



# **Desktop Management Guide**

## Business PCs

Document Part Number: 391759-001

**May 2005**

This guide provides definitions and instructions for using security and Intelligent Manageability features that are preinstalled on some models.

© 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.

---

## **Desktop Management Guide**

Business PCs

First Edition (May 2005)

**Document Part Number: 391759-001**

---

# Contents

## Desktop Management Guide

Initial Configuration and Deployment	2
Altiris Deployment Solution Agent	2
HP Local Recovery	3
Remote System Installation	3
Software Updating and Management	4
HP System Software Manager	4
HP Client Manager Software	5
HP Client Management Solutions using Altiris	5
HP OpenView Management Suite for Desktops Using Radia	7
HP Local Recovery	8
Dantz Retrospect Express	10
Proactive Change Notification	11
Subscriber's Choice	11
Retired Solutions	11
ROM Flash	12
Remote ROM Flash	13
HPQFlash	13
Boot Block Emergency Recovery Mode	13
Replicating the Setup	14
Dual-State Power Button	22
World Wide Web Site	23
Building Blocks and Partners	23
Asset Tracking and Security	24
Password Security	28
Establishing a Setup Password Using Computer Setup	28
Establishing a Power-On Password Using Computer Setup	29
DriveLock	34
Smart Cover Sensor	35
Smart Cover Lock	37

Cable Lock Provision . . . . .	39
Fingerprint Identification Technology . . . . .	39
Fault Notification and Recovery . . . . .	39
Drive Protection System . . . . .	40
Surge-Tolerant Power Supply . . . . .	40
Thermal Sensor . . . . .	40

## **Index**

---

# Desktop Management Guide

HP Client Management Solutions provides standards-based solutions for managing and controlling desktops, workstations, and notebook PCs in a networked environment. HP pioneered desktop manageability in 1995 with the introduction of the industry's first fully manageable desktop personal computers. HP is a patent holder of manageability technology. Since then, HP has led an industry-wide effort to develop the standards and infrastructure required to effectively deploy, configure, and manage desktops, workstations, and notebook PCs. HP works closely with leading management software solution providers in the industry to ensure compatibility between HP Client Management Solutions and these products. HP Client Management Solutions are an important aspect of our broad commitment to providing you with PC Lifecycle Solutions that assist you during the four phases of the desktop PC lifecycle—planning, deployment, management, and transitions.

The key capabilities and features of desktop management are:

- Initial configuration and deployment
- Remote system installation
- Software updating and management
- ROM flash
- Asset tracking and security
- Fault notification and recovery



---

Support for specific features described in this guide may vary by model or software version.

---

## Initial Configuration and Deployment

The computer comes with a preinstalled system software image. After a brief software “unbundling” process, the computer is ready to use.

You may prefer to replace the preinstalled software image with a customized set of system and application software. There are several methods for deploying a customized software image. They include:

- Installing additional software applications after unbundling the preinstalled software image.
- Using software deployment tools, such as Altiris Deployment Solution, to replace the preinstalled software with a customized software image.
- Using a disk cloning process to copy the contents from one hard drive to another.

The best deployment method depends on your information technology environment and processes. The PC Deployment section of the HP Lifecycle Solutions Web site (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>) provides information to help you select the best deployment method.

The *Restore Plus!* CD, ROM-based setup, and ACPI hardware provide further assistance with recovery of system software, configuration management and troubleshooting, and power management.

## Altiris Deployment Solution Agent

This program is pre-loaded on the computer. When installed, it enables communication with the administrator Deployment Solution console.

To install Altiris Deployment Solution Agent:

1. Click **Start**.
2. Click **All Programs**.
3. Click **Software Setup**.
4. Click **Next**.
5. Scroll down and click on the link to install Altiris AClient.

## HP Local Recovery

Local Recovery backs-up data and system files to a protected area on the hard drive. If data or files are lost, deleted, or corrupted, Local Recovery can be used to retrieve data or restore the last good system image.

To install this pre-loaded program:

1. Click **Start**.
2. Click **Local Recovery**.
3. Click **Next**.
4. Scroll down and click on the link to install HP Local Recovery.

## Remote System Installation

Remote System Installation allows you to start and set up the system using the software and configuration information located on a network server by initiating the Preboot Execution Environment (PXE). The Remote System Installation feature is usually used as a system setup and configuration tool, and can be used for the following tasks:

- Formatting a hard drive
- Deploying a software image on one or more new PCs
- Remotely updating the system BIOS in flash ROM (“[Remote ROM Flash](#)” on page 13)
- Configuring the system BIOS settings

To initiate Remote System Installation, press **F12** when the F12 = Network Service Boot message appears in the lower-right corner of the HP logo screen. Follow the instructions on the screen to continue the process. The default boot order is a BIOS configuration setting that can be changed to always attempt to PXE boot.

HP and Altiris have partnered to provide tools designed to make the task of corporate PC deployment and management easier and less time-consuming, ultimately lowering the total cost of ownership and making HP PCs the most manageable client PCs in the enterprise environment.

## Software Updating and Management

HP provides several tools for managing and updating software on desktops, workstations, and notebooks:

- HP System Software Manager
- HP Client Manager Software
- HP Client Management Solutions using Altiris
- HP OpenView Management Suite for Desktops using Radia
- HP Local Recovery
- Dantz Backup and Recovery
- HP Proactive Change Notification
- HP Subscriber's Choice

### HP System Software Manager

HP System Software Manager (SSM) is a free utility that automates remote deployment of device drivers and BIOS updates for your networked HP business PCs. When SSM runs, it silently (without user interaction) determines the revision levels of drivers and BIOS installed on each networked client system and compares this inventory against system software SoftPaqs that have been tested and stored in a central file store. SSM then automatically updates any down-revision system software on the networked PCs to the later levels available in the file store. Since SSM only allows distribution of SoftPaq updates to the correct client system models, administrators can confidently and efficiently use SSM to keep system software updated.

System Software Manager integrates with enterprise software distribution tools such as HP OpenView Management Suite using Radia and Microsoft Systems Management Server (SMS). Using SSM, you can distribute customer-created or third-party updates that have been packaged in the SSM-format.

SSM may be downloaded at no charge by visiting [www.hp.com/go/ssm](http://www.hp.com/go/ssm).



## HP Client Manager Software

HP Client Manager Software developed with Altiris, is available free for all supported HP business desktop, notebook, and workstation models. SSM is integrated into HP Client Manager, and enables central tracking, monitoring, and management of the hardware aspects of HP client systems.

