HP Business Desktop BIOS

HP BIOS Philosophy

While many computers contain the same processor, chipset, operating systems, and software choices, the BIOS (Basic Input Output System) is one critical computer component that varies significantly in quality and features between competing vendors. The BIOS is the set of routines typically stored in read-only memory that enable a computer to load the operating system and communicate with the various devices in the computer, such as storage drives, keyboard, monitor, printer, and communications ports.

The HP BIOS is industry-standard compatible. Industry standards and de facto standards define most of the interfaces and components that comprise the HP BIOS design. The HP BIOS development, though, has always added value to the HP Business Desktop computer products. HP has a dedicated team of developers and testers focused on the BIOS to help resolve real-world customer problems. While industry-standard resolutions are always considered first when addressing a problem, many new technologies and customer circumstances are not easily addressed by current standards. In these situations, HP BIOS may contain value-add features and components that lack standardization. When appropriate, HP works within the industry and with partners to create standards for new and evolving BIOS functionality.

One of the most critical benefits to customers is that HP can quickly enhance or modify BIOS designs to meet critical customer requirements, unique configurations, and deployment schedules. By maintaining HP's own BIOS code, it can eliminate the delays and costs associated with relying on a third-party vendor to make changes. HP's BIOS code has been maintained internally since the original Compaq PC - in fact, Compaq invented the first "clone PC" and IBM PC-compatible BIOS.

All HP BIOS designs undergo a rigorous quality assurance process, which includes internal verification and independent compatibility testing. Internal test teams exhaustively test for compatibility with industry and de facto standards (refer to Testing on HP Business Desktop PCs, a white paper, at www.hp.com). External test certifications, such as Windows Hardware Quality Labs (WHQL), help assure the customer that the HP Business Desktop computers' BIOS meets industry partner's testing criteria. HP participates in major industry interoperability test events, which allows third-party hardware and software providers to evaluate their products with the latest HP computer designs. This participation is extremely valuable in helping to ensure that the HP BIOS is compatible with new and emerging technologies. HP customers reap the benefits of smoother computer deployment and fewer compatibility issues.

This paper highlights many of the features, value-add capabilities, and enabling technologies incorporated into the HP BIOS. Each category will be examined to reveal how HP provides BIOS solutions for customer needs. HP BIOS features vary by model and system configuration. Some features may not be included on all models.

HP Business Desktop BIOS Features

This paper provides an overview of the features provided or enabled by HP Business Desktop BIOS. It explains how HP's BIOS solutions for Business Desktops address the following customer concerns:

- Deployment and manageability
- Stability
- Security
- Thermal and power management
- Serviceability
- Upgrades and recovery

Deployment and Manageability

The HP BIOS provides several technologies that help integrate the HP Business Desktop computer into a corporate enterprise. More detailed information, including customer success stories, can be found at the http://www.hp.com/go/im.

Installing a new computer

The HP BIOS supports Preboot Execution Environment (PXE). PXE is an industry-standard method of booting a computer to a network server, which provides remote management features such as initial operating system deployment and configuration. With PXE support, a new computer can be installed into a networked environment without using CD-ROMS or boot diskettes—the computer can simply download an image for installation over the network. In addition, the emergency boot function allows a computer to boot to a network image, in the event that the local operating system or storage has been compromised. The PXE environment can also allow an HP computer that is configured without local storage to boot to a network image for normal user operation (similar to a thin client deployment). The HP BIOS allows PXE boot devices to be added to the boot sequence either locally or remotely (for example, boot to CD–ROM, then diskette, then PXE). The HP BIOS enables the computer to be set up anywhere in the networked enterprise without having an IT support person present.

It is often desirable to configure the BIOS settings on a large batch of new computers before the OS is deployed. Rather than manually entering F10 setup to make the desired changes on each computer, an HP BIOS utility called Replicated Setup (REPSET.EXE) is available to automate this procedure. Replicated Setup runs in a DOS environment and can be configured in a DOS image that can be downloaded via PXE, or loaded from a bootable diskette, CD, or USB storage device. Replicated Setup requires a text file (CPQSETUP.TXT) containing a list of BIOS settings. This file is easily created from one computer on which the configuration is originally built using F10 setup. This text file is human-readable and can be edited by the administrator, if desired. After the file is created, the administrator simply runs the utility and associated text file from the chosen media. Assign Password is an associated utility designed to attach a password to the Replicated Setup utility. This is necessary if the computer already has a setup password in place. If a setup password is not in place when Replicated Setup is run, a password can be set as part of the replicated settings. (The Business Desktop BIOS Utility for Replicated Setup SoftPaq contains these tools and additional information at http://h18007.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.)

Remote computer configuration

The HP BIOS enables the network administrator to perform some functions over the network instead of manually. In this way, the administrator can control HP Business Desktop computer configurations throughout the enterprise from one central location. All the administrator has to do is download the utility along with the text file to the client for remote execution.

Similar to the Replicated Setup utility, the BIOS settings can be deployed throughout the enterprise under the OS by using System Software Manager SSM (http://www.hp.com/go/ssm). SSM software provides the GETCONFIG.EXE utility, which is used to create a CONFIG.TXT (a BIOS settings file similar to CPQSETUP.TXT). As with the Replicated Setup text file, the configuration settings can be edited for the desired changes and then deployed across the enterprise.

New systems, starting with the HP Compaq dc7600 and HP xw4300 Workstation, support a new manageability interface called HP Client Manager Interface (or HP CMI for short). HP CMI is built into the BIOS and provides, via WMI (Windows Management Interface), the ability to read or change BIOS settings, read supported sensor events, or receive alerts. Since it is built into the BIOS, HP CMI is an agent-less interface that can't accidentally be deleted from the system. Any management console or scripting facility that can connect to WMI can use the HP CMI interface, either locally or remotely. Some older HP systems will be supported by a WMI software provider that will emulate the native BIOS HP CMI support. Details of the interface are provided in a separate white paper *Managing and*

Monitoring BIOS Configuration Settings via HP Client Management Interface. Example VB scripts will be provided on hp.com in SoftPAQ SP29792.exe.

There is also a new tool for making BIOS settings locally from a Windows OS environment: HP BIOS Configuration for Protect Tools. This tool is supplied as a plug-in for HP Protect Tools.

