Desktop Management Guide

HP Business PCs

Desktop Management Guide

HP Business PCs

Fourth Edition (September 2009)

Document Part Number: 581009-001

About This Book

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

⚠ **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.

NOTE: Text set off in this manner provides important supplemental information.

Table of contents

1 Desktop Management Overview

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 develops its own management software and 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 solutions that assist you in lowering the total cost of owning and maintaining the PCs throughout their lifecycle.

The key capabilities and features of desktop management are:

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

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

2 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 HP Client Automation Standard Edition or HP Client Automation Enterprise Edition (based on Radia technology) 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.

ROM-based setup and ACPI hardware provide further assistance with recovery of system software, configuration management and troubleshooting, and power management.

HP Client Automation Agent

The management agent used by both HP Client Automation Standard and Enterprise Editions is pre-loaded on the computer. When installed, it enables communication with the HP management console.

To install the HP Client Automation Agent:

1. Click **Start**.
2. Click **All Programs**.
3. Click **HP Manageability**.
4. Click the **HP Management Agent Readme** applicable to the language you desire.
5. Review and follow the instructions contained in the Readme file to install the HP Client Automation Agent.

HP Client Automation Agent is a key infrastructure component for enabling all of the HP Client Automation solutions. To learn about the other infrastructure components necessary for implementing the HP configuration management solutions, please visit http://h20229.www2.hp.com/solutions/ascm/index.html.

HP Client Manager

HP Client Manager (HPCM) is a free solution developed by Symantec for all supported HP business desktop, notebook, workstation and HP Blade PCs. HPCM integrates HP specific tools such as System Software Manager, HP Instant Support Professional Edition, and HP Client Management Interface to enable a centralized model for the managing, tracking, and monitoring of all supported HP hardware.

HP Client Manager 7.0 features a brand new Portal Page which serves as a one-stop-shop where the administrator can accomplish the following management tasks:

- Inventory
- Alerts
- BIOS Management
- Driver Updates
- Perform HP Instant Support Health Scan and Diagnostics
- Perform Embedded Security tasks
- View the overall HP Health Alert Trend over the last 3-6 months
- View the overall compliance of supported computers with HP Instant Support Health Scan and Diagnostics
- View the Summary of HP Computers – a breakdown of the various supported desktops, notebooks, workstations and HP Blade PCs
- View Alerts: Asset, Threshold, Hardware Health
- Reports
- Administrative tasks to update HP specific tools

HPCM can be downloaded from http://www.symantec.com/business/theme.jsp by clicking on **HP Client Manager** under **Strategic Partner Products**. A free permanent license can also be obtained from the download page.

HPCM “How to” videos are also published on http://www.symantec.com/connect. Search for **HP Client Manager 7.0** to view step by step videos for various tasks within HPCM.

3 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)

  NOTE: There are facilities to flash the system BIOS from within the Microsoft Windows operating system.

- 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 when the computer is booting up. 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.

4 Software Updating and Management

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

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard, and Enterprise Editions
- HP Client Manager from Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- Intel vPro-branded PCs with Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

Regardless of the system management tools your IT department uses, managing both your hardware and software assets is important to keeping your IT costs low and your business agile. The IT administrator can access the HP Client Management Interface by writing simple scripts and integrating those scripts to the management solution of their choice.

With the HP Client Management Interface (HP CMI), new HP business computers seamlessly integrate into your managed IT environment. HP CMI provides an interface that simplifies the integration of HP business computers with popular industry system management tools (including Microsoft Systems Management Server, IBM Tivoli Software, and HP Operations) and custom in-house developed management applications. Using HP CMI, systems management tools and applications can request in-depth client inventory, receive health status information, and manage system BIOS settings by communicating directly with the client computer, reducing the need for agent or connector software to achieve integration.

HP Client Management Interface is based on industry standards that include Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS), and Advanced Configuration and Power Interface (ACPI). HP CMI is a foundation

technology utilized in HP Client Management Solutions. With HP CMI, HP gives you flexibility in choosing how you manage your HP client computers.

