Security

User Guide

First Edition: March 2006

Document Part Number: 406809-001

Table of contents

1 Security features

NOTE Security solutions are designed to act as deterrents. These deterrents may not prevent a product from being mishandled or stolen.

NOTE Your computer supports CompuTrace, which is an online security-based tracking and recovery service. If the computer is stolen, CompuTrace can track the computer if the unauthorized user accesses the Internet. You must purchase the software and subscribe to the service in order to use CompuTrace. For information about ordering the CompuTrace software, visit http://www.hpshopping.com.

Security features provided with your computer can protect the computer, personal information, and data from a variety of risks. The way you use your computer will determine which security features you need to use.

The Microsoft® Windows® operating system offers certain security features. Additional security features are listed in the following table. Most of these additional security features can be configured in the Computer Setup utility (referred to hereafter as Computer Setup).

To protect against	Use this security feature
Unauthorized use of the computer	• Power-on authentication using passwords or smart cards • ProtectTools Security Manager
Unauthorized access to Computer Setup (f10)	Setup password in Computer Setup*
Unauthorized access to the contents of a hard drive	DriveLock password in Computer Setup*
Unauthorized reset of Computer Setup (f10) passwords.	Stringent security feature in Computer Setup
Unauthorized startup from an optical drive, diskette drive, or internal network adapter	Boot options feature in Computer Setup*
Unauthorized access to a Windows user account	Credential Manager for ProtectTools
Unauthorized access to data	• Firewall software • Windows updates • ProtectTools Security Manager
Unauthorized access to Computer Setup settings and other system identification information	Setup password in Computer Setup*
Unauthorized removal of the computer	Security cable slot (used with an optional security cable).

*Computer Setup is a non-Windows utility accessed by pressing f10 when the computer is turned on or restarted. When using Computer Setup, you must use the keys on your computer to navigate and make selections.

2 Passwords

Most security features use passwords. Whenever you set a password, write down the password and store it in a secure location away from the computer. Note the following password considerations:

- Setup, power-on, and DriveLock passwords are set in Computer Setup and are managed by the system BIOS.
- The smart card PIN and the embedded security password, which are ProtectTools Security Manager passwords, can be enabled in Computer Setup to provide BIOS password protection in addition to their normal ProtectTools functions. The smart card PIN is used with a supported smart card reader, and the embedded security password is used with the optional embedded security chip.
- Windows passwords are set only in the Windows operating system.
- If you forget the setup password set in Computer Setup, you will not be able to access the utility.
- If you have the stringent security feature enabled in Computer Setup and you forget the setup password or the power-on password, the computer is inaccessible and can no longer be used. Call Customer Care or your service partner for additional information.
- If you forget the power-on password and the setup password set in Computer Setup, you cannot turn on the computer or restore from hibernation. Call Customer Care or your service partner for additional information.
- If you forget both the user and the master DriveLock passwords set in Computer Setup, the hard drive that is protected by the passwords is permanently locked and can no longer be used.

The following tables list commonly used Computer Setup and Windows passwords and describe their functions.

Computer Setup passwords	Function
Setup password	Protects access to Computer Setup.
Power-on password	Protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.
DriveLock master password	Protects access to the internal hard drive that is protected by DriveLock, and is used to remove DriveLock protection.
DriveLock user password	Protects access to the internal hard drive that is protected by DriveLock.
Smart card PIN	Protects access to smart card and Java™ Card contents, and protects computer access when a smart card or Java Card and a smart card reader is used.
Embedded security password	When enabled as a BIOS password, protects access to the computer contents when the computer is turned on, restarted, or restored from hibernation.

Computer Setup passwords	Function
	This password requires the optional embedded security chip to support this security feature.

Windows passwords	Function
Administrator password*	Protects access to Windows administrator-level computer contents.
User password	Protects access to a Windows user account. It also protects access to the computer contents and must be entered when you resume from standby or restore from hibernation.

*For information about setting a Windows administrator password or a Windows user password, select **Start > Help and Support**.

Guidelines for setting passwords

You can use the same password for a Computer Setup feature and for a Windows security feature. You can also use the same password for more than one Computer Setup feature.