Use HP Client Manager to:

- Get valuable hardware information such as CPU, memory, video, and security settings
- Monitor system health to fix problems before they occur
- Install drivers and BIOS updates without visiting each PC
- Remotely configure BIOS and security settings
- Automate processes to quickly resolve hardware problems

HP Client Manager uses the same Altiris infrastructure as the other Altiris client lifecycle management solutions. This design provides a significant benefit for the IT staff, since only one infrastructure needs to be setup and maintained. Since information is stored in one database, you get complete and consistent inventory reports as well as system health and security information. You use a single, consistent console interface for scheduling and tracking progress of both hardware and software management tasks for your client systems.

For more information on HP Client Manager, visit [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## HP Client Management Solutions using Altiris

Additional Altiris client management solutions can be purchased through HP that complement the hardware management capabilities of HP Client Manager. These Altiris solutions address client IT lifecycle challenges including:

- Inventory assessment
- Software license compliance
- Personality migration
- Software image deployment

- Software distribution
- Asset management
- Client backup and recovery
- Problem resolution

For more information on HP Client Management Solutions using Altiris, visit [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

HP and Altiris have a unique alliance that extends beyond sales and marketing to include joint development and technology sharing that spans HP Client, Server, OpenView, and Services groups to provide best-of-breed solutions for HP partners and customers.

Starting in 1999, Compaq personal systems group and Altiris entered into an alliance to combine the strength of Compaq as a pioneer in PC hardware and manageability with the strength of Altiris' PC deployment and migration capabilities. The relationship expanded into a strategic alliance with the introduction of comprehensive cost-reducing IT lifecycle management solutions including the jointly developed HP Client Manager Software, which provides best-of-breed hardware management for HP PCs.

Building upon the success of the personal systems group, in 2001 the industry standard servers group introduced the ProLiant Essentials Rapid Deployment Pack, an OEM version of Altiris Deployment Solution combined with HP's SmartStart Toolkit. HP utilizes this solution for provisioning ProLiant servers (including blade servers) as well as Blade PCs, a core component of HP's Consolidated Client Infrastructure.

Following the HP and Compaq merger, the alliance has continued to expand with the following offerings:

- Altiris Deployment Solution is available for a free 30-day trial for HP business PCs, after which a license may be purchased.
- HP Local Recovery, a client backup/recovery utility, is available for free with HP business PCs.
- Altiris Connector for HP OpenView provides client inventory and event integration with HP OpenView Network Node Manager, Operations, and Service Desk.

- Altiris Connector for HP Systems Insight Manager enables consolidated deployment and management of HP clients and servers from the HP Systems Insight Manager console.

HP leads the market by offering a single management solution and console for deploying and configuring PCs, handhelds, thin clients, and Windows and Linux servers plus rich integration with HP enterprise management tools. HP offers extensive training and services expertise available from the HP Services organization and Altiris. This combination of HP Client Management Solutions and services capability provides the best choice for customers trying to reduce the cost and complexity of managing client systems.

## **HP OpenView Management Suite for Desktops Using Radia**

HP OpenView Management Suite for Desktops using Radia is highly scalable, policy-based change and configuration management software that enables administrators to efficiently and reliably inventory, deploy, and maintain software and content across heterogeneous desktop platforms from a web-based console.

HP OpenView Management Suite for Desktops using Radia ensures availability of desktop applications and that the operating systems, applications, and content that employees, partners, or customers need are 100% right, all the time.

HP OpenView Management Suite for Desktops using Radia is proven by enterprise customers around the world to deliver greater than 99% deployment reliability in highly complex and large-scale IT environments. It automates change management, resulting in dramatic IT cost savings, accelerated time-to-market for software and content, and increased user productivity and satisfaction.

HP OpenView Management Suite for Desktops using Radia enables IT professionals to:

- Collect hardware and software inventory across multiple platforms
- Prepare an application package and conduct impact analysis prior to distribution

- Target individual desktops, workgroups, or entire populations of desktops for deployment and maintenance of software and content according to policies
- Provision and manage operating systems, applications, and content on distributed desktop computers from any location
- Integrate with HP OpenView Service Desk and other help desk and system management tools
- Leverage a common infrastructure for management of software and content on virtually any device, any platform, and any network for all enterprise users
- Scale to meet enterprise needs

HP OpenView Management Suite for Desktops using Radia is offered as a stand-alone solution and is also fully integrated with other HP OpenView Management Suite using Radia products as an essential component of HP's unique desired-state management approach, which provides automated and ongoing maintenance of all software residing on enterprise computing devices. The HP OpenView Management Suite using Radia products ensure that the entire software infrastructure is always in its desired state—up-to-date, reliable, and secure.

For more information on HP OpenView Management Suite for Desktops using Radia, visit [http://managementsoftware.hp.com/products/radia\\_mdsk/index.html](http://managementsoftware.hp.com/products/radia_mdsk/index.html).

## HP Local Recovery

Local Recovery provides data and system file protection for HP business desktops, notebooks, and workstations. With Local Recovery, you can quickly recover and get back to work when information is accidentally deleted or your operating system is corrupted. Designed for disconnected or seldom-connected users, Local Recovery protects your HP computer's data and system state through scheduled snapshots stored in a protected area on the local hard disk. You can initiate a backup or restore by simply clicking your mouse or pressing the F11 key in a pre-boot environment. System backup and disaster recovery is now easy for all users regardless of connectivity.

Local Recovery is available for free with HP business PCs. Two additional client recovery products are also available. Upgrading to these products provides you with additional recovery features:

- **Local Recovery Pro**—Provides all the capabilities of Local Recovery plus support for backup and recovery to a secondary hard drive and for open and locked files. During a backup snapshot, open/locked file support preserves information in open applications such as E-mail messages, presentations, and word processing documents.
- **Recovery Solution**—Provides complete enterprise-level backup and recovery of PC's from a central administrative console. The solution supports data backup to a protected area on the local hard disk drive as well as to a network storage area. This network-based recovery feature provides a high level of protection against data lost due to hard drive failure or stolen and misplaced PCs.

For more information on HP Local Recovery, visit [www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy).