HP Client Management Interface used in conjunction with system management software can:

- Request in-depth client inventory information—Capture detailed information about the processors, hard drives, memory, BIOS, drivers, including sensor information (such as fan speed, voltage, and temperature).
- Receive health status information—Subscribe for a wide range of client hardware alerts (such as over-temperature, fan stall, and hardware configuration changes) to be sent to the system management console, application, or to the local client computer. Alerts are sent real-time when triggered by hardware events.
- Manage system BIOS settings—Perform F10 functions including setting and changing the BIOS passwords and computer boot order remotely from your system management console on any or all of your client systems without having to visit each machine.

For more information on HP Client Management Interface, refer to http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager is a free, easy-to-use interface for locating and downloading software updates for the HP client PC models in your environment. By specifying your models, operating system, and language, you can quickly locate, sort, and select the softpaqs you need. To download HP SoftPaq Download Manager, visit http://www.hp.com/go/sdm.

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 Client Automation solutions, HP Client Manager from Symantec, 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 http://www.hp.com/go/ssm.

NOTE: SSM does not currently support remote ROM flash on systems that have Windows BitLocker Drive Encryption enabled and are using TPM measurements to protect the BitLocker keys because flashing the BIOS would invalidate the trust signature that BitLocker created for the platform. Disable BitLocker via Group Policy in order to flash the system BIOS.

You can enable BitLocker support without TPM measurements of BIOS to avoid invalidating the BitLocker keys. HP recommends you keep a secure backup of the BitLocker credentials in case of recovery emergencies.

HP ProtectTools Security Manager

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

HP ProtectTools Security Manager is the single console through which all other modules are accessed.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

HP ProtectTools provides two versions that can be utilized: HP ProtectTools Security Manager and HP ProtectTools Administrative Console. Both Administrator and user versions are available in the **Start** > **All Programs** menu.

The software modules available for your computer may vary depending on your model. For example, Embedded Security for HP ProtectTools is available only for computers on which the Trusted Platform Module (TPM) embedded security chip is installed.

HP ProtectTools software modules may be preinstalled, preloaded, or available for download from the HP Web site. For select HP Pro Desktops, HP ProtectTools is available as an after market option. Visit http://www.hp.com/products/security for more information.

HP Client Automation Starter and Standard Editions

HP Client Automation is a hardware and software management solution for Windows Vista, Windows XP and HP Thin Client environments that is easy to use and quick to deploy, while providing a strong foundation for future requirements. It is offered in two editions:

- The Starter Edition is a free product for managing HP desktops, notebooks and workstations, providing hardware and software inventory, remote control, HP alert monitoring, HP BIOS and driver updates, integration with HP Protect Tools and add-on support for Intel AMT. The Starter Edition also supports deployment and management of HP Thin Clients.
- The Standard Edition, available for purchase, includes all functionality provided in Starter Edition and adds Windows deployment and migration, patch management capabilities, software distribution and software usage metering.

HP Client Automation Starter and Standard Editions provide a migration path to HP Client Automation Enterprise Edition (based on Radia technology) for automated management of large, heterogeneous and continuously changing IT environments.

For more information about the HP Client Automation solutions, visit http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition is a policy-based solution that enables administrators to inventory, deploy, patch, and continuously manage software and content across heterogeneous client platforms. With the HP Client Automation Enterprise Edition, the IT professional can:

- Automate the entire lifecycle management process from discovery, deployment, and ongoing management through migration and retirement
- Automatically deploy and continuously manage an entire software stack (operating systems, applications, patches, settings, and content) to a desired state
- Manage software on virtually any device, including desktops, workstations, and notebooks, in a heterogeneous or standalone infrastructure
- Manage software on most operating systems

With continuous configuration management, HP customers report dramatic savings in IT costs, accelerated time-to-market for software and content, and increased user productivity and satisfaction.

For more information about the HP Client Automation solutions, visit http://www.hp.com/go/client.

