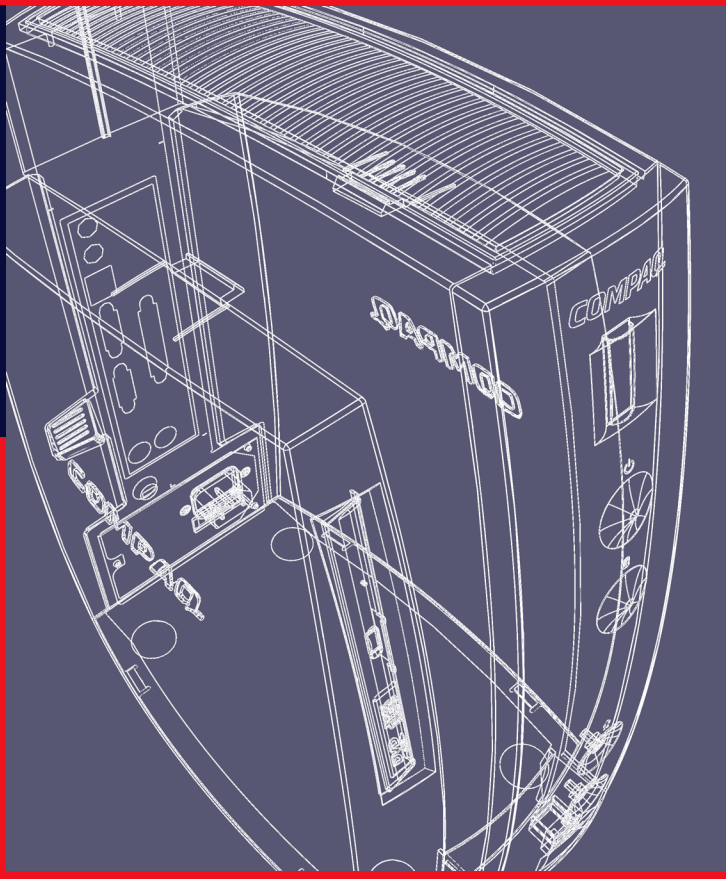
iPaq Family of Internet Devices

Desktop Management Guide



COMPAQ

Notice

The information in this guide is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

The following words and symbols mark special messages throughout this guide:

WARNING: Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

Desktop Management Guide

Compaq iPaq Family of Internet Devices

First Edition (January 2000)
Part Number 166764-001

Compaq Computer Corporation

CONTENTS

Desktop Management

DESKTOP MANAGEMENT

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

This guide summarizes the capabilities and features of the four key components of desktop management:

- Initial Configuration and Deployment
- Asset tracking and security
- Fault notification and recovery
- Software updating and management

The guide also contains an overview of the tools, utilities, and information Compaq provides to help you successfully deploy manageable desktop PCs and Internet Devices.

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

Initial Configuration and Deployment

Compaq iPaq Internet Devices come with a preinstalled system software image. After a very brief software "unbundling" process, the Compaq iPaq is ready to be used.

- Installing additional software applications after unbundling the preinstalled software image
- Using software deployment tools, such as Microsoft MS Batch or NT Distribution Share (NTDS), or Altiris eXpress to replace the preinstalled software with a customized software image
- Using a disk cloning process to copy the contents from one hard drive to another

The best deployment method depends on your information technology environment and processes. The PC Deployment section of the Solutions and Services Web site (www.compaq.com/im/change) provides information to help you select the best deployment method. You'll also find guides and utilities to integrate with Microsoft or PXE-based deployment tools.

Remote System Installation

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

- Deploying a software image on one or more new PCs or Internet Devices.
- Formatting a hard drive.
- Installing application software or drivers.
- Updating the operating system, application software, or drivers.

To initiate Remote System Installation, press F12 when the F12=Network Service Boot message appears in the lower-right corner of the Compaq logo screen. Follow the instructions on the screen to continue the process.

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

Altiris eXpress

Altiris eXpress allows the system administrator to create and quickly deploy a customized, corporate-standard software image across one or more networked client PCs with an interface as simple to use as Windows Explorer. Altiris eXpress supports Intel's Wired for Management and Preboot Execution Environment (PXE). Using Altiris eXpress and the Remote System Installation features of the Compaq iPaq, there is no need for the system administrator to visit each new PC individually to deploy the software image.

