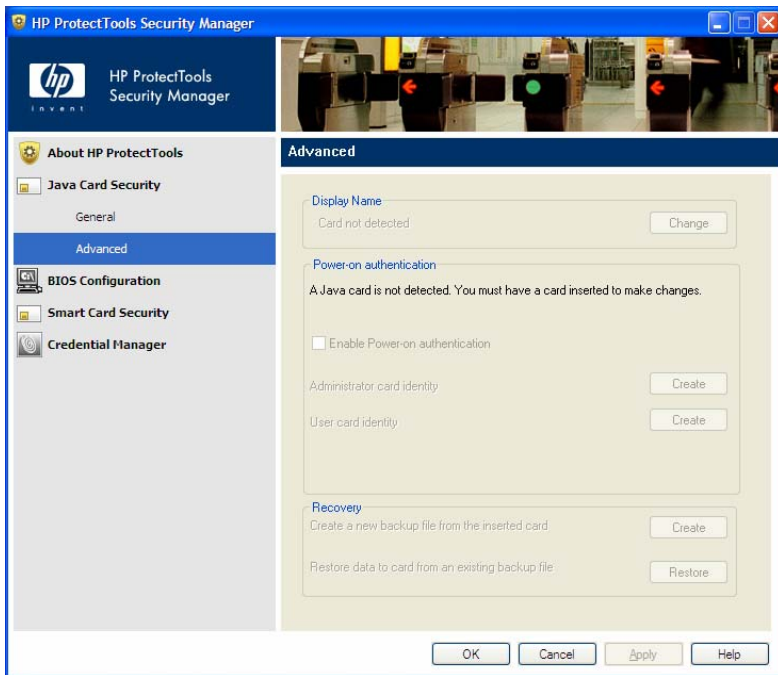


Figure 5 – Java Card Security for HP ProtectTools

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

- Separation of the Administrator and User roles
- 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
- 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 4 – Java Card Security for HP ProtectTools Features and Benefits

Feature	Benefit
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 their 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.

## Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools enables access to Smart Card configuration and security features on systems equipped with a Smart Card reader. Smart Card readers can either be integrated, or can be added using the PC card slot. For authentication, users require a Smart Card

such as the HP ProtectTools Smart Card<sup>2</sup> which can hold their passwords and PIN, and a supported reader, such as the HP PC Card Smart Card Reader.

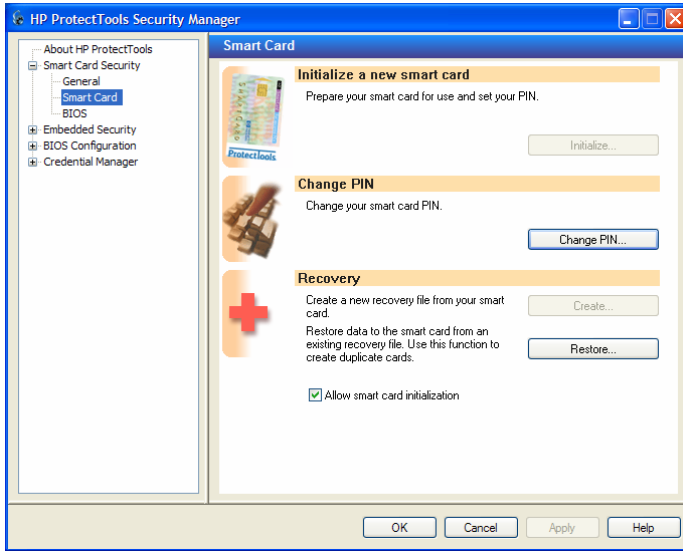


Figure 6 - Smart Card Security for HP ProtectTools

Smart Card Security for HP ProtectTools provides Smart Card management features such as:

- Initialize and configure an HP ProtectTools Smart Card, which enables a Smart Card to be used for user authentication
- Interface with the BIOS to enable/disable Smart Card pre-boot authentication
- Configure separate Smart Cards for administrators and users
- Set and change the Smart Card PIN
- Backup and restore credentials stored on the Smart Card

Smart Card support was previously provided as a standalone application called HP ProtectTools Smart Card Security Manager. All subsequent Smart Card support will be delivered through the Smart Card Security for HP ProtectTools module and will require the HP ProtectTools Security Manager application. The new module brings a previously separate security technology into the new integrated security solution, giving users a single application from which to manage all security features.