A password set in Computer Setup

- Can be any combination of up to Computer Setup letters and numbers and is not case sensitive.
- Must be set and entered with the same keys. For example, if you set a password with keyboard number keys, your password will not be recognized if you subsequently try to enter it with the embedded numeric keypad.

  NOTE Select models include a separate numeric keypad, which functions exactly like the keyboard number keys.

- Must be entered at a Computer Setup prompt. A password set in Windows must be entered at a Windows prompt.

Tips for creating and saving passwords:

- When creating passwords, follow requirements set by the program.
- Write down your passwords and store them in a secure place away from the computer.
- Do not store passwords in a file on the computer.
- Do not use your name or other personal information that could be easily discovered by an outsider.

Computer Setup setup password

The Computer Setup setup password protects the configuration settings and system identification information in Computer Setup. After this password is set, it must be entered to access Computer Setup and to make changes using Computer Setup.

The setup password

- Is not interchangeable with a Windows administrator password, although both passwords can be identical.
- Is not displayed as it is set, entered, changed, or deleted.
- Must be set and entered with the same keys. For example, a setup password set with keyboard number keys will not be recognized if you enter it thereafter with embedded numeric keypad number keys.
- Can include any combination of up to 32 letters and numbers and is not case sensitive.

Setting a setup password

A setup password is set, changed, and deleted in Computer Setup.

To manage this password:

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**, and then press enter.
   - To set a setup password:

     Type your password in the **New password** and **Verify new password** fields, and then press f10.
   - To change an administrator password:

     Type your current password in the **Old password** field, type a new password in the **New password** and **Verify new password** fields, and then press f10.
   - To delete a setup password:

     Type your current password in the **Old password** field, and then press f10.
3. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Entering a setup password

At the **Setup password** prompt, type your setup password (using the same kind of keys you used to set the password), and then press enter. After 3 unsuccessful attempts to enter the setup password, you must restart the computer and try again.

Computer Setup power-on password

The Computer Setup power-on password prevents unauthorized use of the computer. After this password is set, it must be entered each time the computer is turned on.

A power-on password

- Is not displayed as it is set, entered, changed, or deleted.
- Must be set and entered with the same keys. For example, a power-on password set with keyboard number keys will not be recognized if you enter it thereafter with embedded numeric keypad number keys.
- Can include any combination of up to 32 letters and numbers and is not case sensitive.

Setting a power-on password

A power-on password is set, changed, and deleted in Computer Setup.

To manage this password:

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 > Power-On password**, and then press enter.
   - To set a power-on password:

     Type the password in the **New password** and **Verify new password** fields, and then press f10.
   - To change a power-on password:

     Type the current password in the **Old password** field, type the new password in the **New password** and **Verify new password** fields, and then press f10.
   - To delete a power-on password:

     Type the current password in the **Old password** field, and then press f10.
3. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Entering a power-on password

At the **Power-on Password** prompt, type your password (using the same kind of keys you used to set the password), and then press enter. After 3 unsuccessful attempts to enter the password, you must turn off the computer, turn it back on, and then try again.

Requiring a power-on password at restart

In addition to requiring that a power-on password be entered each time the computer is turned on, you can also require that a power-on password be entered each time the computer is restarted.

To enable and disable this feature in Computer Setup:

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 > Password options > Require password on restart**, and then press enter.
3. Use the arrow keys to enable or disable the password feature, and then press f10.
4. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

Computer Setup DriveLock

CAUTION To prevent the DriveLock-protected hard drive from becoming permanently unusable, record the DriveLock user password and the DriveLock master password in a safe place away from your computer. If you forget both DriveLock passwords, the hard drive will be permanently locked and can no longer be used.

DriveLock protection prevents unauthorized access to the contents of a hard drive. DriveLock can be applied only to the internal hard drive(s) of the computer. After DriveLock protection is applied to a drive, a password must be entered to access the drive. The drive must be inserted into the computer, not into an optional docking device or external MultiBay, in order for it to be accessed by the DriveLock passwords.

