



Desktop Management Guide

Business Desktops

Document Part Number: 361202-001

May 2004

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

© Copyright 2004 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 Desktops

First Edition (May 2004)

Document Part Number: 361202-001

Contents

Desktop Management Guide

Initial Configuration and Deployment	2
Remote System Installation	3
Software Updating and Management	4
HP Client Manager Software	4
Altiris Client Management Solutions	4
System Software Manager	5
Proactive Change Notification	6
Subscriber's Choice	6
ROM Flash	7
Remote ROM Flash	7
HPQFlash	8
FailSafe Boot Block ROM	8
Replicating the Setup	10
Dual-State Power Button	19
World Wide Web Site	20
Building Blocks and Partners	20
Asset Tracking and Security	21
Password Security	26
Establishing a Setup Password Using Computer Setup	26
Establishing a Power-On Password Using Computer Setup	27
DriveLock	32
Smart Cover Sensor	34
Smart Cover Lock	35
Master Boot Record Security	38
Before You Partition or Format the Current Bootable Disk	40
Cable Lock Provision	40
Fingerprint Identification Technology	41
Fault Notification and Recovery	41

Drive Protection System	41
Surge-Tolerant Power Supply	42
Thermal Sensor	42

Index

Desktop Management Guide

HP Intelligent Manageability 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 Intelligent Manageability and these products. Intelligent Manageability is 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.

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 7)
- 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 and workstations—HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification; and Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) assists HP customers in managing the hardware aspects of their client computers with features that include:

- Detailed views of hardware inventory for asset management
- PC health check monitoring and diagnostics
- Proactive notification of changes in the hardware environment
- Web-accessible reporting of business critical details such as machines with thermal warnings, memory alerts, and more
- Remote updating of system software such as device drivers and ROM BIOS
- Remote changing of boot order

For more information on the HP Client Manager, visit http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

HP and Altiris have partnered to provide comprehensive, tightly integrated systems management solutions to reduce the cost of owning HP client PCs. HP Client Manager Software is the foundation for additional Altiris Client Management Solutions that address:

- Inventory and Asset Management
 - SW license compliance
 - PC tracking and reporting
 - Lease contract, fixing asset tracking
- Deployment and Migration

- Microsoft Windows XP Professional or Home Edition migration
- System deployment
- Personality migrations
- Help Desk and Problem Resolution
 - Managing help desk tickets
 - Remote troubleshooting
 - Remote problem resolution
 - Client disaster recovery
- Software and Operations Management
 - Ongoing desktop management
 - HP system SW deployment
 - Application self-healing

For more information and details on how to download a fully-functional 30-day evaluation version of the Altiris solutions, visit <http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

On selected desktop and notebook models, an Altiris management agent is included as part of the factory loaded image. This agent enables communication with the Altiris Development Solution which can be used to complete new hardware deployment or personality migration to a new operating system using easy-to-follow wizards. Altiris solutions provide easy-to-use software distribution capabilities. When used in conjunction with System Software Manager, or HP Client Manager Software, administrators can also update ROM BIOS and device driver software from a central console.

For more information, visit <http://h18000.www1.hp.com/im/index.html>.

System Software Manager

System Software Manager (SSM) is a utility that lets you update system-level software on multiple systems simultaneously. When executed on a PC client system, SSM detects both hardware and software versions, then updates the appropriate software from a central repository, also known as a file store. Driver versions that

are supported by SSM are denoted with a special icon on the driver download Web site and on the Support Software CD. To download the utility or to obtain more information on SSM, visit <http://www.hp.com/go/ssm>.

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>.

ROM Flash

The computer comes with 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 ROM, you may:

- Order an upgraded ROMPaq diskette from HP.
- Download the latest ROMPaq images from 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 ROM on remote HP computers directly from the centralized network management console. Enabling the system administrator to perform this task remotely, on multiple computers and personal computers, results in a consistent deployment of and greater control over HP PC ROM 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 ROM on individual PCs through a Windows operating system.