Table 5 – Smart Card Security for HP ProtectTools Features and Benefits

Feature	Benefit
Initialize and configure Smart Card security features such as pre boot Smart Card authentication.	Provides a complete Smart 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 Smart Card.	Provides a mechanism to recover from a situation where a user or administrator loses their Smart Card.
Provides the ability to configure an administrator Smart Card that can be used on multiple systems to access BIOS configuration settings.	Allows an administrator to configure a single Smart Card (or multiple cards) that can be used to securely access BIOS configuration settings without requiring the use of a BIOS administrator password.

## Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools is the glue that brings the different security technologies together to create a behavior. Credential Manager gives users the ability to specify how the

<sup>2</sup> The HP ProtectTools Smart Card part number is DR032A.

different available security technologies work together to provide protection against unauthorized access to the client.

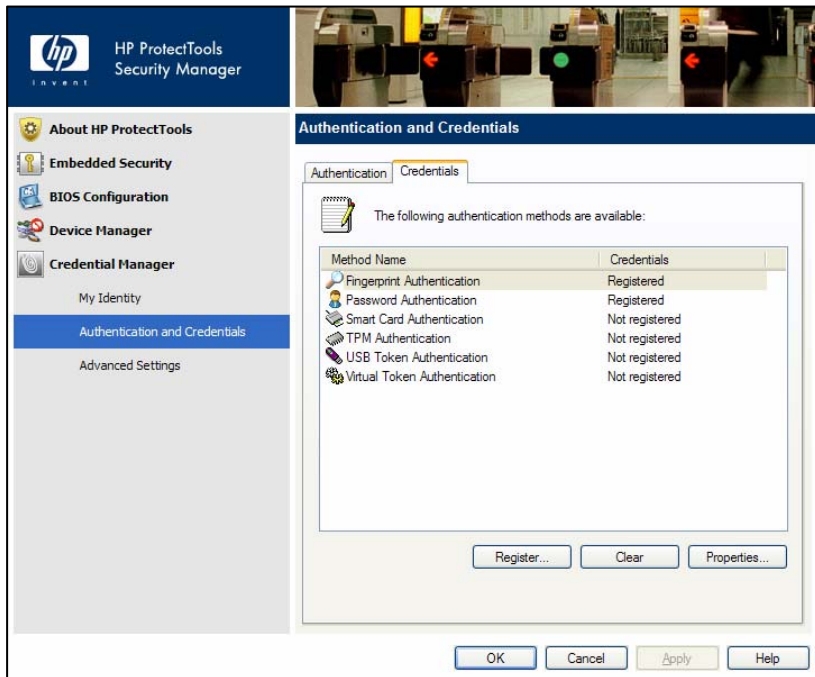


Figure 7 – Credential Manager for HP ProtectTools

These technologies include Smart Cards, Java Cards, Biometrics, USB Tokens and other future technologies. 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:

- Fully integrated with HP ProtectTools Security Manager
- Support for Smart Cards, Java Cards, Biometric fingerprint security, USB Tokens, Virtual Tokens and Passwords
- single sign-on capability protects passwords for websites, applications and network resources

Table 6 – 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.
Windows logon capability	Enables the use of any supported security technology to logon onto Windows providing a more secure and convenient alternative to password authentication.
Single sign-on manages user credentials for websites, applications and protected network resources	Users no longer need to remember multiple passwords for protected websites, applications and network resources. Single sign on works with multifactor authentication capabilities to add additional protection requiring users to re-authenticate when accessing particularly sensitive data. Registering new websites, applications or network logon dialogues is fully automated making it easy for users to begin taking advantage of the added convenience and security of the single sign-on feature.