To apply DriveLock protection to an internal hard drive, a user password and a master password must be set in Computer Setup. Note the following considerations about using DriveLock protection:

- After DriveLock protection is applied to a hard drive, the hard drive can only be accessed by entering either the user password or the master password.
- The owner of the user password should be the day-to-day user of the protected hard drive. The owner of the master password may be a system administrator or the day-to-day user.
- The user password and the master password can be identical.
- You can delete a user password or master password only by removing DriveLock protection from the drive. DriveLock protection can be removed from the drive only with the master password.

NOTE When your power-on password and DriveLock user password are identical, you will be prompted to enter only a power-on password instead of both a power-on password and a DriveLock user password.

Setting a DriveLock password

To access the DriveLock settings in Computer Setup:

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 > DriveLock passwords**, and then press enter.
3. Select the location of the hard drive for protection, and then press f10.
4. Use the arrow keys to select **Enable** in the **Protection** field, and then press f10.
5. Read the warning. To continue, press f10.
6. Type your user password in the **New password** and **Verify new password** fields, and then press f10.
7. Type your master password in the **New password** and **Verify new password** fields, and then press f10.
8. To confirm DriveLock protection on the drive you have selected, type `DriveLock` in the confirmation field, and then press f10.
9. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Entering a DriveLock password

Be sure that the hard drive is inserted into the computer (not into an optional docking device or external MultiBay).

At the **DriveLock HDD Bay Password** prompt, type your user or master password (using the same kind of keys you used to set the password), and then press enter.

After 2 incorrect attempts to enter the password, you must restart the computer and try again.

Changing a DriveLock password

To access the DriveLock settings in Computer Setup:

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 > DriveLock passwords**, and then press enter.
3. Use the arrow keys to select the location of the internal hard drive, and then press f10.
4. Use the arrow keys to select the field for the password you want to change. Type your current password in the **Old password** field, and then type the new password in the **New password** field and in the **Verify new password** field. Then press f10.
5. Type your new password again in the **Confirm New Password** field, and then press enter.
6. When the setup notice message is displayed, press enter to save your changes.
7. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Removing DriveLock protection

To access the DriveLock settings in Computer Setup:

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 > DriveLock passwords**, and then press enter.
3. Use the arrow keys to select the location of the internal hard drive, and then press f10.
4. Use the arrow keys to select **Disable** in the **Protection** field, and then press f10.
5. Type your master password in the **Old password** field. Then press f10.
6. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

3 Computer Setup security features

Device security

From the Boot options menu or the Port options menu in Computer Setup, you can disable or enable system devices.

To disable or reenable the system devices in Computer Setup:

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 **System Configuration > Boot options** or **System Configuration > Port options**, and then enter your preferences.
3. To confirm your preferences, press f10.
4. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Computer Setup stringent security

CAUTION To prevent the computer from becoming permanently unusable, record your configured setup password, power-on password, or smart card PIN in a safe place away from your computer. Without these passwords or PIN, the computer cannot be unlocked.

The stringent security feature enhances power-on security by forcing user authentication with your configured setup password, power-on password, or smart card PIN before granting access to the system.

Setting stringent security

To enable stringent security in Computer Setup:

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 > Password options**, and then press enter.
3. Use the arrow keys to select the **Stringent security** field.
4. Read the warning. To continue, press f10.
5. To enable the feature each time the computer is turned on, press f10.
6. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Removing stringent security

To remove stringent security in Computer Setup:

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 > Password options**, and then press enter.
3. Use the arrow keys to select **Disable** in the **Stringent security** field, and then press f10.
4. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

Computer Setup System Information

The System Information feature in Computer Setup provides 2 types of system information:

- Identification information about the computer model and the battery packs.
- Specification information about the processor, cache, memory, ROM, video revision, and keyboard controller revision.

To view this general system information, use the arrow keys to select File > System Information.

NOTE To prevent unauthorized access to this information, you must create a setup password in Computer Setup. For additional information, refer to "Setting a setup password."

Computer Setup System IDs

The System IDs feature in Computer Setup allows you to display or enter the computer asset tag and ownership tag.