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

FailSafe Boot Block ROM

The FailSafe Boot Block ROM allows for system recovery in the unlikely event of a ROM flash failure, for example, if a power failure were to occur during a ROM upgrade. The Boot Block is a flash-protected section of the ROM that checks for a valid system ROM flash when power to the system is turned on.

- If the system ROM is valid, the system starts normally.
- If the system ROM fails the validation check, the FailSafe Boot Block ROM provides enough support to start the system from a ROMPaq diskette, which will program the system ROM with a valid image.



Some models also support recovery from a ROMPaq CD. ISO ROMPaq images are included with selected models in the downloadable ROM softpaqs.

When the boot block detects an invalid system ROM, the System Power LED blinks RED 8 times, one every second, followed by a 2-second pause. Also 8 simultaneous beeps will be heard. A Boot Block recovery mode message is displayed on the screen (some models).

To recover the system after it enters Boot Block recovery mode, complete the following steps:

1. If there is a diskette in the diskette drive or a CD in the CD drive, remove the diskette and CD and turn off the power.
2. Insert a ROMPaq diskette into the diskette drive or, if permitted on this computer, a ROMPaq CD into the CD drive.

3. Turn on the computer.

If no ROMPaq diskette or ROMPaq CD is found, you will be prompted to insert one and restart the computer.

If a setup password has been established, the Caps Lock light will turn on and you will be prompted to enter the password.

4. Enter the setup password.

If the system successfully starts from the diskette and successfully reprograms the ROM, then the three keyboard lights will turn on. A rising tone series of beeps also signals successful completion.


5. Remove the diskette or CD and turn the power off.

6. Turn the power on again to restart the computer.

The following table lists the various keyboard light combinations used by the Boot Block ROM (when a PS/2 keyboard is attached to the computer), and explains the meaning and action associated with each combination.

Keyboard Light Combinations Used by Boot Block ROM

FailSafe Boot Block Mode	Keyboard LED Color	Keyboard LED Activity	State/Message
Num Lock	Green	On	ROMPaq diskette or ROMPaq CD not present, is bad, or drive not ready.
Caps Lock	Green	On	Enter password.
Num, Caps, Scroll Lock	Green	Blink On in sequence, one at a time—N, C, SL	Keyboard locked in network mode.
Num, Caps, Scroll Lock	Green	On	Boot Block ROM Flash successful. Turn power off, then on to reboot.

 Diagnostic lights do not flash on USB keyboards.

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 dc7100 Ultra-Slim Desktop to a dx6100 Slim Tower.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
-



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

5. If you are using a 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 and hold the **F10** key until you 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 dc7100 Ultra-Slim Desktop to a dx6100 Slim Tower.

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 10](#)).

1. Create a bootable diskette or USB flash media device. See [“Supported USB Flash Media Device” on page 13](#) or [“Unsupported USB Flash Media Device” on page 16](#).
-



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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

6. If you are using a 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 <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, such as an HP Drive Key or a DiskOnKey, have a preinstalled image to simplify the process of making them bootable. 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 16](#)).



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.

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

- One of the following systems:
 - ❑ HP Compaq Business Desktop dc7100 series
 - ❑ HP Compaq Business Desktop dx6100 series
 - ❑ HP Compaq Business Desktop d530 Series - Ultra-Slim Desktop, Small Form Factor, or Convertible Minitower
 - ❑ Compaq Evo D510 Ultra-Slim Desktop
 - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor

Depending on the individual BIOS, future systems may also support booting to a USB flash media device.



CAUTION: If you are using a computer other than one named above, make sure the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive.

- One of the following storage modules:
 - ❑ 16MB HP Drive Key
 - ❑ 32MB HP Drive Key
 - ❑ 32MB DiskOnKey
 - ❑ 64MB HP Drive Key

- 64MB DiskOnKey
 - 128MB HP Drive Key
 - 128MB DiskOnKey
 - 256MB HP Drive Key
 - 256MB DiskOnKey
- 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.
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 11.](#)

Unsupported USB Flash Media Device



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.