HP Client Manager from Symantec

HP Client Manager from Symantec, 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 from Symantec to:

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

Tight integration with HP Instant Support tools reduces hardware troubleshooting time.

- Diagnostics—remotely run & view reports on HP desktop, notebook, and workstation models
- System Health Scan—check for known hardware issues in your installed base of HP client systems
- Active Chat—connect to HP customer support to resolve issues
- HP Knowledgebase—link to expert information
- Automated SoftPaq collection and delivery process for fast resolution of hardware problems
- Identify, inventory, and initialize systems with HP ProtectTools embedded security chip
- Option for health alerts to display locally on the client system
- Report basic inventory information for non-HP clients
- Setup and configure TPM security chip

- Centrally schedule client backup and recovery
- Add on support for managing Intel AMT

For more information on HP Client Manager from Symantec, visit http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite is an easy-to-use solution for full life-cycle software management of desktops, notebooks, and workstations. Client Management Suite includes the following Altiris products:

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

For more information on Altiris Client Management Suite, visit http://www.symantec.com/business/client-management-suite.

HP Client Catalog for Microsoft System Center & SMS Products

The HP Client Catalog enables IT professionals using Microsoft products to automate the deployment of HP software updates (Softpaqs) to HP business PCs. The catalog file contains detailed platform information on HP business desktops, notebooks and workstations. It can be used in conjunction with the custom inventory and update features of Microsoft products to provide automated driver and patch updates to managed HP client computers.

Microsoft products supported by the HP Client Catalog include:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

For more information on HP Client Catalog for SMS, visit http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

Remote Management Technology

Models include either vPro technology or standard technology. Both allow for better discovery, healing, and protection of networked computing assets. Both technologies allow PCs to be managed whether the system is on, off, or the operating system is hung.

The three forms of remote manageability available on business desktops are Alert Standard Format (ASF), Intel Active Management Technology (AMT), and Desktop and mobile Architecture for Systems Hardware (DASH).

Remote management technology features include:

- Network discovery
- Hardware inventory information
- Platform health monitoring
- Power management—power on/off, cycle power
- Remote diagnosis and repair
  - Text console redirection—allows console control of remote PC during its boot phase
  - Media redirection—allows system booting from a remote boot drive, disk, or ISO image (the two variants of this are IDE-Redirect (IDE-R) on AMT platforms and USB Media Redirection)
- Hardware-based isolation and recovery—limit or cut off PC network access, if virus-like activity is detected
- Platform event tracking and auditing
- Integrated web server management portal for remote access and configuration
- Remote management technologies are integrated with HP's management console partners

NOTE: All features above are not available on all platforms.

Configuring the Intel Management Engine

NOTE: For an overview of Intel vPro technology, visit http://www.intel.com/vpro.

For HP-specific information on Intel vPro technology, see the white papers at http://www.hp.com/support. Select your country and language, select **See support and troubleshooting information**, enter the model number of the computer, and press Enter. In the **Resources** category, click **Manuals (guides, supplements, addendums, etc.)**. Under **Quick jump to manuals by category**, click **White papers**.

Available management technologies include the following:

- AMT (includes DASH 1.0)
- ASF
- DASH 1.1 (using a Broadcom NIC)

ASF and AMT may not be configured at the same time, but both are supported.

To configure Intel vPro systems for AMT or ASF:

1. Turn on or restart the computer. If you are in Microsoft Windows, click **Start** > **Shut Down** > **Restart**.
2. As soon as the computer is turned on, press the hot key, Ctrl+P, before the computer boots to the operating system.

NOTE: If you do not press Ctrl+P at the appropriate time, you must restart the computer and again press Ctrl+P before the computer boots to the operating system to access the utility.

