

Security

---

User Guide

© Copyright 2007 Hewlett-Packard  
Development Company, L.P.

Windows is a U. S. registered trademark of  
Microsoft Corporation.

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.

Second Edition: March 2007

First Edition: January 2007

Document Part Number: 419701-002

## Product notice

This user guide describes features that are common to most models. Some features may not be available on your computer.



---

# Table of contents

## 1 Protecting the computer

## 2 Using passwords

Setting passwords in Windows .....	3
Setting passwords in Computer Setup .....	4
Setup password .....	5
Managing a setup password .....	5
Entering a setup password .....	5
Power-on password .....	6
Managing a power-on password .....	6
Entering a power-on password .....	7
Requiring a power-on password at restart .....	7
Using Computer Setup DriveLock .....	8
Setting a DriveLock password .....	9
Entering a DriveLock password .....	10
Changing a DriveLock password .....	10
Removing DriveLock protection .....	10

## 3 Using Computer Setup security features

Securing system devices .....	11
Using Computer Setup stringent security .....	11
Setting stringent security .....	12
Removing stringent security .....	12
Viewing Computer Setup System Information .....	13
Using Computer Setup System IDs .....	14

## 4 Using antivirus software

## 5 Using firewall software

## 6 Installing critical security updates

## 7 Using HP ProtectTools Security Manager (select models only)

## 8 Installing a security cable



# 1 Protecting the computer



**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, see the HP Web site at <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 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	<ul style="list-style-type: none"><li>• Power-on authentication using passwords or smart cards</li><li>• HP ProtectTools Security Manager</li></ul>
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	HP ProtectTools Security Manager
Unauthorized access to data	<ul style="list-style-type: none"><li>• Firewall software</li><li>• Windows updates</li><li>• HP ProtectTools Security Manager</li></ul>
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 Using 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 HP ProtectTools Security Manager passwords, can be enabled in Computer Setup to provide BIOS password protection in addition to their normal HP 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 technical support or your authorized service provider for additional information.
- If you forget both the power-on password and the setup password set in Computer Setup, you cannot turn on the computer or exit Hibernation. Call technical support or your authorized service provider for additional information.
- If you forget both the user password and the master DriveLock password set in Computer Setup, the hard drive that is protected by the passwords is permanently locked and can no longer be used.

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.

Use the following 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.

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



# Setting passwords in Windows

Windows passwords	Function
Administrator password*	Protects access to a Windows administrator-level account.
User password*	Protects access to a Windows user account.

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

## Setting passwords in Computer Setup

Computer Setup passwords	Function
Setup password	Protects access to Computer Setup.
Power-on password	Protects access to the computer contents when the computer turns on, restarts, or exits Hibernation.
DriveLock master password	Protects access to the internal hard drive that is protected by DriveLock. It is also used to remove DriveLock protection. This password is set under DriveLock Passwords during the enable process.
DriveLock user password	Protects access to the internal hard drive that is protected by DriveLock, and is set under DriveLock Passwords during the enable process.
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.
TPM embedded security password	When enabled as a BIOS password, protects access to the computer contents when the computer turns on, restarts, or exits Hibernation.  This password requires the optional embedded security chip to support this security feature.

# 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.

Note the following characteristics of the setup password:

- It is not interchangeable with a Windows administrator password, although both passwords can be identical.
- It is not displayed as it is set, entered, changed, or deleted.
- It 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.
- It can include any combination of up to 32 letters and numbers and is not case sensitive.

## Managing a setup password

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

To manage, set, change, or delete this password, follow these steps:

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 a setup 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.

## 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.

Note the following characteristics of a power-on password:

- It is not displayed as it is set, entered, changed, or deleted.
- It 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.
- It can include any combination of up to 32 letters and numbers and is not case sensitive.

## Managing a power-on password

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

To manage, set, change, or delete this password, follow these steps:

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, follow these steps:

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 **Enable** or **Disable** in the **Require password on restart** 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.

## Using 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 be accessed only 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 either 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, follow these steps:

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 you want to protect, 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, follow these steps:

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, follow these steps:

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 Using Computer Setup security features

### Securing system devices

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

To disable or reenable system devices in Computer Setup, follow these steps:

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**. Then press **enter** and use the arrow keys to select the options you want.
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.