For more information, refer to the Compaq Web site at www.compaq.com.

PC Transplant

PC Transplant, designed to assist you in personalizing the new Compaq iPaq Internet Device, can be downloaded free from the Compaq Web site. It lets you preserve the "personality"—the customized settings such as Start menu entries, drive and printer mappings, software application options, and so on—of an existing PC, then transfer those unique settings to the Compaq iPaq so that you don't have to invest valuable time manually recreating them.

For more information, refer to the Compaq Web site at www.compaq.com.

Asset Tracking and Security

Compaq AssetControl features incorporated into the Internet Device provide key asset tracking data that can be managed using Compaq Insight Manager products and Management Solutions Partners products. Seamless, automatic integration between AssetControl features and these products enables you to choose the management tool that is best suited to your environment and to leverage your investment in existing tools.

Compaq Internet Devices are manufactured with the hardware and firmware required to fully support the DMI 2.0 standard.

Compaq also offers several solutions for controlling access to valuable Internet Device components and information. Security features such as the Memory Change alert, power-on password, and setup password help to prevent unauthorized access to the internal components of the Internet Device. By disabling parallel, serial, or USB ports, or by disabling removable media boot cabability, you can protect valuable data assets. Memory Change alerts can be automatically forwarded to Compaq

Insight Manager products to deliver proactive notification of tampering with the internal components of the Internet Device.

There are three ways to manage security settings on your Compaq Internet Devices:

- Locally, using the Compaq Computer Setup Utilities. See Chapter 1, "Computer Setup Utilities" in the *Reference Guide* on the *Compaq iPaq Reference Library* CD for more information and instructions.
- Remotely, using the Compaq Remote Security Management software. This software enables the secure, consistent deployment and control of security settings from a central point on the network using a third-party PC LAN management application such as Microsoft SMS.
- Remotely, using Compaq Insight Manager LC, a tool for managing PC workgroups.

The following table and sections refer to managing security features of your Computer locally through the Compaq Computer Setup Utilities. Refer to the Remote Management Setup Utilities for more information on using the Remote Security Management software. These utilities are available on the Compaq Web site at www.compaq.com/support/files/index.html. For more information on Insight Manager LC, refer to www.compaq.com/im/lc.

Security Features Overview

Feature	Purpose	How It Is Established
Removable Media Boot Control	Prevents booting from the removable media drives.	From the Compaq Computer Setup Utilities menu.
Serial, Parallel, or USB Interface Control	Prevents transfer of data through the integrated serial, parallel, or USB (universal serial bus) interface.	From the Compaq Computer Setup Utilities menu.
Power-On Password	Prevents use of the Internet Device until the password is entered. This can apply to both initial system startup and restarts.	From the Compaq Computer Setup Utilities menu.
Setup Password	Prevents reconfiguration of the Internet Device (use of the Computer Setup utility) until the password is entered.	From the Compaq Computer Setup Utilities menu.
DriveLock Security	Allows a MultiBay hard drive to be locked, preventing unauthorized access to data stored on the drive. **CAUTION:** A MultiBay hard drive can be rendered permanently unusable if the DriveLock security feature is enabled and the password is forgotten. Be sure to read the "DriveLock Security" section of this guide prior to using the DriveLock security feature.	From the Compaq Computer Setup Utilities menu.
Memory Change Alerts	Detects when memory modules have been added, moved, or removed; notifies end-user and system administrator.	For information on enabling Memory Change Alerts, refer to the online *Intelligent Manageability Guide*.
Ownership Tag	Displays ownership information, as defined by the system administrator, during system startup (protected by setup password).	From the Compaq Computer Setup Utilities menu.
Kensington Cable Lock Provision	Used to secure the Internet Device to a fixed object to prevent theft.	Install a Kensington cable lock to secure the Internet Device to a fixed object.

For more information about Computer Setup, see the *Reference Guide*.

Password Security

This Internet Device supports several password security features—a setup password, a power-on password, and a password to lock a MultiBay hard drive. The power-on password prevents unauthorized use of the Internet Device by requiring entry of a password to access applications or data each time the Internet Device 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 Internet Device.

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.

The DriveLock feature prevents unauthorized access to data stored on MultiBay hard drives.