NOTE To prevent unauthorized access to this information, you must create a setup password in Computer Setup. For additional information, refer to "Setting a setup password."

To manage this feature:

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. To view or enter identification tag IDs for system components, use the arrow keys to select **Security > System IDs**.
3. To confirm the information or your preferences, press f10.
4. To save your preferences, use the arrow keys to select **File > Save changes and exit**. Then follow the instructions on the screen.

   Your preferences go into effect when the computer restarts.

4 Antivirus software

When you use the computer for e-mail, network, or Internet access, you expose the computer to computer viruses. Computer viruses can disable the operating system, applications, or utilities, or cause them to function abnormally.

Antivirus software can detect most viruses, destroy them, and in most cases, repair any damage they have caused. To provide ongoing protection against newly discovered viruses, antivirus software must updated.

Norton Internet Security is preinstalled on the computer. For information about using the Norton Internet Security software, select **Start > All Programs > Norton Internet Security > Help and Support**.

For more information about computer viruses, type `viruses` in the Search field in the Help and Support Center.

5 Firewall software

When you use the computer for e-mail, network, or Internet access, unauthorized persons may be able to gain access to information about you, the computer, and your information. Use the firewall software preinstalled on the computer to protect your privacy.

Firewall features include logging, reporting, and automatic alarms to monitor all incoming and outgoing traffic. Refer to the firewall documentation or contact your firewall manufacturer for more information.

NOTE Under some circumstances a firewall can block access to Internet games, interfere with printer or file sharing on a network, or block authorized e-mail attachments. To temporarily solve the problem, disable the firewall, perform the task that you want to perform, and then reenable the firewall. To permanently resolve the problem, reconfigure the firewall.

6 Critical security updates (select models only)

CAUTION To protect the computer from security breaches and computer viruses, install the online critical updates from Microsoft as soon as you receive an alert.

A *Critical Security Updates for Windows XP* disc may have been included with your computer to provide additional updates delivered after the computer was configured.

To update your system using the *Critical Security Updates for Windows XP* disc:

1. Insert the disc into the drive. (The disc automatically runs the installation application.)
2. Follow the on-screen instructions to install all updates. (This may take a few minutes.)
3. Remove the disc.

Additional updates to the operating system and other software may have become available *after* the computer was shipped. To be sure all available updates are installed on the computer:

- Run Windows Update monthly to install the latest software from Microsoft.
- Obtain updates, as they are released, from the Microsoft Web site and through the updates link in the Help and Support Center.

7 ProtectTools Security Manager (select models only)

Select computer models come with ProtectTools Security Manager preinstalled. This software can be accessed through the Microsoft Windows Control Panel. It provides security features that help protect against unauthorized access to the computer, networks, and critical data. ProtectTools Security Manager is a security console that provides enhanced functionality with the addition of the following modules:

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

Depending on your computer model, add-on modules may be preinstalled, preloaded, or downloadable from the HP Web site. Visit http://www.hp.com for more information.

Embedded Security for ProtectTools

NOTE You must have the optional trusted platform module (TPM) embedded security chip installed in your computer in order to use Embedded Security for ProtectTools.

Embedded Security for ProtectTools has security features that protect against unauthorized access to user data or credentials, which include the following:

- Administrative functions, such as ownership and management of the owner pass phrase.
- User functions, such as user enrollment and management of user pass phrases.
- Settings configuration, including setting up enhanced Microsoft EFS and Personal Secure Drive for protecting user data.
- Management functions, such as backing up and restoring the key hierarchy.
- Support for third-party applications (such as Microsoft Outlook and Internet Explorer) for protected digital certificate operations when using embedded security.

The optional TPM embedded security chip enhances and enables other ProtectTools Security Manager security features. For example, Credential Manager for ProtectTools can use the embedded chip as an authentication factor when the user logs on to Windows. On select models, the TPM embedded security chip also enables enhanced BIOS security features accessed through BIOS Configuration for ProtectTools.

For more information, refer to the Embedded Security for ProtectTools online Help.

