



i n v e n t

# **HP ProtectTools Security Manager Guide**

HP Compaq Business Desktops

Document Part Number: 407154-001

**December 2005**

This guide provides instructions for configuring and using HP ProtectTools Security Manager.

© Copyright 2005 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice.

Microsoft and Windows are trademarks of Microsoft Corporation in the U.S. and other countries.

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.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company.



**WARNING:** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

---



**CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

---

## **HP ProtectTools Security Manager Guide**

HP Compaq Business Desktops

First Edition (December 2005)

Document Part Number: 407154-001

---

# Contents

## 1 Introduction

ProtectTools Security Manager . . . . .	1-1
Accessing the ProtectTools Security Manager . . . . .	1-2
Understanding Security Roles . . . . .	1-3
Managing ProtectTools Passwords . . . . .	1-4
Creating a Secure Password . . . . .	1-8

## 2 Smart Card Security for ProtectTools

Basic Concepts . . . . .	2-1
--------------------------	-----

## 3 Embedded Security for ProtectTools

Basic Concepts . . . . .	3-1
Setup Procedures . . . . .	3-2
HP Client Manager . . . . .	3-3

## 4 BIOS Configuration for ProtectTools

Basic Concepts . . . . .	4-1
Changing BIOS Settings . . . . .	4-1

## 5 Credential Manager for ProtectTools

Basic Concepts . . . . .	5-1
Installation Procedure . . . . .	5-2

**Glossary**

**Index**

---

# Introduction

## ProtectTools Security Manager

ProtectTools Security Manager software provides security features that help protect against unauthorized access to the computer, networks, and critical data. Enhanced security functionality is provided by the following modules:

- Smart Card Security for ProtectTools
- Embedded Security for ProtectTools
- BIOS Configuration for ProtectTools
- Credential Manager for ProtectTools

The modules available for your computer may vary depending on your model. For example, Embedded Security for ProtectTools requires that the Trusted Platform Module (TPM) embedded security chip (some models only) be installed on your computer, and Smart Card Security for ProtectTools requires an optional smart card and reader.

ProtectTools modules may be preinstalled, preloaded, or available for purchase from the HP Web site. Visit <http://www.hp.com> for more information.



Refer to the ProtectTools Help screens for specific instructions for the ProtectTools modules.

---

## Accessing the ProtectTools Security Manager

To access the ProtectTools Security Manager from the Microsoft® Windows Control Panel:

- » Windows® XP  
Click **Start > Control Panel > Windows Security Center > ProtectTools Security Manager.**
- » Windows 2000  
Click **Start > All Programs > HP ProtectTools Security Manager.**



After you have configured the Credential Manager module, you can also open ProtectTools by logging on to Credential Manager directly from the Windows logon screen. For more information, refer to [Chapter 5, “Credential Manager for ProtectTools.”](#)

---

# Understanding Security Roles

In managing computer security (particularly for large organizations), one important practice is to divide responsibilities and rights among various types of administrators and users.

---



In a small organization or for individual use, these roles may all be held by the same person.

---

For ProtectTools, the security duties and privileges can be divided into the following roles:

- **Security officer**—Defines the security level for the company or network and determines the security features to deploy, such as smart cards, biometric readers, or USB tokens.



Many of the features in ProtectTools can be customized by the security officer in cooperation with HP. For more information, visit <http://www.hp.com>.

- **IT administrator**—Applies and manages the security features defined by the security officer. Can also enable and disable some features. For example, if the security officer has decided to deploy smart cards, the IT administrator can enable smart card BIOS security mode.
- **User**—Uses the security features. For example, if the security officer and IT administrator have enabled smart cards for the system, the user can set the smart card PIN and use the card for authentication.


# Managing ProtectTools Passwords

Most of the ProtectTools Security Manager features are secured by passwords. The following table lists the commonly used passwords, the software module where the password is set, and the password function.

The passwords that are set and used by IT administrators only are indicated in this table as well. All other passwords may be set by regular users or administrators.

## Password Management



---

<b>ProtectTools Password</b>	<b>Set in this ProtectTools Module</b>	<b>Function</b>
Computer Setup administrator password  Also known as BIOS administrator, <b>F10</b> Setup, or Security Setup password	BIOS Configuration, by IT administrator	Protects access to the BIOS Computer Setup utility and security settings.
Power-on password	BIOS Configuration	Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.

