

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.

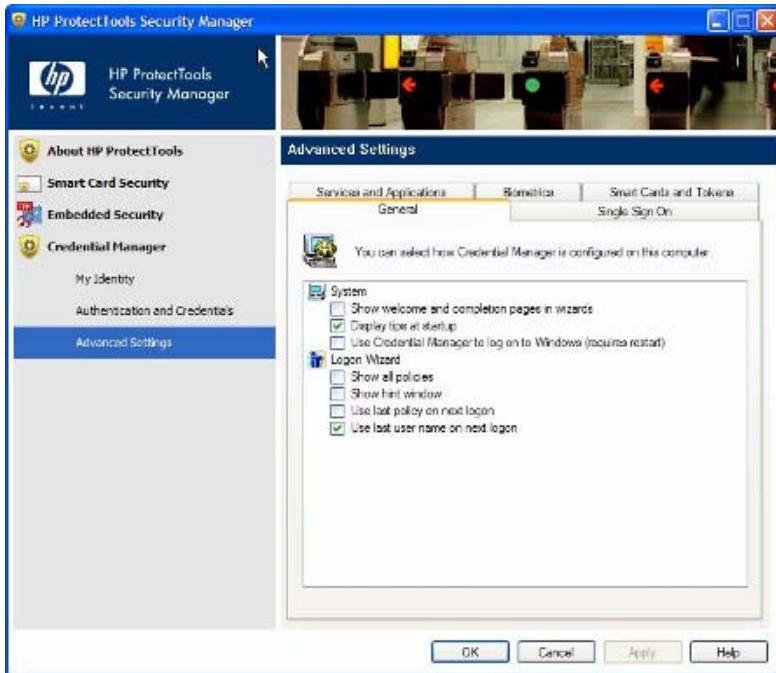


Figure 1 - HP ProtectTools Security Manager Console

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.

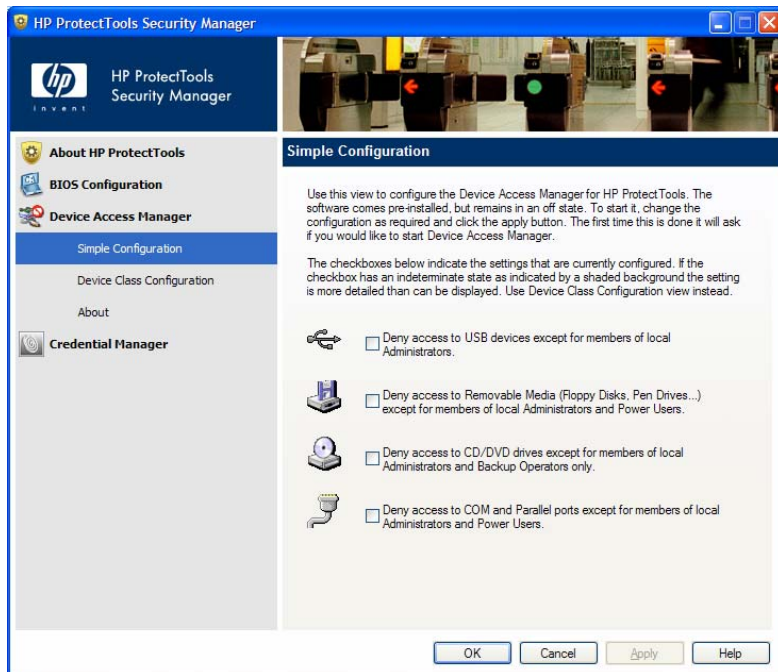


Figure 2 – Device Access Manager for HP ProtectTools

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/

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.

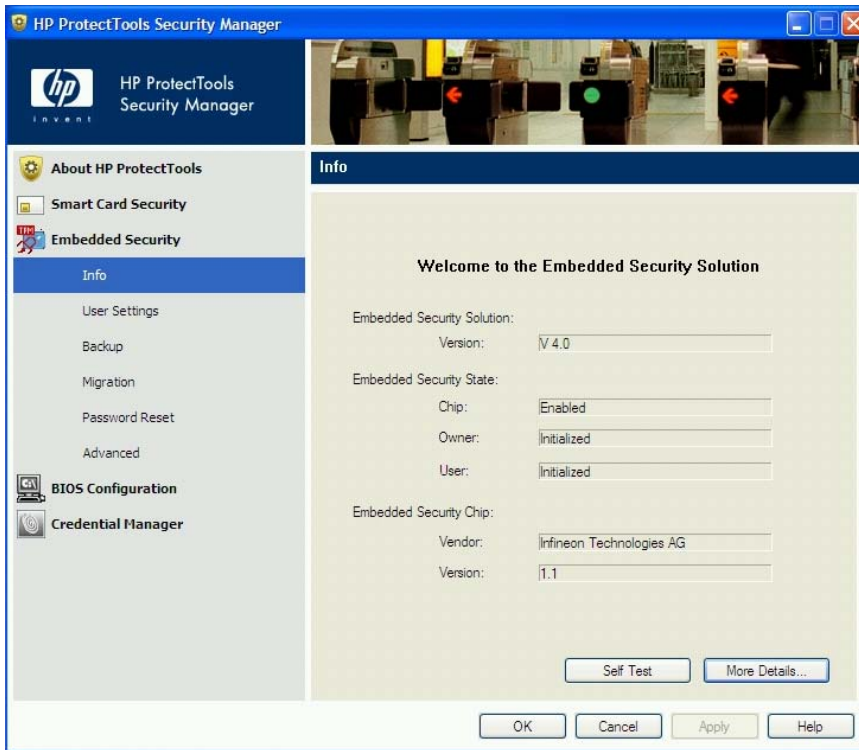


Figure 3 - Embedded Security for HP ProtectTools

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.

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.

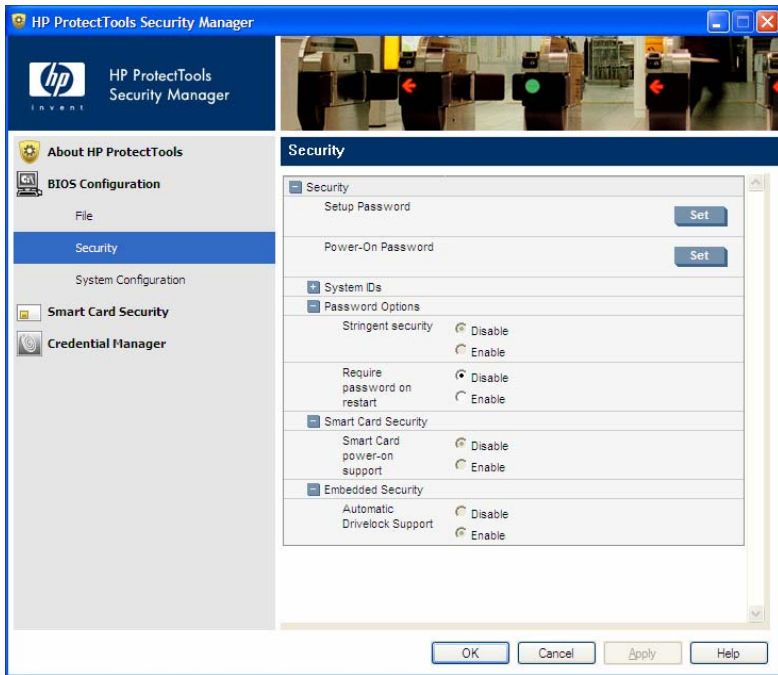


Figure 4 – BIOS configuration for HP ProtectTools

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