Credential Manager for ProtectTools

Credential Manager for ProtectTools has security features that provide protection against unauthorized access to your computer, including the following:

- Alternatives to passwords when logging on to Microsoft Windows, such as using a smart card to log on to Windows.
- Single sign-on capability that automatically remembers credentials for Web sites, applications, and protected network resources.
- Support for optional security devices, such as smart cards and fingerprint readers.

For more information, refer to the Credential Manager for ProtectTools online Help.

BIOS Configuration for ProtectTools

BIOS Configuration for ProtectTools provides access to BIOS (Computer Setup) security and configuration settings within the ProtectTools Security Manager application. This gives users better access to system security features that are managed by Computer Setup.

With BIOS Configuration for ProtectTools, you can

- Manage power-on passwords and setup passwords.
- Configure other power-on authentication features, such as enabling smart card passwords and embedded security authentication.
- Enable and disable hardware features, such as CD-ROM boot or different hardware ports.
- Configure boot options, which includes enabling MultiBoot and changing the boot order.

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

For more information, refer to the BIOS Configuration for ProtectTools online Help.

Smart Card Security for ProtectTools

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

NOTE Both smart cards and Java Cards use a smart card reader.

With Smart Card Security for ProtectTools, you can

- Access smart card security features. Security enhancements are supported by the optional ProtectTools Smart Card and a smart card reader.
- Initialize a ProtectTools Smart Card so that it can be used with Credential Manager for ProtectTools.
- Work with the BIOS 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 that are stored on the smart card.

For more information, refer to the Smart Card Security for ProtectTools online Help.

Java Card Security for ProtectTools

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

NOTE Both Java Cards and smart cards use a smart card reader.

With Java Card Security for ProtectTools, you can

- Access Java Card security features. Security enhancements are supported by the optional ProtectTools Java Card and a smart card reader.
- Create a unique PIN that allows a Java Card to be used with Credential Manager for ProtectTools.
- Work with the BIOS to enable Java Card authentication in a preboot environment, and to configure separate Java Cards for an administrator and a user. This requires a user to insert the Java Card and enter a PIN prior to allowing the operating system to load.
- Set and change the identity used to authenticate users of the Java Card.
- Back up and restore Java Card identity stored on the Java Card.

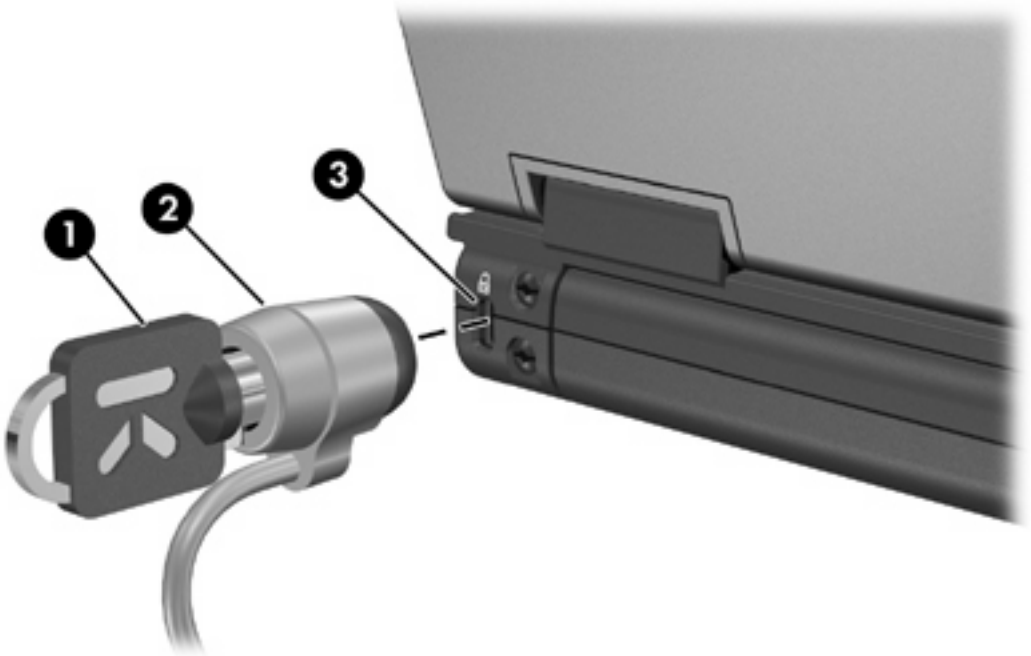
For more information, refer to the Java Card Security for ProtectTools online Help.