---





## Password Management (*Continued*)

<b>ProtectTools Password</b>	<b>Set in this ProtectTools Module</b>	<b>Function</b>
Smart card administrator password   Also known as BIOS administrator card password	Smart Card Security, by IT administrator	Links the smart card to the computer for identification purposes. Allows a computer administrator to enable or disable Computer Setup passwords, generate a new administrator card, and create recovery files to restore user or administrator cards.
Smart card PIN	Smart Card Security	Protects access to the smart card contents and to computer access when an optional smart card and reader is used.
Smart card recovery file password	Smart Card Security	Protects access to the recovery file that contains the BIOS passwords.
Smart card user password   Also known as BIOS user card password	Smart Card Security	Links the smart card to the computer for identification. Allows a user to create a recovery file to restore a user card.

## Password Management (*Continued*)

---

<b>ProtectTools Password</b>	<b>Set in this ProtectTools Module</b>	<b>Function</b>
Basic User Key password  Also known as: Embedded Security password	Embedded Security	When enabled as the BIOS power-on authentication support password, protects access to the computer contents when computer is turned on, restarted, or restored from hibernation.
Emergency Recovery Token password  Also known as: Emergency Recovery Token Key	Embedded Security, by IT administrator	Protects access to the Emergency Recovery Token, which is a backup file for the TPM embedded security chip.
Owner password	Embedded Security, by IT administrator	Protects the system and the TPM chip from unauthorized access to all owner functions of Embedded Security.

---

## Password Management (*Continued*)

<b>ProtectTools Password</b>	<b>Set in this ProtectTools Module</b>	<b>Function</b>
Credential Manager logon password	Credential Manager	<p>This password offers 2 options:</p> <ul style="list-style-type: none"> <li>• It can be used in place of the Windows logon process, allowing access to Windows and Credential Manager simultaneously.</li> <li>• It can be used in a separate logon to access Credential Manager after logging on to Microsoft Windows.</li> </ul>
Credential Manager recovery file password	Credential Manager, by IT administrator	Protects access to the Credential Manager recovery file.
Windows logon password	Windows Control Panel	Can be used in manual logon or saved on the smart card.

## Creating a Secure Password

When creating passwords, you must first follow any specifications that are set by the program. In general, however, consider the following guidelines to help you create strong passwords and reduce the chances of your password being compromised:

- Use passwords with more than 6 characters, preferably more than 8.
- Mix the case of letters throughout your password.
- Whenever possible, mix alphanumeric characters and include special characters and punctuation marks.
- Substitute special characters or numbers for letters in a key word. For example, you can use the number 1 for letters I or L.
- Combine words from 2 or more languages.
- Split a word or phrase with numbers or special characters in the middle, for example, “Mary2-2Cat45.”
- Do not use a password that would appear in a dictionary.
- Do not use your name for the password, or any other personal information, such as birth date, pet names, or mother's maiden name, even if you spell it backwards.
- Change passwords regularly. You might change only a couple of characters that increment.
- If you write down your password, do not store it in a commonly visible place very close to the computer.
- Do not save the password in a file, such as an e-mail, on your computer.
- Do not share accounts or tell anyone your password.

---

# Smart Card Security for ProtectTools

## Basic Concepts

Smart Card Security for ProtectTools manages the smart card setup and configuration for computers equipped with an optional smart card reader.

With Smart Card Security for ProtectTools, you can

- Access Smart Card Security features.
- Initialize a smart card so that it can be used with other ProtectTools modules, such as Credential Manager for ProtectTools.
- Work with the Computer Setup utility to enable smart card authentication in a preboot environment, and to configure separate smart cards for an administrator and a user. This requires a user to insert the smart card and optionally enter a PIN prior to allowing the operating system to load.
- Set and change the password used to authenticate users of the smart card.
- Back up and restore smart card BIOS passwords stored on the smart card.
- Save the BIOS password on the smart card.



Refer to the ProtectTools Help screens for specific instructions for ProtectTools Security Manager.

---



---

# Embedded Security for ProtectTools

## Basic Concepts

---



The integrated Trusted Platform Module (TPM) embedded security chip must be installed in your computer to use Embedded Security for ProtectTools.

---

Embedded Security for ProtectTools protects against unauthorized access to user data or credentials. This module provides the following security features:

- Enhanced Microsoft Encryption File System (EFS) file and folder encryption
- Creation of a personal secure drive (PSD) for encrypting user data
- Data management functions, such as backing up and restoring the key hierarchy
- Support for third-party applications that use MSCAPI (such as Microsoft Outlook and Microsoft Internet Explorer) and applications that use PKCS#11 (such as Netscape) for protected digital certificate operations when using the Embedded Security software

The TPM embedded security chip enhances and enables other ProtectTools Security Manager security features. For example, Credential Manager for ProtectTools can use the TPM embedded chip as an authentication factor when the user logs on to

Windows. On some models, the TPM embedded security chip also enables enhanced BIOS security features accessed through BIOS Configuration for ProtectTools.