Establishing a Setup Password Using Computer Setup

Establishing a setup password through Computer Setup prevents reconfiguration of the Internet Device (use of the Computer Setup utility) until the password is entered.

1. Turn on or restart the Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer.
2. When the F10 Setup message appears in the lower-right corner of the screen, press the F10 key. Press Enter to bypass the title screen, if necessary.

✎ If you do not press the F10 key while the message is displayed, you must restart the Internet Device again 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 Internet Device when power is turned on, unless the password is entered. The password must be entered each time the Internet Device is turned on, when the key icon appears on the monitor.

1. Turn on or restart the Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer.
2. When the F10 Setup message appears in the lower-right corner of the screen, press the F10 key. Press Enter to bypass the title screen, if necessary.

✎ If you do not press the F10 key while the message is displayed, you must restart the Internet Device again 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 Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer.
2. When the key icon appears on the monitor, type your current password, then press the Enter key.

✎ 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 Internet Device, then turn it on again before you can continue.

Entering a Setup Password

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

1. Turn on or restart the Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer.
2. When the F10=Setup message appears in the lower-right corner of the screen, press the F10 key.

✎ If you do not press the F10 key while the message is displayed, you must restart the Internet Device again to access the utility.

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

✎ 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 Internet Device, then turn it on again before you can continue

Changing a Power-On or Setup Password

1. Turn on or restart the Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer. To change the setup password, run Computer Setup.
2. When the key icon appears, type your current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:

   current password/new password/new password

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

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

✎ Refer to the “National Keyboard Delimiter Characters” section in this chapter 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

1. Turn on or restart the Internet Device. If you are in Windows, click Start → Shut Down → Restart the Computer. To delete the setup password, run Computer Setup.
2. When the key icon appears, type your current password followed by a slash (/) or alternate delimiter character as shown:

   current password/
3. Press the Enter key.

✎ Refer to the “National Keyboard Delimiter Characters” section in this chapter for information about alternate delimiter characters.

✎ The power-on password and setup password may also be changed using the Security options in Computer Setup.

Enabling or Disabling DriveLock on a MultiBay Hard Drive

CAUTION: A MultiBay hard drive can be rendered permanently unusable if the DriveLock security feature is enabled and the password is forgotten.

If the drive is shared with others or regularly used in multiple Internet Devices or locations, the Master password should be set and used by the owner of the drive or by the System Administrator to avoid rendering the drive unusable if the User password is forgotten. The risk of rendering a drive permanently inaccessible is reduced when the Master password and the User password are set and maintained separately.

To prevent unauthorized access to Computer Setup, establish a Setup password.

1. With the MultiBay hard drive installed, turn on or restart the Internet Device. If you are in Windows, click Start→Shut Down→Restart the Computer.
2. When the F10=Setup message appears in the lower-right corner of the screen, press the F10 key. Press Enter to bypass the title screen, if necessary.

If you do not press the F10 key while the message is displayed, you must restart the Internet Device again to access the utility.

3. Select Security, then select DriveLock Security. You will be prompted to select a drive from a list of drives in the system that suppport the DriveLock security feature.
   - ❏ To allow another user to enable DriveLock, yet ensure that you can always unlock the drive, set the Master password.
   - ❏ To enable DriveLock, click Enable DriveLock and enter a User password when prompted to do so.
   - ❏ To disable DriveLock, click Disable DriveLock. The user password is cleared and must be reset next time DriveLock is enabled.
4. Before exiting, click File→Save Changes and Exit.

Entering a DriveLock Password on a MultiBay Hard Drive

When DriveLock is enabled, the DriveLock User or Master password must be entered to unlock the drive. To enter a DriveLock password, complete the following steps:

1. Turn on or restart the Internet Device. If you are in Windows, click Start→Shut Down→Restart the Computer.
2. When the DiveLock key icon appears on the monitor, type your Master or User password, then press the Enter key.

✎ 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 two unsuccessful tries, POST will continue without unlocking the drive. You will have to restart the Internet Device and correctly enter the password before you can access the drive.

Changing a DriveLock Password on a MultiBay Hard Drive

1. Turn on or restart the Internet Device. If you are in Windows, click Start→Shut Down→Restart the Computer.
2. When the key icon appears, type your current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:

   current password/new password/new password

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

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

✎ Refer to the "National Keyboard Delimiter Characters" section in this chapter for information about the alternate delimiter characters.