8 Security cable

NOTE The security cable is designed to act as a deterrent, but may not prevent the computer from being mishandled or stolen.

To install a security cable:

1. Loop the security cable around a secured object.
2. Insert the key **(1)** into the cable lock **(2)**.
3. Insert the cable lock into the security cable slot on the computer **(3)**, and then lock the cable lock with the key.



NOTE Your computer may look different from the illustration. The location of the security cable slot varies by model.

9 Fingerprint reader (select models only)

Using the fingerprint reader

NOTE The location of the fingerprint reader varies by model.

Registering fingerprints

A fingerprint reader allows you to log on to Windows using a fingerprint registered in ProtectTools Security Manager, instead of using a Windows password.

Whether you are using an HP computer with an integrated fingerprint reader or an optional fingerprint reader, two steps are required for fingerprint logon to Windows:

1. Set up the fingerprint reader.
2. Use your registered fingerprint to log on to Windows.

Step 1: Set up the fingerprint reader

NOTE If you are using an optional fingerprint reader, connect the reader to the computer before performing the steps below.

To set up the fingerprint reader:

1. In Windows, double-click the **Credential Manager** icon in the notification area of the taskbar.

   – or –

   Select **Start > All Programs > ProtectTools Security Manager**, and then click the **Credential Manager** tab, which is located on the left.

2. On the “My Identity” page, click **Log On**, located in the upper-right corner of the page.

   The Credential Manager Logon Wizard opens.

3. On the “Introduce Yourself” page, click Next to accept the default user name.

   NOTE If there are other users registered on this computer, you can select the person whose fingerprints need to be registered by entering the Windows user name.

4. On the “Enter Password” page, enter the user's Windows password, if one has been established. Otherwise, click **Finish**.

5. On the “My Services and Applications” page, click **Register Fingerprints**.

   NOTE By default, Credential Manager requires registration of at least 2 different fingers.

6. When the Credential Manager Registration Wizard opens, slowly swipe your finger downward over the fingerprint sensor.

   NOTE The right index finger is the default finger for enrolling the first fingerprint. You can change the default by clicking the finger you want to register first, on either the left hand or the right hand. When you click a finger, it will be outlined to show it has been selected.

7. Continue swiping the same finger over the fingerprint sensor until the finger on the screen turns green.

   NOTE The progress indicator advances after each finger swipe. Multiple swipes are necessary to register a fingerprint.

   NOTE If you need to start over during the fingerprint registration process, right-click the highlighted finger on the screen and then click **Start Over**.

8. Click a different finger on the screen to register, and then repeat steps 6 and 7.

   CAUTION You must register at least 2 fingers in order to complete the setup.

   NOTE If you click **Finish** before registering at least 2 fingers, an error message is displayed. Click **OK** to continue.

9. After you have registered at least 2 fingers, click **Finish**, and then click **OK**.

10. To set up the fingerprint reader for a different Windows user, log on to Windows as that user and then repeat steps 1 through 9.

Step 2: Use your registered fingerprint to log on to Windows

To log on to Windows using your fingerprint:

1. Immediately after you have registered your fingerprints, restart Windows.

2. In the upper-left corner of the screen, click **Log on to Credential Manager**.

3. At the **Credential Manager Logon Wizard** dialog box, instead of clicking a user name, swipe any of your registered fingers to log on to Windows.

4. Enter your Windows password to associate the fingerprint with the password.

NOTE When you log on to Windows the first time using your fingerprint, and you have a Windows password, you must enter the password in order to associate the password with the fingerprint. After the password has been associated with the fingerprint, you will not need to enter the password again when using the fingerprint reader.

Index