Once the desired configuration has been established, the system administrator can enable the HP BIOS to store these settings as the computer default settings. With this capability, the administrator can establish the default settings for all HP Business Desktop computers remotely. If for some reason the BIOS settings are lost on a computer, these custom defaults will be restored by the BIOS instead of the BIOS defaults as they shipped from the factory. Factory default settings can be restored if a problem occurs.

Remote problem alerts and reaction

The HP BIOS adheres to the Alert Standard Format (see ASF standards at http://www.dmtf.org/standards/asf/) specification to provide advanced warning and system failure alerts from managed clients to remote consoles. ASF provides methods for sending failure/status information to remote consoles and receiving instructions from remote consoles in Pre-Boot, Boot, and OS unavailable states. This standard helps ensure the interoperability of HP Business Desktop computers with alerting and corrective-action software and devices from other vendors. The HP Business Desktop computer will issue heartbeat (indicates the computer is running fine), temperature problem, fan failure, chassis intrusion, boot failure, memory failure, and processor failure alerts. The BIOS will also accept remote ASF requests to restart, shutdown, or wake up the system over the network. The HP BIOS allows remote ASF messages to override the boot order—remote ASF messages can be used to force the HP Business Desktop computer to boot to PXE, CDROM, or hard disk ahead of the default boot order. Past remote alerting solutions have often been proprietary to the network controller manufacturer. With ASF support, the HP BIOS provides industry-standard alerts that can be monitored by any ASF-compatible software console. On new systems, starting with the HP Compaq dc7600 and HP xw4300 Workstation, alerts can also be received via WMI with the new HP CMI interface. A local alerting utility called *HP Client Management Interface Monitor* will be provided in a SoftPAQ at.www.hp.com.

Remote computer inventory

The HP BIOS provides firmware support for tracking assets through the System Management BIOS Specification standard (see SMBIOS standards at http://www.dmtf.org/standards/smbios/). This functionality provides asset control management tracking ability with HP Systems Insight Manager or other management software products. Detailed computer information concerning the BIOS, processor, memory, communications port, and much more can be obtained remotely across the enterprise. The BIOS is programmed in the HP factory with a unique asset tag/serial number that can be utilized or updated with a customer-specific tracking number of up to 18 alphanumeric characters. With the HP BIOS management feature set, the HP Business Desktop computer can be integrated into the enterprise environment and operated with standards-based management asset tracking software. The HP BIOS provides rich physical asset protection features such as: chassis cover removal alerting, chassis locking, and configuration change alerting. Detailed information is available in the Asset Tracking and Security section of the Desktop Management Guide on the *Documentation CD* that shipped with the computer. On new systems, starting with the dc7600 and xw4300, inventory information can also be pulled via WMI with the new HP CMI interface.

Remote computer control

The HP BIOS provides wake and power-on functions to enable remote system control for management and software maintenance. Remote wakeup features allow the HP Business Desktop computer to be remotely powered on, restarted, or powered off by a system administrator. The HP BIOS also allows the system to be configured for regular, unattended power-up—the unit can be powered on at a specific time and day of the week. These features can be controlled enterprise wide and remotely

configured through the BIOS setup replication utilities. The HP BIOS also allows the system administrator to control the unit once a remote wakeup has been issued. The unit can be configured to boot normally to the local mass storage subsystem or immediately boot to a predetermine network server. The HP BIOS wake and power-on features enable the system administrator to schedule software distribution, security updates, information inquiries, or remote ROM updates when the computers are not being used. The HP BIOS enables the computer to respond quickly to a power resume and/or wake from low power states such as Suspend to RAM (S3) and power off. An HP Business Desktop computer responding to a remote wakeup event from Suspend to RAM normally reinitializes the operating system in approximately 2 seconds.

Power failures or brownouts can often leave computers in an unknown state. The HP BIOS allows the system administrator to configure the HP Business Desktop computer to react in a predictable manner once power is restored. The system can be configured to remain powered off, power up immediately, or remain in the power state preceding the brownout event. This feature helps ensure that HP-BIOS-enabled units will continue to be able to communicate with the enterprise network management system when adverse power conditions are resolved. HP Business Desktop computer systems can continue to respond to remote wakeup LAN messages once power has been restored.

Multilanguage support

The HP BIOS computer setup utility, F10 Setup, provides robust localization support for global enterprise computing (see the Computer Setup (F10) Utility Guide on the *Documentation CD* that shipped with the computer). HP Business Desktop computer products can be deployed throughout a global enterprise without having to update the BIOS language or install a geography-specific version of the BIOS. The setup utilities are included with the HP BIOS to provide a single, global BIOS deliverable supporting the following 12 languages:

- English
- French
- Spanish
- Norwegian
- Finnish
- Italian
- Dutch
- Swedish
- Japanese
- German
- Portuguese
- Danish

Booting from various media

The HP BIOS can load the operating system from various media types. Beyond the traditional capabilities of booting from diskette, ATA and SATA mass storage devices, ATAPI CDROM, and network controllers, the HP BIOS also offers the option of booting from various USB mass storage devices including:

- USB Flash Drives
- USB CDROM and DVDROM Drives
- USB Hard Drives
- USB Floppy Drives

Boot sources can be controlled either locally or remotely through the BIOS setup replication utilities. Boot sources can also be disabled by the system administrator for specific customer security requirements.

Stability

The HP BIOS development team understands the needs of enterprise customers. Each year, new products are introduced at a rapid pace. New technology can improve productivity, but business environments also need stable technology and computers that can be trusted to work in their existing enterprise environment.

Minimizing changes to stable products

Companies carefully evaluate and test potential business products. Significant time and money can be required for the development of one or two computer models and software images for an organization. Given the rapidly changing computer market, the length of time required to evaluate a platform could result in that model not being available as originally tested when orders are ready to be placed or only being available for only a short time. As a critical component of the HP Business Desktop computer, HP strives for BIOS stability for the "Stable and Consistent" class of HP Business Desktop computer products (the dc series). These products assure customers that the computer hardware and software image will be stable for at least 12 to 15 months (depending on model and region).

As a critical component of the stability strategy, the HP BIOS is tightly monitored by version control software. BIOS versions used in the factories to produce the HP Business Desktop computer products are only updated for critical changes. Strict rules govern the BIOS changes that are approved and introduced into production versions. Normal problem fixes and updates are made available on www.hp.com and can be tested and deployed by customers when they deem it appropriate.