✎ DriveLock passwords may also be changed using the Security options in Computer Setup. The Master password can only be changed in Setup if it was used to unlock the device during POST.

National Keyboard Delimiter Characters

Each keyboard is designed to meet country-specific requirements. The syntax and keys that you use for changing or deleting your password depend on the keyboard that came with your Internet Device.

National Keyboard Delimiter Characters

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

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

Clearing Passwords

If you forget your password, you cannot access the Internet Device. Refer to *Troubleshooting* for instructions on clearing passwords.

The Kensington Cable Lock Provision

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

✎ The cable lock can be purchased from Kensington Microware Limited or from Compaq DirectPlus (www.directplus.compaq.com). Ask for the Kensington MicroSaver Security System, Model 64068.

For illustrated instructions, please see the *Reference Guide* on the *Compaq iPaq Reference Library* CD.

Fingerprint Identification Technology

Eliminating the need to enter end-user passwords, Compaq Fingerprint Identification Technology tightens network security, simplifies the login process, and reduces the costs associated with managing corporate networks. Affordably priced and supported by the Compaq iPaq Internet Device, it isn't just for high-tech, high-security organizations anymore.

✎ Fingerprint Identification Technology is currently supported only on the Compaq iPaq standard models, not on iPaq legacy free models.

See www.compaq.com/im/fit/index.html for more information.

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.

When a fault occurs, the Internet Device displays a Local Alert message containing a description of the fault and any recommended actions. You can then view current system health by using the Compaq Management Agent. If the Internet Device is connected to a network managed by Compaq Insight Manager LC, Compaq Insight Manager or other management products from Compaq Management Solutions Partners, the Internet Device also sends a fault notice to the network management application.

Celeron and Pentium III Fault Prediction and Prefailure Warranty

When the processor encounters an excessive number of error checking and correcting (ECC) cache memory errors, the Internet Device displays a Local Alert message. This message contains detailed information about the faulty processor, allowing you to take action before you experience non-correctable cache memory errors. The Prefailure Warranty allows you to replace these processors, free of charge, before they actually fail.

SMART Hard Drive Fault Prediction

✎ SMART hard drive fault prediction and Prefailure Warranty apply only to internal hard drives, not to MultiBay drives.

The SMART hard drive monitors hard drive activity to predict failures and, in some cases, fix faults before failures occur. Fault prediction and failure indication parameters, such as abnormal variations in spinup and seek times, or non-correctable read and write errors, are tracked to determine the hard drive condition. Should these errors become significant, the Internet Device displays a warning message. The warning gives you time to back up the hard drive and replace it prior to experiencing downtime or loss of data.

The Prefailure Warranty for SMART hard drives allows you to replace these drives, free of charge, before the drives fail.

SMART hard drives are compliant with the Small Form Factor Committee Specification for Self-Monitoring, Analysis, and Reporting Technology (SMART). SMART is the industry standard technology, pioneered by Compaq and originally called IntelliSafe, that allows you to prevent data loss and minimize downtime, in concert with Compaq Management Agents.

Introducing the Drive Protection System

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

When Compaq iPaq Internet Devices 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. Your service provider can use this information to help diagnose conditions that caused you to run the DPS software. Refer to *Troubleshooting* for instructions on using DPS.

Ultra ATA Integrity Monitoring

Ultra ATA Integrity Monitoring monitors the integrity of data as it is transferred between an Ultra ATA hard drive and the system's core logic. If the Internet Device detects an abnormal number of transmission errors, the Internet Device displays a Local Alert message with recommended actions. An alert is also sent over the network to the system administrator.

Surge-Tolerant Power Supply

An integrated surge-tolerant power supply provides greater reliability when the Internet Device 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 Internet Device. This feature displays a warning message when the normal range is exceeded, which gives you time to take action before internal components are damaged or data is lost.

Software Updating and Management

Compaq provides several tools for managing and updating software on Compaq Internet Devices—Altiris eXpress, Insight Manager LC, System Software Manager, and Remote Management Setup Utilities.

Using Insight Manager LC, you can also monitor a workgroup of PCs from a central console and remotely update the system software, including flash ROM or hardware device drivers, for each of the managed PCs individually.