### Using 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, follow these steps:

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 **Enable** in 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, follow these steps:

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.

# Viewing 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 batteries.
- Specification information about the processor, cache, memory, ROM, video revision, and keyboard controller revision.

To view this general system information, follow these steps:

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 **File > System Information**, and then press **enter**.



---

**NOTE:** To prevent unauthorized access to this information, you must create a setup password in Computer Setup.

---

# Using 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.

---

To manage this feature, follow these steps:

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 > System IDs**, and then press **enter**.
3. To enter asset tag information, use the arrow keys to highlight the Asset Tracking Number field or the Ownership Tag field, and then enter the information.
4. Press **f10** when finished.
5. 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 Using antivirus software

When you use the computer to access e-mail, a network, or the Internet, 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 be 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 Help and Support.

---

## 5 Using firewall software

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

Firewall features include information on logging and 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 Installing critical security updates



**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.

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 observe these guidelines:

- 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 Help and Support.

---

## 7 Using HP ProtectTools Security Manager (select models only)

Select computer models include HP ProtectTools Security Manager. This software can be accessed through Windows Control Panel. It provides security features that help protect against unauthorized access to the computer, networks, and critical data. For more information, refer to the HP ProtectTools online Help.

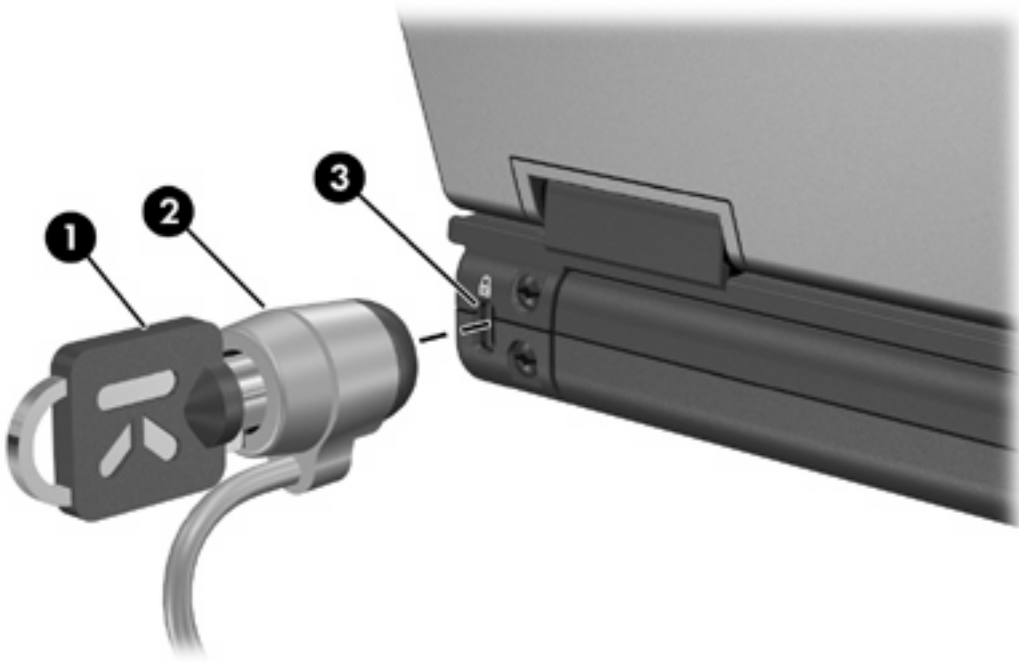


## 8 Installing a security cable



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

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.

---

# Index

## A

administrator password 3  
antivirus software 15

## C

cable, security 19  
Computer Setup  
    device security 11  
    DriveLock password 8  
    power-on password 6  
    setup password 5  
    stringent security 11  
critical updates, software 17

## D

device security 11  
DriveLock password  
    changing 10  
    description 8  
    entering 10  
    removing 10  
    setting 9

## F

firewall software 16

## H

HP ProtectTools Security  
    Manager 18

## P

passwords  
    administrator 3  
    DriveLock 8  
    power-on 6  
    setup 5  
    user 3

## S

security cable 19

security, protecting the  
    computer 1  
software  
    antivirus 15  
    critical updates 17  
    firewall 16  
stringent security 11

## U

user password 3