In some cases, processor changes initiate BIOS revisions. Many processor technologies require the addition of microcode updates (sometimes called 'patches') to the BIOS for proper functionality. The HP BIOS has developed a flash delivery method in which new microcode patches can be added to the BIOS without altering the core functionality. With this capability, the HP factory will load the appropriate microcode update to the existing stable BIOS image. Since the BIOS remains on an already tested version, business customers experience no impact to their software image by adding only the microcode patches required to an already tested BIOS version.

HP works closely with all chipset and processor vendors to minimize hardware changes and prevent any potential impact to customer's software images or environment. HP BIOS fully supports Intel's Stable Image Platform Program (SIPP) as part of this process. Image and BIOS stability is a fundamental concern in decisions made regarding BIOS contents, testing, and deployment.

BIOS change notification in advance

Critical BIOS changes for stable and consistent products that must be introduced into the factory are preceded by a Product Change Notification (PCN) approximately 30 to 60 days prior to the update for all the computers affected. This allows customers to plan for any impending BIOS changes. Customers can register on the PCN website at http://www.hp.com/go/pcn for specific computer notifications.

Security

Information security is critical to any business. Securing the computer environment is a prime concern in order to protect valuable information. The HP BIOS helps provide and enable several security technologies to assist the business customer in protecting sensitive company data.

A security model may be divided into several parts:

- Physically securing parts of the computer
- Enabling user trust in the computer
- Enabling computer (administrator) trust in the user

Out of this general model, a set of security policies will usually be put in place to adapt this model to the specific needs of each organization. This allows the proper balance between security and ease of use. The HP BIOS plays a vital role in enabling each part of the security model and has the flexibility to let the system administrator develop an effective set of security policies for their organization.

In order for the administrator to trust the user, the administrator must trust that the user's platform can prevent unauthorized access (authentication) and unauthorized changes to the established trusted platform state. Likewise, in order for the user to trust the administrator, the user must also trust that the platform can prevent unauthorized access (authentication) and unauthorized changes to the established trusted platform state.

Thus, both the administrator and the user must trust the platform to be secure. The HP BIOS security features work equally well to assure trust in the platform for both the user and the administrator. The following table lists possible attacks on a computer and how the HP BIOS security features help protect the system.

Computer Attacks	
Attack	**BIOS Enabled Security Features**
Subversion of OS security by booting rogue OS.	Removable media boot disable. Network Service Boot —> Boot Source Network Service Boot —> Disable Boot Order —> Device Disable DriveLock (for MultiBay HDD) IDE/SATA controller —> Disable USB port —> Disable Power-on Password Longhorn Secure startup support*
Removal of Sensitive Data	I/O port —> disable IDE/SATA controller —> Disable DriveLock (for MultiBay HDD) Diskette Write Protect TPM support Longhorn Secure startup support*
Removal of hardware devices	Hoodlock Control
Computer startup by unauthorized users	Power-on Password User Smart Card TPM Preboot Authentication
Attacks on BIOS Settings	Setup Password Administrator Smart Card
Flash of rogue computer BIOS image	Setup Password Administrator Smart Card TPM/TCG BIOS metrics

Securing trust

Each time the user turns on the computer, they need to know that the computer will function predictably and reliably. The user also needs to know that no one has tampered with their sensitive data. The system administrator wants to be assured that unauthorized changes are not made to the computer configuration, even by individuals with user authorization.

The installed operating system (OS) probably provides some security functions designed for this purpose, but, as the next section describes, this is not enough.

Preboot security is vital to OS security

Since the computer BIOS is the first operation to run at startup (pre-OS boot or preboot) and ultimately controls which operating system software is loaded, BIOS preboot security is a vital link in total computer security. Without BIOS preboot security, it is not difficult to subvert the security of the installed operating system by booting to a different OS on removable media (such as CD, diskette, USB key, etc). When a rogue OS is started on removable media, instead of the installed OS, the security policies of the installed OS are not in force. This gives an unauthorized user (hacker) the ability to examine and potentially compromise any data or stored security policies of the computer. Tools such as *ERD Commander* exist just for the purpose of bypassing OS security and manipulating OS security settings.

Installing a power-on password might be sufficient for the user to trust that no one else has accessed their computer. However, to satisfy the system administrator that not even the owner of the power-on password can boot from removable media, the system administrator can use the BIOS preboot security features to select which devices are bootable. This can effectively prevent undesirable OS loads from removable media (such as diskette or USB external devices). In addition, computer I/O ports can also be locked down and hidden. In the hidden state, no program has access to these ports, **not even the operating system**. This can help prevent unauthorized removal of sensitive data.

Certain new systems (dc7600) also have a BIOS and hardware that will support the Secure Startup feature of the Microsoft Longhorn OS. Secure startup used the TPM, BIOS TCG metrics, and logic in the OS loader to lock the boot partition to the specific machine and known copy of Longhorn.

User authentication

The HP Business Desktop BIOS supports five different user credentials:

1. **Setup password**—Sometimes called the administrator password, controls updates to BIOS options (F10 setup) and BIOS configuration and can be used in place of the power-on password to boot the computer (administrator authentication)
2. **Power-on password**—controls booting into the Operating System (user authentication)
3. **Two-Level DriveLock password**—controls access to HDD contents using industry-standard ATA security features on supported hard drives and drives installed in MultiBay slots. This password may be set to match the power-on password, in which case the BIOS will automatically unlock the HDD using the power-on password typed by the user. NOTE: DriveLock is only supported on hard drives and Multibay drives that provide the ATA security features.
4. **User Smart Card**—When enabled, takes the place of the power-on password
5. **Administrator Smart Card**—Takes the place of the setup password
6. **TPM Preboot Authentication**—Uses the TPM to authenticate the user via TPM user credentials

Securing the Trusted Platform State (TPS)

Administrator authentication is enabled by setting a setup password or by creating an administrator smart card. Administrator authentication provides controls over important BIOS functions and security policies. HP recommends that a company's IT department establish administrator authentication on all machines to control all changes to the BIOS. The IT department can establish a common, organization-wide setup password or administrator smart card credential to provide easy access to all machines by system administrators.

If no setup password or administrator smart card is established, then administrator authentication is disabled, and anyone or any program can change BIOS settings and anyone can make BIOS flash upgrades. A few security policy settings, however, cannot be enabled without first enabling administrator authentication.