## Dantz Retrospect Express

Dantz Retrospect Express protects a single Windows desktop or notebook computer. Retrospect Express allows recovery from data loss due to viruses, newly installed software, user error, damaged hardware, hardware upgrades, hackers, and lost or stolen computers. It offers a choice between simple duplicates or comprehensive backups and an intuitive setup wizard to get you up and running in minutes. Retrospect Express comes with Disaster Recovery built into the product for the best protection available. [Click here to view a list of hardware manufacturers who bundle Retrospect with their products and to learn where to buy these products.](#)

Install Retrospect Express and perform your first backup in less than two minutes. With Retrospect, you can implement a backup plan by answering a few simple questions. Restores are quick and painless. When you need to perform a restore, Retrospect Express automatically locates files even if you do not know which piece of backup media contains the files.

Duplicate Files and Folders to an External Hard Drive with the Push of a Button. The duplicate operation copies information from the computer's hard drive to the external hard drive. (For external hard drives with a built-in backup button, duplicates can be initiated simply by pressing the button.) With duplicates, the files and folders on the external hard drive can be easily viewed, manipulated, and restored by using Windows Explorer. The duplication process saves space by overwriting any previous backup data on the external drive and saves time by copying only files that are new or that have changed since the last backup.

Back Up Multiple Versions of Files and Folders. Comprehensive backups retain prior versions of files and folders and allow you to roll back a computer to any prior point in time before a data-corrupting event occurred. Each time a backup operation is performed, Retrospect Express creates a restore point, which can contain all the information a user needs to retrieve files or restore an entire computer (disaster recovery)—including all operating system files and settings, device drivers, and applications and their settings. Restore points are captured quickly and they provide 100% accurate restores to any point in time that a backup was performed—exceeding the capability of other backup software.

For more information on Dantz Retrospect Express, visit [http://www.dantz.com/en/products/win\\_express/index.shtml](http://www.dantz.com/en/products/win_express/index.shtml).

## Proactive Change Notification

The Proactive Change Notification program uses the Subscriber's Choice Web site in order to proactively and automatically:

- Send you Proactive Change Notification (PCN) E-mails informing you of hardware and software changes to most commercial computers and servers, up to 60 days in advance
- Send you E-mail containing Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins, and Driver alerts for most commercial computers and servers

You create your own profile to ensure that you only receive the information relevant to a specific IT environment. To learn more about the Proactive Change Notification program and create a custom profile, visit <http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

## Subscriber's Choice

Subscriber's Choice is a client-based service from HP. Based on your profile, HP will supply you with personalized product tips, feature articles, and/or driver and support alerts/notifications. Subscriber's Choice Driver and Support Alerts/Notifications will deliver E-mails notifying you that the information you subscribed to in your profile is available for review and retrieval. To learn more about Subscriber's Choice and create a custom profile, visit <http://h30046.www3.hp.com/subhub.php>.

## Retired Solutions

The Desktop Management Task Force (DMTF) introduced the Desktop Management Interface (DMI) standard almost ten years ago. Due to new standards adoption such as the Common Information Model (CIM), the DMTF has initiated end-of-life for DMI. Given other advancements in HP Client Management Solutions, HP Systems Insight Manager, and Microsoft's implementation of CIM, known as Windows Management Instrumentation (WMI), the HP

Insight Management Agent is no longer being provided on new HP commercial desktop, workstation, and notebook models introduced after January 1, 2004.

The Insight Management (IM) Agent provided the following features:

- DMI support allowed a client system to be managed by Insight Manager 7 or other DMI-compliant management applications.
- A Web agent allowed the system to be managed both locally and remotely by a web browser.
- Health alerting could notify the user locally or be sent to a central console.

Insight Manager has been replaced by HP Systems Insight Manager Software (HP SIM). HP SIM uses WMI to retrieve client system information. The Altiris Connector for HP Systems Insight Manager is available and enables the HP Client Management Solutions through the HP SIM console.

While local alerting is currently not supported with HP Client Management Solutions, health alerts are reported to a system management console. Microsoft WMI is standard with Windows 2000 and Windows XP. WMI provides hardware inventory and alert information directly through the Windows OS to a system management application.

## ROM Flash

The computer's BIOS is stored in a programmable flash ROM (read only memory). By establishing a setup password in the Computer Setup (F10) Utility, you can protect the ROM from being unintentionally updated or overwritten. This is important to ensure the operating integrity of the computer. Should you need or want to upgrade the BIOS, you may download the latest BIOS images from the HP driver and support page, <http://www.hp.com/support/files>.



**CAUTION:** For maximum ROM protection, be sure to establish a setup password. The setup password prevents unauthorized ROM upgrades. System Software Manager allows the system administrator to set the setup password on one or more PCs simultaneously. For more information, visit <http://www.hp.com/go/ssm>.

---



## Remote ROM Flash

Remote ROM Flash allows the system administrator to safely upgrade the BIOS on remote HP computers directly from the centralized network management console. Enabling the system administrator to perform this task remotely on multiple computers results in a consistent deployment of, and greater control over, HP PC BIOS images over the network. It also results in greater productivity and lower total cost of ownership.



---

The computer must be powered on, or turned on through Remote Wakeup, to take advantage of Remote ROM Flash.

---

For more information on Remote ROM Flash, refer to the HP Client Manager Software or System Software Manager at <http://h18000.www1.hp.com/im/prodinfo.html>.

## HPQFlash

The HPQFlash utility is used to locally update or restore the system BIOS of individual PCs from a Windows operating system.

For more information on HPQFlash, visit <http://www.hp.com/support/files> and enter the model number of the computer when prompted.

## Boot Block Emergency Recovery Mode

Boot Block Emergency Recovery Mode permits system recovery in the unlikely event of a ROM flash failure. For example, if a power failure were to occur during a BIOS upgrade, the ROM flash would be incomplete. This would render the system BIOS unusable. The Boot Block is a flash-protected section of the ROM that contains code that checks for a valid system BIOS image when the system is turned on.

- If the system BIOS image is valid, the system starts normally.
- If the system BIOS image is not valid, a failsafe Boot Block BIOS provides enough support to

- ❑ search removable media for BIOS image files. If an appropriate BIOS image file is found, it is automatically flashed into the ROM.
- ❑ start the system from bootable removable media that automatically invokes system BIOS upgrade utilities.

When an invalid system BIOS image is detected, the system power LED will blink red 8 times, one blink every second. Simultaneously, the speaker will beep 8 times. If the portion of the system ROM containing the video option ROM image is not corrupt, "Boot Block Emergency Recovery Mode" will be displayed on the screen.

To recover the system after it enters Boot Block Emergency Recovery Mode, complete the following steps:

1. Turn off the power.
2. Insert a diskette, CD, or USB flash device containing the desired BIOS image file in the root directory. Note: The media must be formatted using the FAT12, FAT16, or FAT32 file system.
3. Turn on the computer.