This hot-key enters the Intel Management Engine BIOS Execution (MEBx) setup utility. This utility allows the user to configure various aspects of the management technology. Some of the configuration options are listed below:

- Main Menu
  - Intel ® ME Configuration
  - Intel ® AMT Configuration
  - Change Intel ® ME Password
  - Exit
- Intel ® ME Platform Configuration
  - Intel ® ME State Control (enable/disable)
  - Intel ® ME Firmware Local Update (enable/disable)
  - Intel ® ME Features Control
  - Intel ® ME Power Control
- Intel ® AMT Configuration
  - Host Name
  - TCP/IP
  - Provision Model (Enterprise, SMB)
  - Setup and Configuration
  - Un-Provision
  - SOL/IDE-R (enable/disable)
  - Password Policy
  - Secure Firmware Update (enable/disable)
  - Set PRTC
  - Idle Timeout
- Change Intel ® ME Password (HP highly recommends that this password be changed. The default password is **admin**.)

In order to remotely manage AMT systems, the administrator must use a remote console that supports AMT. Enterprise management consoles are available from suppliers such as HP, Altiris and Microsoft SMS. In SMB mode, the client provides a Web browser interface. To access this feature, open a browser from any other system on the network and enter `http://host_name:16992` where `host_name` is the name assigned to the system. Alternatively, the IP address may be used in place of the host name.

To configure systems with a Broadcom DASH capable NIC:

Check for the latest documentation on the http://www.hp.com site under **Support & Troubleshooting**, then select your specific model, then select **Manuals**, then **White papers** referring to DASH or the Broadcom NIC.

Verdiem Surveyor

Verdiem Surveyor is a software solution that helps manage PC energy costs. Surveyor measures and reports how much energy each PC consumes. It also provides control over PC power settings enabling administrators to easily implement energy saving strategies across their networks. An HP SoftPaq containing the Surveyor agent may be downloaded from the HP Support site and installed on supported commercial desktop models. Surveyor licenses for managing PCs may be purchased through your HP representative.

HP 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-mail 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

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

Two software packages, Altiris Local Recovery, and Dantz Retrospect, will no longer be shipping on HP business desktops, notebooks, or workstations.

5 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.

NOTE: SSM does not currently support remote ROM flash on systems that have Windows BitLocker Drive Encryption enabled and are using TPM measurements to protect the BitLocker keys because flashing the BIOS would invalidate the trust signature that BitLocker created for the platform. Disable BitLocker via Group Policy in order to flash the system BIOS.

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://www.hp.com/go/ssm/.

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.

6 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.

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 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 is found, you will be prompted to insert media containing a BIOS image file.

   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.

NOTE: BitLocker prevents Windows Vista from booting when a CD containing the BIOS image file is in an optical drive. If BitLocker is enabled, remove this CD before attempting to boot to Windows Vista.

7 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.

NOTE: Both procedures require a diskette drive or a supported USB flash drive.

NOTE: System Software Manager (SSM) can be used to replicate computer setup information from within the Windows operating system. For more information see the SSM User's Guide at http://www.hp.com/go/ssm.

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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

   NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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 before the computer boots to the operating system 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.

NOTE: 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 18.

   △ **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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

   NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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 http://welcome.hp.com/country/us/en/support.html 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 18).

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 messages 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.

NOTE: 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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 before the computer boots to the operating system 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.

NOTE: 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 (F10) Utility* 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.

8 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 standby 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.

9 HP Web Site Support

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.

10 Industry Standards

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

11 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, HP Configuration Management Solution, HP Client Configuration 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 http://www.hp.com/products/security.) 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.

NOTE: 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* included with the computer for additional information and instructions on using the Computer Setup Utilities.
- Remotely, using HP Client Manager from Symantec, HP Client Automation, or System Software Manager. This software enables the secure, consistent deployment and control of security settings.

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

Table 11-1 Security Features Overview

Option	Description
Setup Password	Allows you to set and enable setup (administrator) password. **NOTE:** 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.
Power-On Password	Allows you to set and enable power-on password. The power-on password prompt appears after a power cycle. If the user does not enter the correct power-on password, the unit will not boot. **NOTE:** This password does not appear on warm boots , such as Ctrl+Alt+Delete or **Restart from Windows**, unless enabled in **Password Options** (see below).