The first feature of administrator authentication is that it can override user authentication (see below). This allows administrators access to a machine even if the user has a user smartcard, power-on password or TPM preboot authentication set and the user forgets the password, or does not have the user smart card, or the administrator needs access to the machine in the user's absence. The setup password can be entered at the password prompt in place of the power-on password, or the administrator smart card can be inserted at the smart card prompt in place of the user smart card.

Administrator authentication also protects BIOS flash upgrades. If the setup password is set, the BIOS cannot be upgraded without providing that setup password or an administrator smart card. This helps the administrator maintain a common BIOS image and prevent undesired upgrades.

All other BIOS configuration settings, including security policies, are also protected by administrator authentication. This includes all settings in F10 setup, except the time and date. The time and date is the only function that is allowed to be changed without administrator privileges. By default, all BIOS settings are protected by administrator authentication even while the OS is running. As a security policy option, the administrator can set the BIOS to allow the OS to change legacy resources even when administrator authentication is enabled. BIOS administrator authentication also protects setting made via the new HP CMI interface. BIOS settings made via HP CMI are also protected by the normal OS administrator rights and WMI security policies. For example, remote access to WMI settings can be disabled from within Windows.

Securing the BIOS flash

The computer BIOS image is stored in a nonvolatile memory device on the motherboard known as flash memory. In order for the computer to start and run correctly, this flash memory must contain a valid BIOS image. The image in the flash memory may be reprogrammed from time to time to update the BIOS version. Virus software, such as the Chernobyl virus, has been able to corrupt nonvolatile memory, including flash memory, on some computers. When this happens, the computer motherboard may have to be replaced because the computer may not be able to restart. The HP BIOS uses hardware mechanisms on most HP Business Desktops to prevent access to the BIOS flash memory by any software other than the BIOS. This hardware traps any attempts to update the flash memory that do not originate from the BIOS itself.

BIOS images that work with HP Windows-based BIOS update tools (flash tools), such as HPQFlash and SSM, contain a digital signature that allows the flash tools to authenticate the BIOS image. This ensures that the image originated from HP and has not been corrupted or tampered with in any way.

As mentioned earlier, administrator authorization allows the system administrator to control all BIOS image updates.

BIOSes on select newer products also now support TCG (Trusted Computing Group) BIOS metrics. This is an industry standard method of measuring the BIOS and OS bootloader and storing the measurements securely in the TPM (Trusted Platform Module). For more information on the TPM, see white paper *HP ProtectTools Embedded Security Guide*. Software can then detect if the BIOS image changes in any way.

Securing startup

The power-on password, user smart card, and TPM preboot authentication functions as a user authentication and boot access control mechanism. If this password is set or either smart card or TPM preboot authentication is established, the user will be prompted to enter this password or smart card on each startup and optionally on each restart. The startup process is halted if the correct password or smart card is not entered. TPM preboot authentication uses the TPM user credential (passphrase) to authenticate the user.

Device boot control is a series of settings that control which devices can be booted and in what order. This feature is important to prevent subversion of the installed OS as described earlier. The settings in this category are

1. Network Service Boot (enable/disable)
2. Removable Media Boot (enable/disable)
3. Remote Wake Boot Source (controls which device will boot on wakeup)
4. Boot Order (controls which devices can be booted and in what order)
5. USB port and mass storage controller disable (mentioned earlier)
6. DriveLock

Securing portable data

Computers that contain mobile technology hard disk drives used in MultiBay slots can protect the data on those drives with a DriveLock password. The password is stored on the drive and the drive firmware controls access so that the DriveLock security goes with the drive, not the platform. Each time the computer is restarted, the drive will remain inaccessible until the DriveLock password is provided. This drive locking mechanism is an industry standard (ATA–5).

It is recommended that the system administrator establish a master DriveLock password on each drive and then allow the user to establish the user DriveLock password. This is the only way to recover a drive if the DriveLock password is lost. The master DriveLock password provides a mechanism to clear the user DriveLock password, if it is forgotten. **Otherwise, the drive is rendered useless and all data will be lost.**

As a convenience to the user, the DriveLock password and power-on passwords (or smart card credentials) can be set to match. In this case, the BIOS will use the Power-on password or smart card credential to unlock the drive for the user without additional prompts. For the sake of security, there is no copy of the DriveLock password permanently stored in any fashion in the BIOS. Of course, if the power-on password and DriveLock passwords are set to match, then an encrypted version of the DriveLock password is contained in the BIOS, since the power-on password is stored in the BIOS flash memory. For this reason some users may choose to make their DriveLock password different from the power-on password.

Smart cards

Using smart cards for user or administrator preboot authentication provides one of two benefits: ease of use or multifactor authentication. In addition, the same smart card can hold OS user credentials.

If the administrator has enabled the use of smart cards in BIOS setup, the smart card will replace the typed-in passwords. BIOS administrator authentication and user authentication are handled with two separate smart cards: the user smart card and the administrator smart card. If smart cards are enabled, the administrator smart card must be enabled first. After enabled the administrator smart card, enabling the user smart card is optional.

When enabling the smart cards, the administrator has the choice of enabling multifactor authentication, which requires a PIN (Personal Identification Number, a 4- to 10-digit number required to enable smart card access), or single-factor authentication, which does not require a PIN. Single-factor authentication is more convenient (only requires possession of the card), while multifactor authentication is more secure (requires possession of the card and knowledge of the PIN). If single-

factor authentication is selected, the smart card could be stolen and an unauthorized person might gain access to the machine.

Each smart card holds a BIOS passphrase as its credential. This BIOS pass phrase is a string of up to 32 characters. This pass phrase can be chosen by the administrator or a random 32-byte value can be generated by the smart card tools. The administrator may configure the computer so that the DriveLock passwords are established by using the smart card pass phrases. In this case, the smart card pass phrase will automatically be used to unlock the drive during startup.

Preventing unauthorized data removal

Device security is a feature that uses either chipset or motherboard hardware to hide I/O (input/output) ports from the OS or disable mass storage controllers or devices. When hidden, the selected ports are not accessible to the OS or any other software. Only the BIOS can re-enable these ports. This feature is useful for those that are concerned about unauthorized removal of sensitive data from the machine using these I/O ports. The ports that can be secured may vary by model, but generally include the serial port(s), parallel port, USB port(s), network connection, and audio.