If no appropriate BIOS image file is found, the failsafe Boot Block BIOS will attempt to start the system from a bootable device. If no bootable device is found, you will be prompted to insert media containing a BIOS image file or BIOS upgrade utility.

If the system successfully reprograms the ROM, the system will automatically power off.

4. Remove the removable media used to upgrade the BIOS.
5. Turn the power on to restart the computer.

## Replicating the Setup

The following procedures give an administrator the ability to easily copy one setup configuration to other computers of the same model. This allows for faster, more consistent configuration of multiple computers.



Both procedures require a diskette drive or a supported USB flash media device, such as an HP Drive Key.

---

## Copying to Single Computer



**CAUTION:** A setup configuration is model-specific. File system corruption may result if source and target computers are not the same model. For example, do not copy the setup configuration from a dc7xxx PC to a dx7xxx PC.

---

1. Select a setup configuration to copy. Turn off the computer. If you are in Windows, click **Start > Shut Down > Shut Down**.
  2. If you are using a USB flash media device, insert it now.
  3. Turn on the computer.
  4. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
- 



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

5. If you are using a diskette, insert it now.
6. Click **File > Replicated Setup > Save to Removable Media**. Follow the instructions on the screen to create the configuration diskette or USB flash media device.
7. Turn off the computer to be configured and insert the configuration diskette or USB flash media device.
8. Turn on the computer to be configured.
9. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
10. Click **File > Replicated Setup > Restore from Removable Media**, and follow the instructions on the screen.
11. Restart the computer when the configuration is complete.

## Copying to Multiple Computers

---



**CAUTION:** A setup configuration is model-specific. File system corruption may result if source and target computers are not the same model. For example, do not copy the setup configuration from a dc7xxx PC to a dx7xxx PC.

---

This method takes a little longer to prepare the configuration diskette or USB flash media device, but copying the configuration to target computers is significantly faster.

---



A bootable diskette is required for this procedure or to create a bootable USB flash media device. If Windows XP is not available to use to create a bootable diskette, use the method for copying to a single computer instead (see [“Copying to Single Computer” on page 15](#)).

---

1. Create a bootable diskette or USB flash media device. See [“Supported USB Flash Media Device” on page 17](#) or [“Unsupported USB Flash Media Device” on page 19](#).
- 



**CAUTION:** Not all computers can be booted from a USB flash media device. If the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive, the computer can be booted from a USB flash media device. Otherwise, a bootable diskette must be used.

---

2. Select a setup configuration to copy. Turn off the computer. If you are in Windows, click **Start > Shut Down > Shut Down**.
  3. If you are using a USB flash media device, insert it now.
  4. Turn on the computer.
  5. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
- 



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

6. If you are using a diskette, insert it now.

7. Click **File > Replicated Setup > Save to Removable Media**. Follow the instructions on the screen to create the configuration diskette or USB flash media device.
8. Download a BIOS utility for replicating setup (repset.exe) and copy it onto the configuration diskette or USB flash media device. To obtain this utility, go to [tap://welcome.hp.com/support/files](http://welcome.hp.com/support/files) and enter the model number of the computer.
9. On the configuration diskette or USB flash media device, create an autoexec.bat file containing the following command:  
**repset.exe**
10. Turn off the computer to be configured. Insert the configuration diskette or USB flash media device and turn the computer on. The configuration utility will run automatically.
11. Restart the computer when the configuration is complete.

## Creating a Bootable Device

### Supported USB Flash Media Device

Supported devices have a preinstalled image to simplify the process of making them bootable. All HP or Compaq and most other USB flash media devices have this preinstalled image. If the USB flash media device being used does not have this image, use the procedure later in this section (see “[Unsupported USB Flash Media Device](#)” on page 19).

To create a bootable USB flash media device, you must have:

- a supported USB flash media device
- a bootable DOS diskette with the FDISK and SYS programs (If SYS is not available, FORMAT may be used, but all existing files on the USB flash media device will be lost.)
- a PC that is bootable from a USB flash media device



**CAUTION:** Some older PCs may not be bootable from a USB flash media device. If the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive, the computer can be booted from a USB flash media device. Otherwise, a bootable diskette must be used.

---

1. Turn off the computer.

2. Insert the USB flash media device into one of the computer's USB ports and remove all other USB storage devices except USB diskette drives.
3. Insert a bootable DOS diskette with FDISK.COM and either SYS.COM or FORMAT.COM into a diskette drive and turn on the computer to boot to the DOS diskette.
4. Run FDISK from the A:\ prompt by typing **FDISK** and pressing Enter. If prompted, click **Yes (Y)** to enable large disk support.
5. Enter Choice [**5**] to display the drives in the system. The USB flash media device will be the drive that closely matches the size of one of the drives listed. It will usually be the last drive in the list. Note the letter of the drive.

USB flash media device drive: \_\_\_\_\_



---

**CAUTION:** If a drive does not match the USB flash media device, do not proceed. Data loss can occur. Check all USB ports for additional storage devices. If any are found, remove them, reboot the computer, and proceed from step 4. If none are found, either the system does not support the USB flash media device or the USB flash media device is defective. **DO NOT** proceed in attempting to make the USB flash media device bootable.

---

6. Exit FDISK by pressing the **Esc** key to return to the A:\ prompt.
7. If your bootable DOS diskette contains SYS.COM, go to step 8. Otherwise, go to step 9.
8. At the A:\ prompt, enter **SYS x:** where x represents the drive letter noted above.



---

**CAUTION:** Be sure that you have entered the correct drive letter for the USB flash media device.

---

After the system files have been transferred, SYS will return to the A:\ prompt. Go to step 13.

9. Copy any files you want to keep from your USB flash media device to a temporary directory on another drive (for example, the system's internal hard drive).
10. At the A:\ prompt, enter **FORMAT /S X:** where X represents the drive letter noted before.



**CAUTION:** Be sure that you have entered the correct drive letter for the USB flash media device.

---

FORMAT will display one or more warnings and ask you each time whether you want to proceed. Enter **Y** each time. FORMAT will format the USB flash media device, add the system files, and ask for a Volume Label.

11. Press **Enter** for no label or enter one if desired.
  12. Copy any files you saved in step 9 back to your USB flash media device.
  13. Remove the diskette and reboot the computer. The computer will boot to the USB flash media device as drive C.
- 



The default boot order varies from computer to computer, and it can be changed in the Computer Setup (F10) Utility.