## Setup Procedures

---



**CAUTION:** To reduce security risk, it is highly recommended that your IT administrator immediately initialize the TPM embedded security chip. Failure to initialize the TPM embedded security chip could result in an unauthorized user, a computer worm, or a virus could initialize the TPM embedded security chip and restrict access to the PC.

---

The TPM embedded security chip can be enabled in the BIOS Computer Setup utility, BIOS Configuration for ProtectTools, or HP Client Manager.

To enable the TPM embedded security chip:

1. Open Computer Setup by turning on or restarting the computer, and then pressing F10 while the “F10 = ROM Based Setup” message is displayed in the lower-left corner of the screen.
2. Use the arrow keys to select Security > Setup Password. Set a password.
3. Select Embedded Security Device.
4. Use the arrow keys to select Embedded Security Device—Disable. Use the arrow keys to change it to Embedded Security Device—Enable.
5. Select Enable > Save changes and exit.



Refer to the ProtectTools Help screens for specific instructions for ProtectTools Embedded Security.

---



## **HP Client Manager**

HP Client Manager has several management features. For more information, see

[http://h18000.www1.hp.com/im/client\\_mgr.html](http://h18000.www1.hp.com/im/client_mgr.html).



---

# BIOS Configuration for ProtectTools

## Basic Concepts

BIOS Configuration for ProtectTools provides access to the Computer Setup utility security and configuration settings. This gives users Windows access to system security features that are managed by Computer Setup.

With BIOS Configuration, you can

- Manage power-on passwords and setup passwords.
- Enable smart card BIOS support.
- Enable and disable hardware features, such as CD-ROM boot or different hardware ports.
- Configure boot options, such as changing the boot order.



Many of the features in BIOS Configuration for ProtectTools are also available in the Computer Setup utility.

---

## Changing BIOS Settings

BIOS Configuration allows you to manage various computer settings that would otherwise be accessible only by pressing **F10** at startup and entering the Computer Setup utility. Refer to the *Computer Setup (F10) Utility Guide* on the *Documentation CD* that shipped with the computer for information on settings and features.



Refer to the ProtectTools Help screens for specific instructions for ProtectTools BIOS Configuration.

---

---

# Credential Manager for ProtectTools

## Basic Concepts

Credential Manager for ProtectTools has security features that provide a secure and convenient computing environment. These features include the following:

- Alternatives to passwords when logging on to Microsoft Windows, such as using a smart card or biometric reader
- Single Sign On feature that automatically remembers credentials (user ids and passwords) for Web sites, applications, and protected network resources
- Support for optional security devices, such as smart cards and biometric readers
- Support for additional security settings, such as requiring authentication with an optional security device to unlock the computer and access applications
- Enhanced encryption for stored passwords, when implemented with a TPM embedded security chip

## Installation Procedure

Credential Manager for ProtectTools is preloaded on the computer, but it must be installed before it can be used. To install Credential Manager:

- » Click **Start > All Programs > Credential Manager for ProtectTools**.

You can choose to log on to Credential Manager in any of the following ways:

- Credential Manager Logon Wizard (preferred)
- Credential Manager icon in the notification area
- ProtectTools Security Manager



If you use the Credential Manager Logon prompt on the Windows Logon screen to log in to Credential Manager, you are logged in to Windows at the same time.

---

## Logging On for the First Time

The first time you open Credential Manager, log on with your regular Windows Logon password. A Credential Manager account is then automatically created with your Windows logon credentials.

After logging on to Credential Manager, you can register additional credentials, such as a fingerprint or a smart card.

At the next logon, you can select the logon policy and use any combination of the registered credentials.



Refer to the ProtectTools Help screens for specific instructions for ProtectTools Security Manager.

---

---

# Glossary

The following terms are used in this document and throughout the ProtectTools Security Manager.

**Authentication**—Process of verifying whether a user is authorized to perform a task, for example, accessing a computer, modifying settings for a particular program, or viewing secured data.

**Biometric**—Category of authentication credentials that use a physical feature, such as a fingerprint, to identify a user.