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

- One of the following systems:
 - ❑ HP Compaq Business Desktop dc7100 series
 - ❑ HP Compaq Business Desktop dx6100 series
 - ❑ HP Compaq Business Desktop d530 Series - Ultra-Slim Desktop, Small Form Factor, or Convertible Minitower
 - ❑ Compaq Evo D510 Ultra-Slim Desktop
 - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor

Depending on the individual BIOS, future systems may also support booting to a USB flash media device.



CAUTION: If you are using a computer other than one named above, make sure the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive.

- 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.
 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 and hold the **F10** key until you 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 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 11.

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. ProtectTools Embedded Security, if installed, prevents unauthorized access to data and checks system integrity and authenticates third-party users attempting system access. (Refer to *HP ProtectTools Embedded Security Guide*, on the *Documentation CD* for more information.) Security features such as ProtectTools, the Smart Cover Sensor and the Smart Cover Lock, available on select 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.






ProtectTools, the Smart Cover Sensor, and the Smart Cover Lock are available as options on select 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 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 CD</i> 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 CD</i> 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 (CTRL+ALT+DEL).</p> <p>See the <i>Desktop Management Guide</i> on the <i>Documentation CD</i> 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"> • Enable/disable the Cover Lock. • Enable/disable the Cover Removal Sensor. <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 select models only. See the <i>Desktop Management Guide</i> on the <i>Documentation CD</i> for more information.</p>
<p> For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation CD</i>.</p> <p>Support for security features may vary depending on the specific computer configuration.</p>	




Security Features Overview *(Continued)*

Option	Description
Embedded Security	<p>Allows you to:</p> <ul style="list-style-type: none"> • Enable/disable the Embedded Security device. • Reset the device to Factory Settings. <p>This feature is supported on select models only. See <i>HP ProtectTools Embedded Security Guide</i>, on the <i>Documentation CD</i> for more information.</p>
Device Security	<p>Enables/disables serial ports, parallel port, front USB ports, system audio, network controllers (some models), MultiBay devices (some models), and SCSI controllers (some models).</p>
Network Service Boot	<p>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.)</p>
System IDs	<p>Allows you to set:</p> <ul style="list-style-type: none"> • Asset tag (18-byte identifier) and ownership Tag (80-byte identifier displayed during POST). <p>See the <i>Desktop Management Guide</i> on the <i>Documentation CD</i> for more information.</p> <ul style="list-style-type: none"> • 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.) <p>Keyboard locale setting (for example, English or German) for System ID entry.</p>
	<p>For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation CD</i>.</p> <p>Support for security features may vary depending on the specific computer configuration.</p>

Security Features Overview (Continued)

Option	Description
DriveLock	<p>Allows you to assign or modify a master or user password for MultiBay hard drives (not supported on SCSI 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 MultiBay drive that supports the DriveLock feature is attached to the system.</p> <p>See the <i>Desktop Management Guide</i> on the <i>Documentation CD</i> for more information.</p>
Master Boot Record Security	<p>Allows you to enable or disable Master Boot Record (MBR) Security.</p> <p>When enabled, the BIOS rejects all requests to write to the MBR on the current bootable disk. Each time the computer is powered on or rebooted, the BIOS compares the MBR of the current bootable disk to the previously-saved MBR. If changes are detected, you are given the option of saving the MBR on the current bootable disk, restoring the previously-saved MBR, or disabling MBR Security. You must know the setup password, if one is set.</p> <p> Disable MBR Security before intentionally changing the formatting or partitioning of the current bootable disk. Several disk utilities (such as FDISK and FORMAT) attempt to update the MBR.</p> <p>If MBR Security is enabled and disk accesses are being serviced by the BIOS, write requests to the MBR are rejected, causing the utilities to report errors.</p> <p>If MBR Security is enabled and disk accesses are being serviced by the operating system, any MBR change will be detected by the BIOS during the next reboot, and an MBR Security warning message will be displayed.</p>
<p> For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation CD</i>.</p> <p>Support for security features may vary depending on the specific computer configuration.</p>	