If you have used a DOS version from Windows 9x, you may see a brief Windows logo screen. If you do not want this screen, add a zero-length file named LOGO.SYS to the root directory of the USB flash media device.

---

Return to [“Copying to Multiple Computers” on page 16.](#)

## Unsupported USB Flash Media Device

To create a bootable USB flash media device, you must have:

- a USB flash media device
  - a bootable DOS diskette with the FDISK and SYS programs (If SYS is not available, FORMAT may be used, but all existing files on the USB flash media device will be lost.)
  - a PC that is bootable from a USB flash media device
- 



**CAUTION:** Some older PCs may not be bootable from a USB flash media device. If the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive, the computer can be booted from a USB flash media device. Otherwise, a bootable diskette must be used.

---

1. If there are any PCI cards in the system that have SCSI, ATA RAID or SATA drives attached, turn off the computer and unplug the power cord.



---

**CAUTION:** The power cord **MUST** be unplugged.

---

2. Open the computer and remove the PCI cards.
3. Insert the USB flash media device into one of the computer's USB ports and remove all other USB storage devices except USB diskette drives. Close the computer cover.
4. Plug in the power cord and turn on the computer.
5. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



---

If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

6. Go to **Advanced > PCI Devices** to disable both the PATA and SATA controllers. When disabling the SATA controller, note the IRQ to which the controller is assigned. You will need to reassign the IRQ later. Exit setup, confirming the changes.

SATA IRQ: \_\_\_\_\_

7. Insert a bootable DOS diskette with FDISK.COM and either SYS.COM or FORMAT.COM into a diskette drive and turn on the computer to boot to the DOS diskette.
8. Run FDISK and delete any existing partitions on the USB flash media device. Create a new partition and mark it active. Exit FDISK by pressing the **Esc** key.
9. If the system did not automatically restart when exiting FDISK, press **Ctrl+Alt+Del** to reboot to the DOS diskette.
10. At the A:\ prompt, type **FORMAT C: /S** and press **Enter**. Format will format the USB flash media device, add the system files, and ask for a Volume Label.
11. Press **Enter** for no label or enter one if desired.



12. Turn off the computer and unplug the power cord. Open the computer and re-install any PCI cards that were previously removed. Close the computer cover.
13. Plug in the power cord, remove the diskette, and turn on the computer.
14. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
15. Go to **Advanced > PCI Devices** and re-enable the PATA and SATA controllers that were disabled in step 6. Put the SATA controller on its original IRQ.
16. Save the changes and exit. The computer will boot to the USB flash media device as drive C.



The default boot order varies from computer to computer, and it can be changed in the Computer Setup (F10) Utility. Refer to the *Computer Setup Guide* on the *Documentation and Diagnostics CD* for instructions.

If you have used a DOS version from Windows 9x, you may see a brief Windows logo screen. If you do not want this screen, add a zero-length file named LOGO.SYS to the root directory of the USB flash media device.

---

Return to [“Copying to Multiple Computers”](#) on page 16.

## Dual-State Power Button

With Advanced Configuration and Power Interface (ACPI) enabled, the power button can function either as an on/off switch or as a standby button. The stand-by feature does not completely turn off power, but instead causes the computer to enter a low-power standby state. This allows you to power down quickly without closing applications and to return quickly to the same operational state without any data loss.

To change the power button's configuration, complete the following steps:

1. Left click on the **Start Button**, then select **Control Panel > Power Options**.
2. In the **Power Options Properties**, select the **Advanced** tab.
3. In the **Power Button** section, select **Stand by**.

After configuring the power button to function as a standby button, press the power button to put the system in a very low power state (standby). Press the button again to quickly bring the system out of standby to full power status. To completely turn off all power to the system, press and hold the power button for four seconds.



**CAUTION:** Do not use the power button to turn off the computer unless the system is not responding; turning off the power without operating system interaction could cause damage to or loss of data on the hard drive.

---

## World Wide Web Site

HP engineers rigorously test and debug software developed by HP and third-party suppliers, and develop operating system specific support software, to ensure performance, compatibility, and reliability for HP computers.

When making the transition to new or revised operating systems, it is important to implement the support software designed for that operating system. If you plan to run a version of Microsoft Windows that is different from the version included with the computer, you must install corresponding device drivers and utilities to ensure that all features are supported and functioning properly.

HP has made the task of locating, accessing, evaluating, and installing the latest support software easier. You can download the software from <http://www.hp.com/support>.

The Web site contains the latest device drivers, utilities, and flashable ROM images needed to run the latest Microsoft Windows operating system on the HP computer.

## Building Blocks and Partners

HP management solutions integrate with other systems management applications, and are based on industry standards, such as:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LAN Technology
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) support

## Asset Tracking and Security

Asset tracking features incorporated into the computer provide key asset tracking data that can be managed using HP Systems Insight Manager, HP Client Manager or other system management applications. Seamless, automatic integration between asset tracking features and these products enables you to choose the management tool that is best suited to the environment and to leverage the investment in existing tools.

HP also offers several solutions for controlling access to valuable components and information. HP Embedded Security for ProtectTools, if installed, prevents unauthorized access to data and checks system integrity and authenticates third-party users attempting system access. (For more information, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com).) Security features such as HP Embedded Security for ProtectTools, the Smart Cover Sensor and the Smart Cover Lock, available on some models, help to prevent unauthorized access to the internal components of the personal computer. By disabling parallel, serial, or USB ports, or by disabling removable media boot capability, you can protect valuable data assets. Memory Change and Smart Cover Sensor alerts can be automatically forwarded to system management applications to deliver proactive notification of tampering with a computer's internal components.



HP Embedded Security for ProtectTools, the Smart Cover Sensor, and the Smart Cover Lock are available as options on some systems.




---

Use the following utilities to manage security settings on the HP computer:

- Locally, using the Computer Setup Utilities. See the *Computer Setup (F10) Utility Guide* on the *Documentation and Diagnostics* CD included with the computer for additional information and instructions on using the Computer Setup Utilities.
- Remotely, using HP Client Manager Software or System Software Manager. This software enables the secure, consistent deployment and control of security settings from a simple command-line utility.

The following table and sections refer to managing security features of the computer locally through the Computer Setup (F10) Utilities.