System Software Manager (SSM) is a utility that lets you update system-level software on multiple systems simultaneously. When executed on a PC client system, SSM detects both hardware and software versions, then updates the appropriate software from a file store. Support software that works with SSM is flagged with the PC Lifecycle Management icon on the Compaq Web site. To download the utility or to obtain more information on SSM, visit the Compaq Web site at http://www.compaq.com/im.

In addition to its PC configuration capabilities mentioned in a previous section, Altiris eXpress also includes easy to use software distribution capabilities. You can use Altiris eXpress to update operating systems and application software from a central console. When used in conjunction with SSM, Altiris eXpress can also update ROM BIOS and device driver software.

Finally, the Compaq Remote Management Setup Utilities, when integrated with Management Solutions Partners products, deliver an on-going management solution. These utilities supplement the capabilities of Solutions Partners products for distributing new applications, device drivers, and other system software. The Compaq Web site include updated ROM images and device drivers which can be distributed to client PCs using these software tools.

For more information, refer to the online Remote Management Administrators Guide. The Remote Management Administrators Guide is included with the Remote Management Setup Utilities, which are available on the Compaq Web site at www.compaq.com/support/files/index.html. The following sections provide information on using these utilities to accomplish various remote management functions including ROM flash, changing security settings, and wakeup/shutdown.

Remote ROM Flash

Your Internet Device comes with reprogrammable flash ROM (read only memory). By establishing a setup password in Security Management, you can protect the ROM from being unintentionally updated or overwritten. This is important to ensure the operating integrity of the Internet Device. Should you need or want to upgrade your ROM, you may:

- Order an upgraded ROMPaq diskette from Compaq.
- Download the latest ROMPaq images from the Compaq World Wide Web site (www.compaq.com).

CAUTION: For maximum ROM protection, be sure to establish a setup password. The setup password prevents unauthorized ROM upgrades. Compaq Insight Manager LC allows the system administrator to set the setup password on one or more PCs simultaneously. For more information, visit the Compaq Web site at www.compaq.com.

Using Remote ROM Flash

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

All Compaq iPaq ROMPaq ROM images from Compaq are digitally signed to ensure authenticity and minimize potential corruption.

✎ Your Internet Device must be powered on, or turned on through Remote Wakeup, to take advantage of Remote ROM Flash. Use of Remote ROM Flash also requires an established setup password.

For more information on enabling Remote ROM Flash, refer to the online *Remote Management Administrators Guide.* The *Remote Management Administrators Guide* is included with the Remote Management Setup Utilities, and is available on the Compaq Web site at www.compaq.com.

Remote Security Management

Remote Security Management allows the system administrator to safely set or modify security features on remote Compaq iPaq Internet Devices, directly from the centralized network management console. Enabling the system administrator to perform these tasks remotely, on multiple computers or Internet Devices, results in consistent deployment of and greater control over Compaq iPaq security parameters over the network. It also results in greater productivity and lower total cost of ownership.

✎ Your Internet Device must be powered on, or turned on through Remote Wakeup, to take advantage of Remote Security Management. Use of Remote Security Management also requires an established setup password.

For more information about the Remote Management Setup software and enabling Remote Security Management, refer to the online *Remote Management Administrators Guide*. The *Remote Management Administrators Guide* is included with the

Remote Management Setup Utilities, and is available on the Compaq Web site at www.compaq.com.

Remote Wakeup and Remote Shutdown

The Compaq iPaq Internet Device features an integrated network interface card that supports the Compaq Remote Wakeup and Remote Shutdown functions. These functions allow a system administrator to power on and power off a Compaq iPaq Internet Device from a remote location, supported by PC LAN management tools.

✎ Third-party software tools are required to remotely distribute software.

Remote Wakeup allows the network interface controller to continue functioning, even when power to the Internet Device has been turned off.

✎ The Internet Device continues to consume a small amount of electricity even after you turn it off. Only when you disconnect the power cord from the electrical outlet does the Internet Device stop consuming electricity.

To enable Remote Wakeup and Remote Shutdown, complete the following steps:

1. Double-click the Network Icon, located in the Control Panel.
2. Double-click the appropriate network controller.
3. Click the Advanced Properties tab.
4. Select Remote Wakeup.
5. Change the value to ON.
6. Click OK to save and apply changes, then click OK to exit the Network dialog.