The IDE and SATA controllers can also be disabled, preventing devices from functioning on these ports. In addition, the diskette controller can be set to disallow saving data to the diskette.

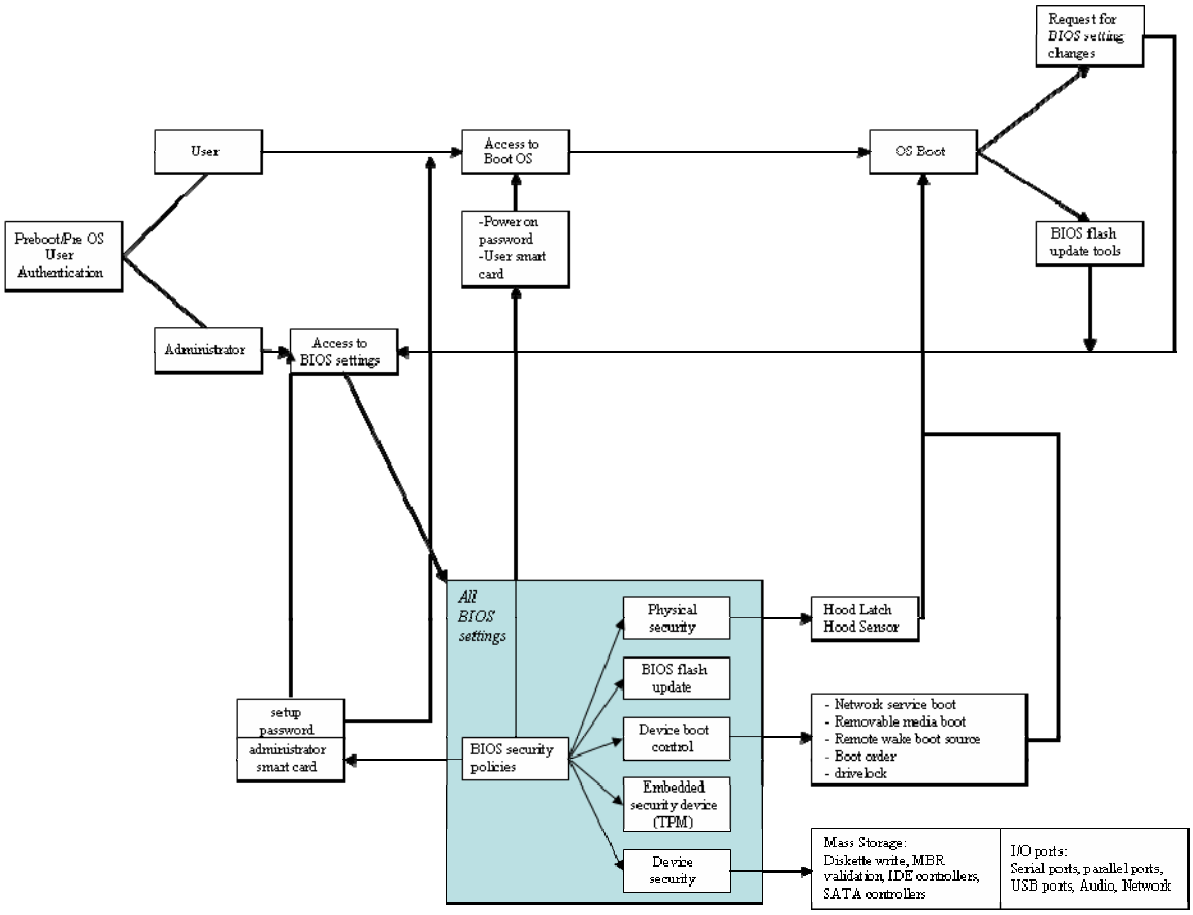
Physically securing the platform hardware

The BIOS provides control with two types of physical security: hood latch and hood sensor. The hood latch is an electronically controlled mechanism that locks the chassis hood. The hood sensor is a device that detects if the chassis hood has been opened or removed. The administrator has the choice of which security policy to enable if a hood sensor event should happen:

- Notify the user on the next startup that the chassis hood has been removed
- Require administrator authorization to continue the startup process
- Ignore any chassis hood removal

Figure 1. Overall BIOS security picture

The following diagram represents the various security levels and interactions enabled by the HP BIOS.



Thermal and Power Management

The HP BIOS provides and enables thermal and power management technologies to assist in operating the HP Business Desktop computer in any enterprise environment.

Balancing thermal and acoustic requirements

HP designs thermal solutions to help assure that the computer performs optimally in the customer environment. The HP BIOS actively controls the environment of the computer by balancing the thermal requirements of the configuration and the acoustic levels of the computer. With today's faster and hotter processors, thermal management becomes paramount. If the processor becomes too hot, it may "throttle" (slow down) the computer until the temperature decreases. Throttling involves reducing the performance of the processor significantly during periods of elevated temperatures. The HP BIOS automatically manages the air flow in the computer to minimize elevated temperatures that could lead to thermal throttling.

The HP BIOS, by default, optimizes the acoustic characteristics of the computer while providing complete protection for the hardware thermal needs. Some customers may wish to control the computer airflow in their computers manually. The HP BIOS allows the user or administrator to configure the nominal fan speed to best suit the work environment. Air flow can be maximized for environments where thermal concerns are most important or minimized for acoustically sensitive

environments. However, the user configurable speed does not compromise the thermal protection over the computer environment. The HP BIOS will adjust air flow to necessary levels when computer conditions require additional cooling regardless of the user settings. Through careful analysis and testing, the HP BIOS minimizes unnecessary fan noise for better idle acoustics and meticulously controls fan ramps to prevent overheating with smooth fan speed transitions.

The HP BIOS also provides thermal alerts to remote management consoles when the computer temperature rises to cautionary or critical levels. With this information, system administrators can adjust computer settings or environmental conditions to eliminate thermal concerns before they become real problems. Combined with the HP Business Desktop computer thermal hardware and cooling components, the HP BIOS plays an active and key roll in controlling the thermal environment and acoustics for a better overall Total Customer Experience (TCE).