## Security Features Overview

Option	Description
Setup Password	<p>Allows you to set and enable setup (administrator) password.</p> <p> If the setup password is set, it is required to change Computer Setup options, flash the ROM, and make changes to certain plug and play settings under Windows.</p> <p>See the <i>Troubleshooting Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p>
Power-On Password	<p>Allows you to set and enable power-on password.</p> <p>See the <i>Troubleshooting Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p>
Password Options (This selection will appear only if a power-on password is set.)	<p>Allows you to specify whether the password is required for warm boot (<b>CTRL+ALT+DEL</b>).</p> <p>See the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p>
Pre-Boot Authorization	<p>Allows you to enable/disable the Smart Card to be used in place of the Power-On Password.</p>
Smart Cover	<p>Allows you to:</p> <ul style="list-style-type: none"> <li>• Enable/disable the Cover Lock.</li> <li>• Enable/disable the Cover Removal Sensor.</li> </ul> <p> <i>Notify User</i> alerts the user that the sensor has detected that the cover has been removed. <i>Setup Password</i> requires that the setup password be entered to boot the computer if the sensor detects that the cover has been removed.</p> <p>This feature is supported on some models only. See the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p>
	<p>For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD.</p> <p>Support for security features may vary depending on the specific computer configuration.</p>

---

## Security Features Overview *(Continued)*

---



Option	Description
Embedded Security	Allows you to: <ul style="list-style-type: none"><li data-bbox="576 352 1136 378">• Enable/disable the Embedded Security device.</li><li data-bbox="576 395 1001 421">• Reset the device to Factory Settings.</li></ul> This feature is supported on some models only. See the <i>HP ProtectTools Security Manager Guide</i> at <a href="http://www.hp.com">www.hp.com</a> for more information.
Device Security	Enables/disables serial ports, parallel port, front USB ports, system audio, network controllers (some models), MultiBay devices (some models), and SCSI controllers (some models).
	For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics CD</i> . Support for security features may vary depending on the specific computer configuration.

---

---

**Security Features Overview** *(Continued)*


---

Option	Description
Network Service Boot	Enables/disables the computer's ability to boot from an operating system installed on a network server. (Feature available on NIC models only; the network controller must reside on the PCI bus or be embedded on the system board.)
System IDs	<p>Allows you to set:</p> <ul style="list-style-type: none"> <li>• Asset tag (18-byte identifier) and ownership Tag (80-byte identifier displayed during POST).</li> </ul> <p>See the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p> <ul style="list-style-type: none"> <li>• Chassis serial number or Universal Unique Identifier (UUID) number. The UUID can only be updated if the current chassis serial number is invalid. (These ID numbers are normally set in the factory and are used to uniquely identify the system.)</li> </ul> <p>Keyboard locale setting (for example, English or German) for System ID entry.</p>
DriveLock (some models)	<p>Allows you to assign or modify a master or user password for ATA hard drives. When this feature is enabled, the user is prompted to provide one of the DriveLock passwords during POST. If neither is successfully entered, the hard drive will remain inaccessible until one of the passwords is successfully provided during a subsequent cold-boot sequence.</p> <p> This selection will only appear when at least one ATA drive that supports the ATA Security command set is attached to the system.</p> <p>See the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD for more information.</p>
	<p>For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation and Diagnostics</i> CD.</p> <p>Support for security features may vary depending on the specific computer configuration.</p>

---

## Password Security

The power-on password prevents unauthorized use of the computer by requiring entry of a password to access applications or data each time the computer is turned on or restarted. The setup password specifically prevents unauthorized access to Computer Setup, and can also be used as an override to the power-on password. That is, when prompted for the power-on password, entering the setup password instead will allow access to the computer.

A network-wide setup password can be established to enable the system administrator to log in to all network systems to perform maintenance without having to know the power-on password, even if one has been established.

## Establishing a Setup Password Using Computer Setup

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com). Establishing a setup password through Computer Setup prevents reconsideration of the computer (use of the Computer Setup (F10) utility) until the password is entered.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. Select **Security**, then select **Setup Password** and follow the instructions on the screen.
4. Before exiting, click **File > Save Changes and Exit**.



## Establishing a Power-On Password Using Computer Setup

Establishing a power-on password through Computer Setup prevents access to the computer when power is turned on, unless the password is entered. When a power-on password is set, Computer Setup presents Password Options under the Security menu. Password options include Password Prompt on Warm Boot. When Password Prompt on Warm Boot is enabled, the password must also be entered each time the computer is rebooted.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. Select **Security**, then **Power-On Password** and follow the instructions on the screen.
4. Before exiting, click **File > Save Changes and Exit**.

## Entering a Power-On Password

To enter a power-on password, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer**.
2. When the key icon appears on the monitor, type the current password, then press **Enter**.



Type carefully; for security reasons, the characters you type do not appear on the screen.

---

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

## Entering a Setup Password

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com).

If a setup password has been established on the computer, you will be prompted to enter it each time you run Computer Setup.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. When the key icon appears on the monitor, type the setup password, then press **Enter**.



Type carefully; for security reasons, the characters you type do not appear on the screen.

---

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

## Changing a Power-On or Setup Password

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com).

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer**.
2. To change the Power-On password, go to step 3.

To change the Setup password, as soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. When the key icon appears, type the current password, a slash (/) or alternate delimiter character, the new password, another slash (/) or alternate delimiter character, and the new password again as shown:

**current password/new password/new password**

---



Type carefully; for security reasons, the characters you type do not appear on the screen.

---

4. Press **Enter**.

The new password takes effect the next time you turn on the computer.

---



Refer to the “[National Keyboard Delimiter Characters](#)” on page 33 for information about the alternate delimiter characters. The power-on password and setup password may also be changed using the Security options in Computer Setup.

---

## Deleting a Power-On or Setup Password

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com).

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer**.
2. To delete the Power-On password, go to step 3.

To delete the Setup password, as soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. When the key icon appears, type the current password followed by a slash (/) or alternate delimiter character as shown:  
**current password/**
  4. Press **Enter**.
- 



Refer to “[National Keyboard Delimiter Characters](#)” for information about the alternate delimiter characters. The power-on password and setup password may also be changed using the Security options in Computer Setup.

---

## National Keyboard Delimiter Characters

Each keyboard is designed to meet country-specific requirements. The syntax and keys that you use to change or delete the password depend on the keyboard that came with the computer.