Security Features Overview *(Continued)*

Option	Description
Save Master Boot Record	Saves a backup copy of the Master Boot Record of the current bootable disk. Only appears if MBR Security is enabled.
Restore Master Boot Record	Restores the backup Master Boot Record to the current bootable disk.  Only appears if all of the following conditions are true: <ul style="list-style-type: none"> • MBR Security is enabled. • A backup copy of the MBR has been previously saved. • The current bootable disk is the same disk from which the backup copy of the MBR was saved. <hr/>  CAUTION: Restoring a previously saved MBR after a disk utility or the operating system has modified the MBR may cause the data on the disk to become inaccessible. Only restore a previously saved MBR if you are confident that the current bootable disk's MBR has been corrupted or infected with a virus.
 For more information about Computer Setup, see the <i>Computer Setup (F10) Utility Guide</i> on the <i>Documentation CD</i> .	Support for security features may vary depending on the specific computer configuration.

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 *HP ProtectTools Embedded Security Guide*, on the *Documentation CD*. Establishing a setup password through Computer Setup prevents reconfiguration 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 *HP ProtectTools Embedded Security Guide*, on the *Documentation CD*.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 *HP ProtectTools Embedded Security Guide*, on the *Documentation CD*.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 31 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 *HP ProtectTools Embedded Security Guide*, on the *Documentation CD*.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 CD* for instructions on clearing passwords.

If the system is equipped with an embedded security device, refer to *HP ProtectTools Embedded Security Guide*, on the *Documentation CD*.

DriveLock

DriveLock is an industry-standard security feature that prevents unauthorized access to the data on MultiBay hard drives. DriveLock has been implemented as an extension to Computer Setup. It is only available when DriveLock-capable hard drives 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 where a system administrator provides users with MultiBay hard drives for use in some computers. The system administrator would be responsible for configuring the MultiBay 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 select 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 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

-
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 select 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 select 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

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 CD*.

Master Boot Record Security

The Master Boot Record (MBR) contains information needed to successfully boot from a disk and to access the data stored on the disk. Master Boot Record Security detects and reports unintentional or malicious changes to the MBR, such as those caused by some computer viruses or by the incorrect use of certain disk utilities. It also allows you to recover the “last known good” MBR, should changes to the MBR be detected when the system is restarted.

To enable MBR Security, 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Security > Master Boot Record Security > Enabled**.
4. Select **Security > Save Master Boot Record**.
5. Before exiting, click **File > Save Changes and Exit**.

When MBR Security is enabled, the BIOS prevents any changes being made to the MBR of the current bootable disk while in MS-DOS or Windows Safe Mode.



Most operating systems control access to the MBR of the current bootable disk; the BIOS cannot prevent changes that may occur while the operating system is running.

Each time the computer is turned on or restarted, the BIOS compares the MBR of the current bootable disk to the previously saved MBR. If changes are detected and if the current bootable disk is the same disk from which the MBR was previously saved, the following message is displayed:

1999—Master Boot Record has changed.

Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk;
- Restore the previously saved MBR; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

If changes are detected and if the current bootable disk is **not** the same disk from which the MBR was previously saved, the following message is displayed:

2000—Master Boot Record Hard Drive has changed.

Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

In the unlikely event that the previously saved MBR has been corrupted, the following message is displayed:

1998—Master Boot Record has been lost.

Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

Before You Partition or Format the Current Bootable Disk

Ensure that MBR Security is disabled before you change partitioning or formatting of the current bootable disk. Some disk utilities, such as FDISK and FORMAT, attempt to update the MBR. If MBR Security is enabled when you change partitioning or formatting of the disk, you may receive error messages from the disk utility or a warning from MBR Security the next time the computer is turned on or restarted. To disable MBR Security, 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 and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.



If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Security > Master Boot Record Security > Disabled**.
4. Before exiting, click **File > Save Changes and Exit**.