# Platform Support

HP ProtectTools Security Manager is supported across a range of HP business notebooks, desktops and workstations. The following table provides details of support per product.

<b>BUSINESS NOTEBOOKS</b>	3400 - New	4200	4400 - New	61x0	61x5 FF	61x5 DF	6200	63x0 FF - New	63x0 DF - New	63x5 - New	6400 - New	7400	8200	8400 - New	9600	9700 - New
<b>Hardware Support</b>																
TPM Embedded Security Chip v.1.1		O		N	N	N	O		N	N			O		N	
TPM Embedded Security Chip v.1.2	S		S					S			S			S		S
Integrated Fingerprint Sensor	S	N	S	N	S	N	N	S	O	O	S	N	N	O	N	O
Integrated Smartcard Reader	O	O	O	O	O	O	S	O	O	O	S	N	S	S	N	S
<i>S = Standard / O = Optional / N = Not Available</i>																
<b>ProtectTools Support</b>																
HP ProtectTools Security Manager	P	P	P	P	P	P	P	P	P	P	P	P	P	P	W	P
Credential Manager for HP ProtectTools	P	P	P	P	P	P	P	P	P	P	P	P	P	P	W	P
BIOS Configuration for HP ProtectTools	P	P	P	P	P	P	P	P	P	P	P	P	P	P	N	P
Embedded Security for HP ProtectTools	P	W	P	N	N	N	W	P	N	N	P	N	W	P	N	P
SmartCard Security for HP ProtectTools	W	W	W	W	W	W	W	W	W	W	W	W	W	W	N	W
Java Card Security for HP ProtectTools	W	W	W	W	W	W	W	W	W	W	W	W	W	W	N	W
Device Access Manager for HP ProtectTools	W	W	W	W	W	W	W	W	W	W	W	W	W	W	N	W
HP Disk Sanitizer	S	N	S	N	N	N	N	S	S	S	S	S	S	N	S	S
LoJack for Laptops	S	S	S	S	N	N	S	S	S	S	S	S	S	S	N	S

*P = Pre-installed / W = Web Release / S = Supported / N = Not Supported*

Table 7 - HP ProtectTools solution set support for Business Notebooks

## Frequently Asked Questions

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

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

- Device Access Manager for HP ProtectTools
- Smart Card Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS configuration for HP ProtectTools
- Embedded Security for HP ProtectTools
- Credential 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
- Biometric (Fingerprint) authentication
- USB Token
- Virtual Token
- Password authentication

**Q.** How does the Smart Card security solution compare to the Biometric solution.

**A.** HP Clients PC's and Software support both Smart Card authentication and biometric authentication. HP business notebooks offer both integrated smartcard readers as well as integrated Biometric sensors. Each has a specific applicability to task, and as a general guideline, HP recommends smartcards 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.** Can Smart Cards be used for pre-boot authentication?

**A.** Yes, Smart Cards can be used for pre-boot authentication. Supported cards include the HP ProtectTools smartcard 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.** 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 utilize 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 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. What if a user utilizes multiple PCs, can the user's identity be used on 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.

## Additional Resources

1. *HP ProtectTools Embedded Security – the HP Trusted Computing Implementation*, Hewlett-Packard Company, October 2003.
2. *HP Embedded Security for ProtectTools - Embedded Security Chip Pre-Boot User Authentication*, Hewlett-Packard Company, January 2005.
3. *HP ProtectTools Embedded Security – Expanding Trust Within the Enterprise Computing Environment*, Hewlett-Packard Company, May 2003.
4. *ProtectTools Smart Card Security Manager*, Hewlett-Packard Company, July 2003.
5. Pearson, Siani, et al, *Trusted Computing Platforms: TCPA Technology in Context*, Prentice Hall PTR, July 2002.

© 2004 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.

Itanium is a trademark or registered trademark of Intel Corporation in the U.S. and other countries and is used under license.

5982-9847EN, 11/2004