### National Keyboard Delimiter Characters

Arabic	/	Greek	-	Russian	/
Belgian	=	Hebrew	.	Slovakian	-
BHCSY*	-	Hungarian	-	Spanish	-
Brazilian	/	Italian	-	Swedish/Finnish	/
Chinese	/	Japanese	/	Swiss	-
Czech	-	Korean	/	Taiwanese	/
Danish	-	Latin American	-	Thai	/
French	!	Norwegian	-	Turkish	.
French Canadian	é	Polish	-	U.K. English	/
German	-	Portuguese	-	U.S. English	/

\* For Bosnia-Herzegovina, Croatia, Slovenia, and Yugoslavia

## Clearing Passwords

If you forget the password, you cannot access the computer. Refer to the *Troubleshooting Guide* on the *Documentation and Diagnostics* CD for instructions on clearing passwords.

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at [www.hp.com](http://www.hp.com).

## DriveLock

DriveLock is an industry-standard security feature that prevents unauthorized access to the data on ATA hard. DriveLock has been implemented as an extension to Computer Setup. It is only available when hard drives that support the ATA Security command set are detected. DriveLock is intended for HP customers for whom data security is the paramount concern. For such customers, the cost of the hard drive and the loss of the data stored on it is inconsequential when compared with the damage that could result from unauthorized access to its contents. In order to balance this level of security with the practical need to accommodate a forgotten password, the HP implementation of DriveLock employs a two-password security scheme. One password is intended to be set and used by a system administrator while the other is typically set and used by the end-user. There is no "back-door" that can be used to unlock the drive if both passwords are lost. Therefore, DriveLock is most safely used when the data contained on the hard drive is replicated on a corporate information system or is regularly backed up. In the event that both DriveLock passwords are lost, the hard drive is rendered unusable. For users who do not fit the previously defined customer profile, this may be an unacceptable risk. For users who do fit the customer profile, it may be a tolerable risk given the nature of the data stored on the hard drive.

## Using DriveLock

The DriveLock option appears under the Security menu in Computer Setup. The user is presented with options to set the master password or to enable DriveLock. A user password must be provided in order to enable DriveLock. Since the initial configuration of DriveLock is typically performed by a system administrator, a master password should be set first. HP encourages system administrators to set a master password whether they plan to enable DriveLock or keep it disabled. This will give the administrator the ability to modify DriveLock settings if the drive is locked in the future. Once the master password is set, the system administrator may enable DriveLock or choose to keep it disabled.

If a locked hard drive is present, POST will require a password to unlock the device. If a power-on password is set and it matches the device's user password, POST will not prompt the user to re-enter the password. Otherwise, the user will be prompted to enter a DriveLock

password. Either the master or the user password may be used. Users will have two attempts to enter a correct password. If neither attempt succeeds, POST will continue but the drive will remain inaccessible.

## **DriveLock Applications**

The most practical use of the DriveLock security feature is in a corporate environment. The system administrator would be responsible for configuring the hard drive which would involve, among other things, setting the DriveLock master password. In the event that the user forgets the user password or the equipment is passed on to another employee, the master password can always be used to reset the user password and regain access to the hard drive.

HP recommends that corporate system administrators who choose to enable DriveLock also establish a corporate policy for setting and maintaining master passwords. This should be done to prevent a situation where an employee intentionally or unintentionally sets both DriveLock passwords before leaving the company. In such a scenario, the hard drive would be rendered unusable and require replacement. Likewise, by not setting a master password, system administrators may find themselves locked out of a hard drive and unable to perform routine checks for unauthorized software, other asset control functions, and support.

For users with less stringent security requirements, HP does not recommend enabling DriveLock. Users in this category include personal users or users who do not maintain sensitive data on their hard drives as a common practice. For these users, the potential loss of a hard drive resulting from forgetting both passwords is much greater than the value of the data DriveLock has been designed to protect. Access to Computer Setup and DriveLock can be restricted through the Setup password. By specifying a Setup password and not giving it to end users, system administrators are able to restrict users from enabling DriveLock.

## **Smart Cover Sensor**

CoverRemoval Sensor, available on some models, is a combination of hardware and software technology that can alert you when the computer cover or side panel has been removed. There are three levels of protection, as described in the following table.


---

## Smart Cover Sensor Protection Levels

---

Level	Setting	Description
Level 0	Disabled	Smart Cover Sensor is disabled (default).
Level 1	Notify User	When the computer is restarted, the screen displays a message indicating that the computer cover or side panel has been removed.
Level 2	Setup Password	When the computer is restarted, the screen displays a message indicating that the computer cover or side panel has been removed. You must enter the setup password to continue.

---

 These settings can be changed using Computer Setup. For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide* on the *Documentation and Diagnostics* CD.

---

## Setting the Smart Cover Sensor Protection Level

To set the Smart Cover Sensor protection level, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. Select **Security > Smart Cover > Cover Removal Sensor**, and select the desired security level.
4. Before exiting, click **File > Save Changes and Exit**.



## Smart Cover Lock

The Smart Cover Lock is a software-controllable cover lock featured on some HP computers. This lock prevents unauthorized access to the internal components. Computers ship with the Smart Cover Lock in the unlocked position.



---

**CAUTION:** For maximum cover lock security, be sure to establish a setup password. The setup password prevents unauthorized access to the Computer Setup utility.

---



---

The Smart Cover Lock is available as an option on some systems.

---

## Locking the Smart Cover Lock

To activate and lock the Smart Cover Lock, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



---

If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. Select **Security > Smart Cover > Cover Lock > Lock** option.
4. Before exiting, click **File > Save Changes and Exit**.

## Unlocking the Smart Cover Lock

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart**.
2. As soon as the computer is turned on, press **F10** when the monitor light turns green to enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



---

If you do not press **F10** at the appropriate time, you must restart the computer and again press **F10** when the monitor light turns green to access the utility.

---

3. Select **Security > Smart Cover > Cover Lock > Unlock**.
4. Before exiting, click **File > Save Changes and Exit**.

## Using the Smart Cover FailSafe Key

If you enable the Smart Cover Lock and cannot enter the password to disable the lock, you will need a Smart Cover FailSafe Key to open the computer cover. You will need the key in any of the following circumstances:

- Power outage
- Startup failure
- PC component failure (such as processor or power supply)
- Forgotten password



---

**CAUTION:** The Smart Cover FailSafe Key is a specialized tool available from HP. Be prepared; order this key before you need one at an authorized reseller or service provider.

---

To obtain the FailSafe Key, do any one of the following:

- Contact an authorized HP reseller or service provider.
- Call the appropriate number listed in the warranty.