**BIOS profile**—Group of BIOS configuration settings that can be saved and applied to other accounts.

**BIOS security mode**—Setting in Smart Card Security for ProtectTools that, when enabled, requires the use of a smart card and a valid PIN for user authentication.

**Certification authority**—Service that issues the certificates required to run a public key infrastructure.

**Credentials**—Method by which a user proves eligibility for a particular task in the authentication process.

**Cryptographic service provider (CSP)**—Provider or library of cryptographic algorithms that can be used in a well-defined interface to perform particular cryptographic functions.

**Cryptography**—Practice of encrypting and decrypting data so that it can be decoded only by specific individuals.

**Decryption**—Procedure used in cryptography to convert encrypted data into plain text.

**Digital certificate**—Electronic credentials that confirm the identity of an individual or a company by binding the identity of the digital certificate owner to a pair of electronic keys that are used to sign digital information.

**Digital signature**—Data sent with a file that verifies the sender of the material, and that the file has not been modified after it was signed.

**Domain**—Group of computers that are part of a network and share a common directory database. Domains are uniquely named, and each has a set of common rules and procedures.

**Emergency recovery archive**—Protected storage area that allows the re-encryption of basic user keys from one platform owner key to another.

**Encryption**—Procedure, such as use of an algorithm, employed in cryptography to convert plain text into cipher text in order to prevent unauthorized recipients from reading that data. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard and public-key encryption.

**Encryption File System (EFS)**—System that encrypts all files and subfolders within the selected folder.

**Identity**—In the ProtectTools Credential Manager, a group of credentials and settings that is handled like an account or profile for a particular user.

**Migration**—a task that allows the management, restoration, and transfer of keys and certificates.

**Network account**—Windows user or administrator account, either on a local computer, in a workgroup, or on a domain.

**Personal secure drive (PSD)**—Provides a protected storage area for sensitive data.



**Power-on authentication**—Security feature that requires some form of authentication, such as a smart card, security chip, or password, when the computer is turned on.

**Public Key Infrastructure (PKI)**—Standard that defines the interfaces for creating, using, and administering certificates and cryptographic keys.

**Reboot**—Process of restarting the computer.

**Single Sign On**—Feature that stores authentication data and allows you to use the Credential Manager to access Internet and Windows applications that require password authentication.

**Smart card**—Small piece of hardware, similar in size and shape to a credit card, which stores identifying information about the owner. Used to authenticate the owner to a computer.

**Smart card administrator password**—Password that links an administrator smart card with the computer in Computer Setup for identification at startup or restart. This password can be set manually by the administrator or randomly generated.

**Smart card user password**—Password that links a user smart card with the computer in Computer Setup for identification at startup or restart. This password can be set manually by the administrator or randomly generated.

**Stringent security**—Security feature in BIOS Configuration that provides enhanced protection for the power-on and administrator passwords and other forms of power-on authentication.

**Trusted Platform Module (TPM) embedded security chip (some models only)**—Integrated security chip that can protect highly sensitive user information from malicious attackers. It is the root-of-trust in a given platform. The TPM provides cryptographic algorithms and operations that meets the Trusted Computing Group (TCG) specifications.

**USB token**—Security device that stores identifying information about a user. Like a smart card or biometric reader, it is used to authenticate the owner to a computer.

**Virtual token**—Security feature that works very much like a smart card and reader. The token is saved either on the computer hard drive or in the Windows registry. When you log on with a virtual token, you are asked for a user PIN to complete the authentication.

**Windows user account**—Profile for an individual authorized to log on to a network or to an individual computer.

---

# Index

## B

Basic User Key password,  
definition 1–6

## BIOS

- administrator card password,  
definition 1–5
- administrator password,  
definition 1–4
- user card password, definition  
1–5

BIOS Configuration for  
ProtectTools 4–1

## C

Computer Setup administrator  
password, definition 1–4

Credential Manager for  
ProtectTools 5–1

- logon password 1–7
- recovery file password 1–7

## E

Embedded Security for  
ProtectTools 3–1

emergency recovery token  
password, definition 1–6

## F

F10 Setup password 1–4

## O

owner password, definition 1–6

## P

passwords

- guidelines 1–8
- managing 1–4

power-on password, definition 1–4

ProtectTools Security Manager  
1–1

## S

security setup password 1–4

smart card

- administrator password,  
definition 1–5
- PIN, definition 1–5
- recovery file password,  
definition 1–5
- user password, definition 1–5

Smart Card Security for  
ProtectTools 2–1

## W

Windows logon password 1–7