Saving power and money

Power cost and consumption are important concerns of the business client. The HP BIOS provides robust power management functionalities and can help address these concerns. Using the industry-standard Advanced Configuration and Power Interface Specification (see ACPI specifications at http://www.acpi.info/spec.htm), the HP BIOS enables the operating system to control the computer's power level safely and efficiently. The HP BIOS helps the business customer safely enable lower power management states. This functionality allows individual subsystems and peripherals to enter low power or off states without affecting other elements of the system.

The HP BIOS offers a wide range of configurable power management options to meet the customer's unique needs. The ACPI defines several system states described below, all of which HP supports:

- S1—Standby state resulting in the processor being halted, but context is not lost. All other devices remain at the normal power state. This state offers the fastest wakeup time and the lowest power savings.
- S3—Standby state known as Suspend to RAM. All devices in the system are powered down, except for computer memory. Recovery is almost instant (approximately 2 to 3 seconds) and power consumption is very low (typically <5W).
- S4—This state is referred to as Hibernation. The computer's memory content is saved to the hard drive, then most power is removed from the system.
- S5—This state is often referred to as Soft Off. The computer is off. This state offers the slowest wakeup time and the greatest power savings (typically <2W).

To understand the cost savings, consider an example using the power difference between enabling Suspend to RAM (system power dissipation is under 5W) versus simply allowing a system to idle (system power dissipation is approximately 90W in a mainstream Pentium4 configuration). In this scenario, assume users simply let their system idle when they are not working. Calculate the cost savings during after-work hours (5pm to 8am) in an enterprise with 1000 systems. Saving approximately 80W for 15 hours/day at an average energy cost of 12 cents/kWh, for an average work year of 250 days, would result in a cost savings of $36,000.00 annually for an installation of 1000 systems.

Typically, computer users will also not power off their systems at the end of the work day due to the inconvenience of waiting for the system to power up and complete the initial loading of their operating system. In the Suspend-to-RAM state, HP Business Desktop computers are instantly available. Users can touch the mouse, keyboard, or power button and have the unit ready for interaction in approximately 2 seconds.

The HP BIOS has also been a key component in achieving power management accreditations such as Energy Star, Blue Angel, and Federal Energy Management Program (FEMP) Standby Power compliance (refer to http://www.eere.energy.gov/femp for more information on the FEMP). Both the software image (operating system and applications) and the HP BIOS provide a cohesive power

management environment that is fully tested and robust. Helping to lower power costs, improve user convenience, and increase product durability are all positive Total-Cost-of-Ownership (TCO) impacts of the HP BIOS.

Enabling future power savings

HP BIOS engineers are working constantly with partners such as Intel and Microsoft to help ensure that HP Business Desktop computer designs will enable the latest processor and operating system thermal and power management technologies. The HP BIOS also provides runtime power management for some configurations that support processor throttling of frequency and voltage during situations where the operating system detects excess computing capability for the tasks it needs to perform. Runtime power management involves lowering the processor's power requirements when the computer is not executing processor intensive activities. The computer is completely on and responsive to the user, but, when the processor is not fully engaged, it can be throttled to save up to 40% power consumption without affecting the user's productivity. Typically, this feature is available in high performance processors. These computers can dissipate system power, up to 90W idling at normal operating frequency and voltage and significantly more in the working state. The runtime power management feature can save tens of KWHs per machine per year without sacrificing computing performance.

Serviceability

Unplanned downtime can be extremely costly to any business. The HP BIOS can play a key role in the serviceability of the HP Business Desktop computer. Constant feedback from customers and field service personal is integrated into each successive HP BIOS family, resulting in improved serviceability and customer satisfaction. Some of the serviceability features in the HP BIOS are problem diagnosis and resolution and detailed service information

Problem diagnosis and resolution

HP Business Desktop computers, designed with the HP BIOS, provide information to aid the user in diagnosing problems. Visual alerts are produced by blinking the power LED light red instead of the normal green color. Audio beep alerts are supported on computers containing a computer speaker. These alerts allow the user, administrator, or service technician to diagnose problems quickly at the component level and take effective action onsite. Issues can be diagnosed correctly the first time to avoid random replacement of computer components and costly computer downtime. See the Troubleshooting Guide on the *Documentation CD* that shipped with the computer for more information. Problem alerts are provided for the following failures:

HP BIOS Diagnostic Codes

Problem	Computer Reaction
Processor Thermal Protection Activated	Power LED blinks RED 2 times, one every second, followed by a 2-second pause.
Processor not installed (not an indicator for a bad processor).	Power LED blinks RED 3 times, one every second, followed by a 2-second pause.
Power Failure (power supply is overloaded)	Power LED blinks red 4 times, one every second, followed by a 2-second pause.
Pre-video Memory Error	Power LED blinks RED 5 times, one every second, followed by a 2-second pause. Also 5 simultaneous beeps will be heard.
Pre-video Graphics Error	Power LED blinks RED 6 times, one every second, followed by a 2-second pause. Also 6 simultaneous beeps will be heard.

HP BIOS Diagnostic Codes	
Problem	**Computer Reaction**
PCA failure (ROM detected failure prior to video)	Power LED blinks RED 7 times, one every second, followed by a 2-second pause. Also 7 simultaneous beeps will be heard.
Invalid ROM based on bad checksum	Power LED blinks RED 8 times, one every second, followed by a 2-second pause. Also 8 simultaneous beeps will be heard.
Watchdog timer alarm (no BIOS code being executed)	Power LED blinks RED 9 times, one every second, followed by a 2-second pause. Also 9 simultaneous beeps will be heard.

The HP BIOS extensive Power-On Self Test (POST) provides exhaustive error messages to inform the user or administrator when a computer failure has been detected. The POST is a series of diagnostic tests that execute when the HP Business Desktop computer is turned on. If an error is detected, the error notification displayed contains a brief problem description and recommended action, in most cases. Typically, HP Business Desktop computers are configured to execute a reduced set of POST tests to increase boot speed during normal power cycles. However, if a computer has been experiencing difficulty or the customer environment demands more stringent test requirements, F10 setup provides configurable levels of POST testing. The full complement of POST tests can be set to execute on every boot or once every 1 to 30 days. In addition, computer health information can be viewed by a system administrator using HP Client Manager Software (see http://www.hp.com/go/im for more information). Networked computers using HP Insight Manager, HP Client Manager, or other system management application can receive alerts for most error conditions from HP Business Desktop computers.