For more information about using the Smart Cover FailSafe Key, consult the *Hardware Reference Guide* on the *Documentation and Diagnostics* CD.

## Cable Lock Provision

The rear panel of the computer accommodates a cable lock so that the computer can be physically secured to a work area.

For illustrated instructions, please see the *Hardware Reference Guide* on the *Documentation and Diagnostics* CD.

## Fingerprint Identification Technology

Eliminating the need to enter user passwords, HP Fingerprint Identification Technology tightens network security, simplifies the login process, and reduces the costs associated with managing corporate networks. Affordably priced, it is not just for high-tech, high-security organizations anymore.



---

Support for Fingerprint Identification Technology varies by model.

---

For more information, visit:

<http://h18004.www1.hp.com/products/security/>.

## Fault Notification and Recovery

Fault Notification and Recovery features combine innovative hardware and software technology to prevent the loss of critical data and minimize unplanned downtime.

If the computer is connected to a network managed by HP Client Manager, the computer sends a fault notice to the network management application. With HP Client Manager Software, you can also remotely schedule diagnostics to automatically run on all managed PCs and create a summary report of failed tests.

## Drive Protection System

The Drive Protection System (DPS) is a diagnostic tool built into the hard drives installed in some HP computers. DPS is designed to help diagnose problems that might result in unwarranted hard drive replacement.

When HP computers are built, each installed hard drive is tested using DPS, and a permanent record of key information is written onto the drive. Each time DPS is run, test results are written to the hard drive. The service provider can use this information to help diagnose conditions that caused you to run the DPS software. Refer to the *Troubleshooting Guide* on the *Documentation and Diagnostics* CD for instructions on using DPS.

## Surge-Tolerant Power Supply

An integrated surge-tolerant power supply provides greater reliability when the computer is hit with an unpredictable power surge. This power supply is rated to withstand a power surge of up to 2000 volts without incurring any system downtime or data loss.

## Thermal Sensor

The thermal sensor is a hardware and software feature that tracks the internal temperature of the computer. This feature displays a warning message when the normal range is exceeded, which gives you time to take action before internal components are damaged or data is lost.

---

# Index

## A

access to computer, controlling 24  
Altiris 1–5  
    AClient 1–2  
    Deployment Solution Agent 1–2  
asset tracking 24

## B

bootable device  
    creating 17 to 21  
    DiskOnKey 17 to 21  
    HP Drive Key 17 to 21  
    USB flash media device 17 to 21

## C

cable lock provision 39  
cautions  
    cover lock security 37  
    FailSafe Key 38  
    protecting ROM 12  
change notification 11  
changing operating systems, important information 23  
changing password 31  
clearing password 33  
cloning tools, software 2  
Computer Setup Utilities 14  
configuring power button 22  
controlling access to computer 24  
cover lock security, caution 37  
cover lock, smart 37  
customizing software 2

## D

Dantz Retrospect Express 1–10  
deleting password 32  
delimiter characters, table 33  
deployment tools, software 2  
diagnostic tool for hard drives 40  
disk, cloning 2  
DiskOnKey  
    *see also* HP Drive Key  
    bootable 17 to 21  
drive, protecting 40  
Drivelock 34 to 35  
dual-state power button 22

## E

entering  
    power-on password 29  
    setup password 30

## F

FailSafe Key  
    caution 38  
    ordering 38  
fault notification 39  
fingerprint identification technology 39

## H

hard drives, diagnostic tool 40  
HP Client Management Solutions 1–5  
HP Client Manager Software 1–5  
HP Drive Key  
    *see also* DiskOnKey

- bootable 17 to 21
- HP Lifecycle solutions 1–2
- HP Local Recovery 1–8
- HP OpenView Management Suite for Desktops Using Radia 1–7
- HP System Software Manager 1–4

## I

- initial configuration 2
- internal temperature of computer 40
- Internet addresses, See Web sites

## K

- keyboard delimiter characters, national 33

## L

- Local Recovery 1–3
- locking Smart Cover Lock 37

## M

- Multibay security 34 to 35

## N

- national keyboard delimiter characters 33
- notification of changes 11

## O

- operating systems, important information about 23
- ordering FailSafe Key 38

## P

- password
  - changing 31
  - clearing 33
  - deleting 32
  - power-on 29
  - security 28
  - setup 28, 30
- PC deployment 1–2
- PCN (Proactive Change Notification) 11
- power button

- configuring 22
  - dual-state 22
- power supply, surge-tolerant 40
- power-on password
  - changing 31
  - deleting 32
  - entering 29
- Preboot Execution Environment (PXE) 3
- preinstalled software image 2
- Proactive Change Notification (PCN) 11
- protecting hard drive 40
- protecting ROM, caution 12
- PXE (Preboot Execution Environment) 3

## R

- recovery, software 2
- Remote ROM Flash 13
- remote setup 3
- Remote System Installation 1–3
  - accessing 3
- retired solutions 1–11
- ROM
  - flash 1–12
  - Remote Flash 13

## S

- security
  - DriveLock 34 to 35
  - features, table 25
  - MultiBay 34 to 35
  - password 28
  - settings, setup of 24
  - Smart Cover Lock 37 to 38
  - Smart Cover Sensor 35
- setup
  - initial 2
  - replicating 14
- setup password
  - changing 31
  - deleting 32

- 
- entering 30
  - setting 28
  - Smart Cover FailSafe Key, ordering 38
  - Smart Cover Lock 37 to 38
    - locking 37
    - unlocking 38
  - Smart Cover Sensor 35
    - protection levels 36
    - setting 36
  - software
    - Altiris AClient 1–2
    - Altiris Deployment Solution Agent 1–2
    - asset tracking 24
    - Computer Setup Utilities 14
    - Drive Protection System 40
    - Fault Notification and Recovery 39
    - HP Local Recovery 1–3
    - integration 2
    - recovery 2
    - Remote ROM Flash 13
    - Remote System Installation 3
    - updating and management 1–4
  - Subscriber's Choice 1–11
  - surge-tolerant power supply 40
- T**
- temperature, internal computer 40
  - thermal sensor 40
- U**
- unlocking Smart Cover Lock 38
  - URLs (Web sites). See Web sites
  - USB flash media device, bootable 17 to 21
- W**
- Web sites
    - Fingerprint Identification Technology 39
    - HPQFlash 13
    - PC deployment 2
    - Proactive Change Notification 11
    - Remote ROM Flash 13
    - replicating setup 17
    - ROM Flash 12
    - software support 23
    - Subscriber's Choice 11