Table 11-1 Security Features Overview (continued)

Password Options (This selection appears only if a power-on password or setup password is set.)	Allows you to: • Lock legacy resources (appears if a setup password is set) • Enable/disable network server mode (appears if a power-on password is set) • Specify whether the password is required for warm boot (Ctrl+Alt+Delete) (appears if a power-on password is set) • Enable/Disable Setup Browse Mode (appears if a setup password is set) (allows viewing, but not changing, the F10 Setup Options without entering setup password) • Enable/disable Stringent Password (appears if a power-on password is set), which when enabled bypasses the onboard password jumper to disable the power-on password See the *Desktop Management Guide* for more information.
Smart Cover (some models)	Allows you to: • Lock/unlock the Cover Lock. • Set the Cover Removal Sensor to Disable/Notify User/Setup Password. **NOTE:** *Notify User* alerts the user that the sensor has detected that the cover has been removed. *Setup Password* requires that the setup password be entered to boot the computer if the sensor detects that the cover has been removed. This feature is supported on some models only.
Device Security	Allows you to set Device Available/Device Hidden for: • Serial ports • Parallel port • Rear USB ports • Front USB ports • Internal USB ports • System audio • Network controllers (some models) • Legacy diskette • Embedded security device (some models) • SATA0 • SATA1 (some models) • SATA2 (some models) • SATA3 (some models) • eSATA (some models)
LoJack for HP ProtectTools	Allows you to remotely monitor, manage, and track your computer. Once activated, LoJack Pro for HP ProtectTools is configured from the Absolute Software Customer Center. From the Customer Center, the administrator can configure LoJack for HP ProtectTools to monitor or manage the computer. If the system is misplaced or stolen, the Customer Center can assist local authorities to locate and recover the computer. If configured, LoJack Pro can continue to function even if the hard drive is erased or replaced.

Table 11-1 Security Features Overview (continued)

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 be either a PCI expansion card or embedded on the system board.)
System IDs	Allows you to set: • Asset tag (18-byte identifier), a property identification number assigned by the company to the computer. • Ownership tag (80-byte identifier) displayed during POST. • 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.) • Keyboard locale setting (for example, English or German) for System ID entry.
DriveLock Security	Allows you to assign or modify a master or user password for 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. **NOTE:** This selection will only appear when at least one drive that supports the DriveLock feature is attached to the system.
Setup Security Level	Provides a method to allow end-users limited access to change specified setup options, without having to know the Setup Password. This feature allows the administrator the flexibility to protect changes to essential setup options, while allowing the user to view system settings and configure nonessential options. The administrator specifies access rights to individual setup options on a case-by-case basis via the Setup Security Level menu. By default, all setup options are assigned Setup Password, indicating the user must enter the correct Setup Password during POST to make changes to any of the options. The administrator may set individual items to None, indicating the user can make changes to the specified options when setup has been accessed with invalid passwords. The choice, None, is replaced by Power-On Password if a Power-On Password is enabled. **NOTE:** Setup Browse Mode must be set to Enable in order for the user to enter Setup without knowing the setup password.
System Security (some models: these options are hardware dependent)	Data Execution Prevention (some models) (enable/disable) - Helps prevent operating system security breaches. Virtualization Technology (some models) (enable/disable) - Controls the virtualization features of the processor. Changing this setting requires turning the computer off and then back on. Virtualization Technology Directed I/O (some models) (enable/disable) - Controls virtualization DMA remapping features of the chipset. Changing this setting requires turning the computer off and then back on. Trusted Execution Technology (some models) (enable/disable) - Controls the underlying processor and chipset features needed to support a virtual appliance. Changing this setting requires turning the computer off and then back on. To enable this feature you must enable the following features: • Embedded Security Device Support • Virtualization Technology • Virtualization Technology Directed I/O Embedded Security Device Support (some models) (enable/disable) - Permits activation and deactivation of the Embedded Security Device. Changing this setting requires turning the computer off and then back on.