Detailed service information

The HP BIOS computer setup utility, F10 setup, is an extremely valuable service tool (see the Computer Setup (F10) Utility Guide on the *Documentation CD* that shipped with the computer). The System Information option provides detailed information including: product name, processor type/speed/stepping, memory configuration, integrated MAC address for enabled or embedded NIC, and asset tracking number. The F10 Setup Storage menu lists all storage devices controlled by the HP BIOS. Depending on device type, detailed information, such as type, model, firmware version, translation mode, transfer mode, and multi-sector transfer setting, is provided.

The Drive Protection System (DPS) tests option is also provided for devices that support this type of built-in self-test (see Drive Protection System, a white paper, at ftp://ftp.compaq.com/pub/products/desktops/whitepapers/DPSWhitePaper_092299.doc). The DPS is a valuable tool to help diagnose device problems that could result in unwarranted hard drive replacement. During factory configuration, each installed hard drive is DPS-tested, and the permanent record of test results is stored on the device itself. Results of each subsequent execution of the DPS test are stored on the hard drive and compared to the original factory results. Service providers can use this information to diagnose potential problems quickly and efficiently. During POST, capable drives are queried for health information, which can help predict some hard disk failures before valuable data is lost.

Upgrades and Recovery

The HP BIOS provides numerous ways to upgrade HP Business Desktop computers for the constantly changing enterprise environment. Each BIOS upgrade is packaged into a SoftPaq deliverable and made available on www.hp.com. The SoftPaq contains detailed instructions to perform BIOS updates in any of the available formats. The following sections provide a brief description of the various BIOS upgrade options and recovery mechanisms:

- Local BIOS update
- BIOS update while in Windows
- Remote BIOS update
- Fail-safe flash recovery

One key feature of all HP BIOS upgrade methods is that all system settings and user data is preserved. There is no need to 'set defaults' or re-configure settings as with some competing systems.

Local BIOS update

HP Business Desktop computer BIOS can be updated locally by using the F10 setup "Flash System ROM" feature. This flash utility offers the user the option of selecting the media containing the BIOS image file (7D1_MMmm.bin) provided in the SoftPAQ. The F10 ROM-based flash can accept the binary file from the root directory of any removable media such as USB, legacy floppy diskette, or CD. The selected media must have a formatted FAT16 or FAT32 primary partition containing the binary image. If a setup password has been established on the HP Business Desktop, that password must be used to enter the F10 setup utility and update the BIOS.

The DOS Flash (FLASHBIN.EXE) is the DOS-compatible flash utility that can be used from a DOS-bootable flash media device (1.44MB diskette or USB flash media device). To flash the computer BIOS locally, the SoftPaq provides a DOS Flash folder that can be copied to the media. As with the other BIOS upgrades, administrator security is available through the use of the setup password.

BIOS update while in Windows

HPQFLASH is a utility that is designed to flash the HP BIOS within a Windows environment. If the computer has a setup password enabled, then HPQFLASH will prompt for the password to be entered before completing the flash process. This utility is designed for business applications in which DOS images may not be available, users may not be comfortable in DOS environments, or security concerns prevent computers from booting to removable media.

Remote BIOS update

Many customer computer environments require strict control of BIOS versions. BIOS updates are only distributed after exhaustive testing has been completed. For these environments, the HP BIOS provides support for remote BIOS upgrades through several tools. The BIOS SoftPaqs can be delivered to remote computers as a self-contained upgrades using System Software Manager (SSM) to update the HP BIOS on appropriate computers on a network. Refer to http://www.hp.com/go/ssm for more information and for detailed instructions and downloads. The SoftPaq can also be distributed through HP Client Manager Software (HPCMS) and Altiris Notification Server to remotely target, distribute, and update the HP BIOS on network HP Business Desktop computers. The HP Client Management Solutions website (http://www.hp.com/go/im) contains information about this feature and other management options. DOS Flash (FLASHBIN.EXE) can also be remotely executed through Altiris eXpress. Remote BIOS updating is accomplished by executing the DOS Flash within the limited DOS extended environment that exists while running Altiris eXpress.

Fail-safe flash recovery

Regardless of the delivery mechanism, HP BIOS-based computers include a write-protected boot block ROM that provides recovery from a failed flashing of the computer BIOS. If the BIOS image fails the POST integrity test after being updated, the boot block code automatically executes, warns the user of the failure, and provides the minimum amount of support necessary to allow the HP Business Desktop computer to search removable media, such as floppy, CD, or USB flash devices, for BIOS image files. The system power LED blinks red 8 times, once per second, to indicate fail-safe flash recovery. Simultaneously, if the system is so equipped, the system speaker beeps 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. If the computer finds an appropriate BIOS image file, it is automatically flashed into the ROM.

Industry Standards

The HP BIOS is fully industry-standard compliant. In many situations, the HP BIOS has led in the formation of various standards. The following table shows some of the more common standards supported by the HP BIOS and HP's contributions:

HP BIOS Compatibility

Technology/Standard	Web Site	Standard's value to the product
Advanced Configuration Power Interface (ACPI)*	http://www.acpi.info/spec.htm	ACPI allows operating system controlled configuration and Power Management. This interface is necessary to fully unleash the power of Windows operating system products. HP provided early critical input to the specification and supplied on of the first ACPI hardware and BIOS capable computers to Microsoft for ACPI development in both Windows 98 and Windows 2000.
Alert Standard Format	http://www.dmtf.org/standards/documents/ASF/DSP0136.pdf	ASF defines method of sending notifications to the network when the computer does not successfully complete the POST or has an alert condition (chassis intrusion, processor failure, memory failure, or temperature alert) in a manner that can be monitored by remote consoles. Specification also defines remote control functions. HP is a contributing member of the DMTF group defining the evolution of this standard.
AT Attachment—7 with Packet Interface (ATA/ATAPI-7)	http://www.t13.org	ATA is the interface mostly used for storage device interface in most computers.
ATAPI Removable Media Device BIOS Specification	http://www.phoenix.com/NR/rdonlyres/EDD1AAA0-177E-4024-A0B1-E4BD06B673F7/0/specsatapi.pdf	This specification provides the BIOS interface for large capacity ATA removable ATA devices. HP co-authored the ATAPI specification.
BIOS Boot Specification	http://www.phoenix.com/NR/rdonlyres/56E38DE2-3E6F-4743-835F-B4A53726ABED/0/specsbbs101.pdf	The BIOS Boot Specification provides the user with increased flexibility in selecting the unit boot media order (diskette, hard drive, CD ROM, and third-party plug-in adapter controlled media). HP co-authored this standard.
BIOS32 Service Directory	http://www.phoenix.com/NR/rdonlyres/ECF22CEC-A1B2-4F38-A7F9-629B49E1DCAB/0/specsbios32sd.pdf	Provides a single searchable signature for BIOS services that are designed to be utilized by 32-bit BIOS clients.