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 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 select 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 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 21
Altiris 4
asset tracking 21

B

bootable device
 creating 13 to 18
 DiskOnKey 13 to 18
 HP Drive Key 13 to 18
 USB flash media device 13 to 18
bootable disk, important information 40

C

cable lock provision 40
cautions
 cover lock security 35
 FailSafe Key 37
 protecting ROM 7
change notification 6
changing operating systems, important information 20
changing password 29
clearing password 31
cloning tools, software 2
Computer Setup Utilities 10
configuring power button 19
controlling access to computer 21
cover lock security, caution 35
cover lock, smart 35
customizing software 2

D

deleting password 30
delimiter characters, table 31
deployment tools, software 2
diagnostic tool for hard drives 41
disk, cloning 2
DiskOnKey
 see also HP Drive Key
 bootable 13 to 18
drive, protecting 41
Drivelock 32 to 33
dual-state power button 19

E

entering
 power-on password 27
 setup password 28

F

FailSafe Boot Block ROM 8
FailSafe Key
 caution 37
 ordering 37
fault notification 41
fingerprint identification technology 41
formatting disk, important information 40

H

hard drives, diagnostic tool 41
HP Client Manager 4
HP Drive Key
 see also DiskOnKey

bootable 13 to 18

I

initial configuration 2
internal temperature of computer 42
Internet addresses, See Web sites
invalid system ROM 8

K

keyboard delimiter characters, national 31
keyboard lights, ROM, table 9

L

locking Smart Cover Lock 36

M

Master Boot Record Security 38 to 39
Multibay security 32 to 33

N

national keyboard delimiter characters 31
notification of changes 6

O

operating systems, important information
 about 20
ordering FailSafe Key 37

P

partitioning disk, important information 40
password
 changing 29
 clearing 31
 deleting 30
 power-on 27
 security 26
 setup 26, 28
PCN (Proactive Change Notification) 6
power button
 configuring 19
 dual-state 19
power supply, surge-tolerant 42

power-on password

 changing 29
 deleting 30
 entering 27

Preboot Execution Environment (PXE) 3
preinstalled software image 2
Proactive Change Notification (PCN) 6
protecting hard drive 41
protecting ROM, caution 7
PXE (Preboot Execution Environment) 3

R

recovering system 8
recovery, software 2
Remote ROM Flash 7
remote setup 3
Remote System Installation, accessing 3
ROM
 invalid 8
 keyboard lights, table 9
 Remote Flash 7
 upgrading 7

S

security
 DriveLock 32 to 33
 features, table 22
 Master Boot Record 38 to 39
 MultiBay 32 to 33
 password 26
 settings, setup of 21
 Smart Cover Lock 35 to 37
 Smart Cover Sensor 34
setup
 initial 2
 replicating 10
setup password
 changing 29
 deleting 30
 entering 28

- setting 26
- Smart Cover FailSafe Key, ordering 37
- Smart Cover Lock 35 to 37
 - locking 36
 - unlocking 36
- Smart Cover Sensor 34
 - protection levels 34
 - setting 35
- software
 - asset tracking 21
 - Computer Setup Utilities 10
 - Drive Protection System 41
 - FailSafe Boot Block ROM 8
 - Fault Notification and Recovery 41
 - integration 2
 - Master Boot Record Security 38 to 39
 - recovery 2
 - Remote ROM Flash 7
 - Remote System Installation 3
 - System Software Manager 6
 - updating multiple machines 6
- SSM (System Software Manager) 5
- surge-tolerant power supply 42
- system recovery 8
- System Software Manager (SSM) 5

T

- temperature, internal computer 42
- thermal sensor 42

U

- unlocking Smart Cover Lock 36
- upgrading ROM 7
- URLs (Web sites). See Web sites
- USB flash media device, bootable 13 to 18

W

- Web sites
 - Altiris 5
 - Fingerprint Identification Technology 41
 - HP Client Manager 4
 - HPQFlash 8
 - PC deployment 2
 - Proactive Change Notification 6
 - Remote ROM Flash 7
 - replicating setup 12, 13
 - ROM Flash 7
 - ROMPaq images 7
 - software support 20
 - Subscriber's Choice 6
 - System Software Manager (SSM) 6