Table 11-1 Security Features Overview (continued)

	NOTE: To configure the Embedded Security Device, a Setup password must be set. • Reset to Factory Settings (some models) (Do not reset/Reset) - Resetting to factory defaults will erase all security keys. Changing this setting requires turning the computer off and then back on. **CAUTION:** The embedded security device is a critical component of many security schemes. Erasing the security keys will prevent access to data protected by the Embedded Security Device. Choosing Reset to Factory Settings may result in significant data loss. • Reset authentication credentials (some models) (Do not reset/Reset) - Selecting Reset disables the power-on authentication support and clears the authentication information from the Embedded Security Device. Changing this setting requires turning the computer off and then back on OS management of Embedded Security Device (some models) (enable/disable) - This option allows the user to limit operating system control of the Embedded Security Device. Changing this setting requires turning the computer off and then back on. This option allows the user to limit OS control of the Embedded Security Device. • Reset of Embedded Security Device through OS (some models) (enable/disable) - This option allows the user to limit the operating system ability to request a Reset to Factory Settings of the Embedded Security Device. Changing this setting requires turning the computer off and then back on. **NOTE:** To enable this option, a Setup password must be set. PAVP (Some models) (disabled/min/max) - PAVP enables the Protected Audio Video Path in the Chipset. This may allow viewing of some protected high definition content that would otherwise be prohibited from playback. Selecting Max will assign 96 Megabytes of system memory exclusively to PAVP.

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.

NOTE: System Software Manager (SSM) can be used to create and manage BIOS passwords from within the Windows operating system. For more information see the SSM User's Guide at http://www.hp.com/go/ssm.

NOTE: HP Client Management Interface (HP CMI) provides access to BIOS setting management including BIOS passwords from within the Windows operating system. For more information see the HP Client Management Interface Technical Whitepaper at http://www.hp.com/go/hpcmi.

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 http://www.hp.com. 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 F10 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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.

NOTE: 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 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system to access the utility.

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

NOTE: 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 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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`

NOTE: 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.

NOTE: Refer to the National Keyboard Delimiter Characters on page 29 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 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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.

NOTE: Refer to National Keyboard Delimiter Characters on page 29 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
-	BHCMSS*	-	Hungarian	-	Spanish
/	Brazilian	-	Italian	/	Swedish/Finnish
/	Chinese	/	Japanese	-	Swiss
-	Czech	/	Korean	/	Taiwanese
-	Danish	-	Latin American	/	Thai
!	French	-	Norwegian	.	Turkish
é	French Canadian	-	Polish	/	U.S. English
-	German	-	Portuguese		

* For Bosnia-Herzegovina, Croatia, Montenegro, Serbia, and Slovenia

Clearing Passwords

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

If the system is equipped with an embedded security device, refer to the *HP ProtectTools Security Manager Guide* at 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

When one or more hard drives that support the ATA Security command set are detected, 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. On a cold boot, either the master or the user password may be used. On a warm boot, enter the same password used to unlock the drive during the preceding cold-boot. Users will have two attempts to enter a correct password. On a cold boot, if neither attempt succeeds, POST will continue but the drive will remain inaccessible. On a warm boot or restart from Windows, if neither attempt succeeds, POST will halt and the user will be instructed to cycle power.

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 and a temporary user 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

Cover Removal 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.

Table 11-2 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.

NOTE: These settings can be changed using Computer Setup. For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide*.

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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

   NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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.

NOTE: 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

   NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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 before the computer boots to the operating system to enter Computer Setup. Press Enter to bypass the title screen, if necessary.

   NOTE: If you do not press F10 at the appropriate time, you must restart the computer and again press F10 before the computer boots to the operating system 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*.

Cable Lock Provision

The rear panel of the computer (some models) 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*.

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.

NOTE: Support for Fingerprint Identification Technology varies by model.

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* 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 caution message when the normal range is exceeded, which gives you time to take action before internal components are damaged or data is lost.

CAUTION: A high temperature condition can result in damage to the system or data loss.

Index