HP BIOS Compatibility		
Technology/Standard	**Web Site**	**Standard's value to the product**
Desktop Management Interface (DMI)	DMTF: http://www.dmtf.org/home/ System Management BIOS Reference Specification: http://www.dmtf.org/standards/smbios/ DMTF Steering and Technical Committees: http://www.dmtf.org/about/list/	This specification defines how computers present management information so that management applications can obtain detailed configuration input without resorting to error-prone probing methods. HP is a founding member of DMTF and co-author the original DMI Specification, which is now known as System Management BIOS Reference Specification or SMBIOS. Current member of the DMTF Steering and Technical Committees.
Drive Self Test (DST)	DST: ftp://ftp.compaq.com/pub/products/desktops/whitepapers/DPSWhitePaper_092299.doc ANSI ATA/ATAPI–5 specification: http://www.t13.org/	HP developed the DST in collaboration with several leading hard drive manufacturers and it was standardized the industry standards body ANSI. The Drive Self Test was integrated as part of the ANSI ATA/ATAPI–5 specification.. HP enhanced the DST to give a user access to this self-test in F10 Computer Setup. This enhancement of the DST is called Drive Protection System (DPS).
El Torito CD–ROM Boot Specification	http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf	Standardizes information needed to make a CDROM bootable.
Enhanced Disk Drive Specification	http://www.phoenix.com/NR/rdonlyres/9BEDED98-6B3F-4DAC-BBB7-FA89FA5C30F0/0/specsedd11.pdf	Contributed to enhancements included in version 3.0 of the specification, which provided compatibility between fixed and removable media.
Multiprocessor Specification (MPS)	http://www.intel.com/design/archives/processors/pro/docs/242016.htm	Specification utilized to provide multiprocessor and computer configuration information.
Peripheral Component Interconnect (PCI)	PCI: http://www.pcisig.com/specifications PCI SIG steering committee directors: http://www.pcisig.com/membership/about_us/board_of_directors/	Defines methods for configuring PCI devices whether embedded or installed in expansion slots. The BIOS also supports the latest PCI Express technology, which is available on selected models. HP has been PCI SIG steering committee directors since the committee's inception, and has co-authored many versions of the specification.
Post Memory Manager	http://www.phoenix.com/NR/rdonlyres/873A00CF-33AC-4775-B77E-08E7B9754993/0/specspmm101.pdf	Defines a method for allocating RAM buffers to be used by option ROM configuration needs during POST.
Preboot Execution Environment (PXE)	ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf	Allows the BIOS to boot a system that has no operating system installed on its hard drive and to download the software from a server.
Serial ATA (SATA)	http://www.serialata.org/	Serial evolution of the ATA interface specification offering higher speed transactions and more efficient cabling for the desktop computer.

HP BIOS Compatibility		
Technology/Standard	**Web Site**	**Standard's value to the product**
SMART (Self Monitoring Analysis and Reporting Technology) hard drives	ATA/ATAPI specification: http://www.t13.org/	SMART is an early warning system for pending drive problems. HP led the development effort and co-authored the specifications for SMART hard drives, which became part of the ATA/ATAPI specification.
Trusted Computing Group (TCG)	https://www.trustedcomputinggroup.org/home	TCG develops security specifications for trusted computing components and software interfaces. HP is a founding member of the TCG committed to the enhancement of the secure computing environment.
Wired for Management (WfM)	ftp://download.intel.com/labs/manage/wfm/download/base20.zip	The Wired for Management (WfM) Initiative is an industry-supported effort to make systems easily manageable and universally managed in a network environment, without sacrificing agility or performance. This initiative enables products to be centrally managed over networks to reduce Total Cost of Ownership (TCO). HP co-authored the WfM specification.
Universal Serial Bus (USB)	http://www.usb.org/developers/docs/	This specification defines the software protocols and physical interface for the USB ports. HP co-authored the USB specification and has been shipping USB connectors on computers since 3Q96.
Advanced Configuration Power Interface (ACPI)*	http://www.acpi.info/spec.htm	ACPI allows operating system controlled configuration and Power Management. This interface is necessary to fully unleash the power of Windows operating system products. HP provided early critical input to the specification and supplied on of the first ACPI hardware and BIOS capable computers to Microsoft for ACPI development in both Windows 98 and Windows 2000.

* Most specifications are linked to their respective Web sites. Refer to this White Paper at www.hp.com to access the white paper URLs.

Summary

In summary, the HP BIOS is a valuable and innovative component of the overall system, designed with an understanding of the business customer's issues and requirements. The HP BIOS implements and enables many solutions for use in the business enterprise and can easily be adapted to meet individual customer needs. The HP BIOS has, and will continue, to champion new standards and technologies that provide value to the business customer.

For More Information

For more information about HP Business Desktop computers, visit our website at www.hp.com.

For the HP sales office nearest you, refer to your local phone directory, or call the HP regional office listed below.

Corporate and North American headquarters
Hewlett-Packard
3000 Hanover Street
Palo Alto, CA 94304–1185
Phone: (650) 857–1501
Fax: (650) 857–5518

Regional headquarters
Latin America
Hewlett-Packard
Waterford Building, 9th Floor
5200 Blue Lagoon Drive
Miami, Florida 33126 USA
Phone: (305) 267–4220

Europe, Africa, Middle East
Hewlett-Packard
Route du Nant–d'Avril 150
CH–1217 Meyrin 2
Geneva, Switzerland
Phone: (41 22) 780–8111

Asia Pacific
Hewlett-Packard Asia Pacific Ltd.
Hewlett-Packard Hong Kong Ltd.
9/F, Cityplaza One
111 King's Road
Taikoo Shing
Hong Kong
Phone: (852) 2599–7777

371246-002, 05/2005