For more information on using Remote Wakeup and Remote Shutdown, refer to the online *Remote Management Administrators Guide*. The *Remote Management Administrators Guide* is included with the Remote Management Setup Utilities, and is available on the Compaq Web site at www.compaq.com.

NIC Alert

The NIC Alert function enables desktop PCs to send an immediate alert to the network administrator when there is a hardware or operating system failure, or evidence of tampering, even if the system is powered off or the operating system is not yet started.

Replicating Your Setup

This procedure gives an administrator the ability to easily copy one setup configuration to other Internet Devices of the same model. This allows for faster, more consistent configuration of multiple Internet Devices. To replicate your setup:

1. Access the Computer Setup Utilities menu.
2. Click File → Save to Diskette. Follow the instructions on the screen.

✎ This requires a MultiBay LS-120 drive or a portable, external diskette drive.

3. To replicate the configuration, click File → Restore from Diskette, and follow the instructions on the screen.

Altiris eXpress and PC Transplant make it easy to replicate the configuration and custom settings of one PC and copy it to one or more PCs. For more information, visit the Compaq Web site at www.compaq.com.

Dual-State Power Button

With Advanced Power Management (APM) enabled in Windows 95 or Windows 98 or Advanced Configuration and Power Interface (ACPI) enabled for Windows 98 and Windows 2000, the power button can function either as an on/off switch or as a suspend button. The suspend feature does not turn off power altogether, but instead causes the Internet Device to enter a low-power standby. This allows you to quickly power down without closing applications and to quickly return to the same operational state without any data loss.

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

1. Access the Computer Setup menu.
2. Select Power→Energy Saver. Select Minimal or Advanced to turn on the Energy Saver Options menu.
3. Select Power→Energy Saver Options. Set the power button configuration to either On/Off or Suspend/Wakeup, as desired.

   Refer to the *Reference Guide* for more detailed information about the features of Computer Setup.
4. Select File → Save Changes and Exit.

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

✎ If you have selected the "Blink LED during Energy Save" option in Computer Setup, the power-on light will blink green once every two seconds while the Internet Device is in suspend. Refer to the *Reference Guide* for more information on using Computer Setup.

Power Management

Power Management is a feature that saves energy by shutting down certain components of the Internet Device when they are not in use, saving energy without having to shut down the Internet Device. Timeouts (the period of inactivity allowed before shutting down these components) can be enabled, customized, or disabled using Computer Setup.

1. Access the Computer Setup menu.
2. Select Power→Energy Saver. Select Advanced to turn on the Timeouts menu.
3. Select Power→Timeouts. Enable, customize, or disable timeouts.

   Refer to the *Reference Guide* for more detailed information about the features of Computer Setup.
4. Select File → Save Changes and Exit.

✎ To avoid potential conflicts, never enable monitor timeouts in Windows 95 or Windows 98 while system timeouts are enabled in Computer Setup.

Use Display Properties to establish, modify, or disable Power Management settings for the monitor. To access Display Properties, right-click on the Windows Desktop, then choose Properties.

World Wide Web Site

Compaq engineers rigorously test and debug software developed by Compaq and third-party suppliers, and develop operating-system specific support software, to ensure the highest level of performance, compatibility, and reliability for Compaq Internet Devices.

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 or Microsoft Windows NT Workstation that is different from the version included with your Internet Device, you must install corresponding Compaq device drivers and utilities to ensure all features are supported and functioning properly.

- Compaq has made the task of locating, accessing, evaluating, and installing the latest support software easier. You can download the software from the Compaq World Wide Web site at www.compaq.com.

The Web site contains the latest device drivers, utilities, and flashable ROM images needed to run Windows 95, Windows 98, Windows 2000, and Windows NT Workstation on your Compaq commercial desktop product.

✎ If you call Compaq to place an order, be sure to have the serial number of your Internet Device available. For the location of the serial number, refer to *Getting Started*. This number is necessary for all purchases.

Building Blocks and Partners

Compaq management solutions are based on industry standards, including DMI 2.0, Web-Based Enterprise Management, Intel's "Wired for Management," SNMP, and Net PC technologies. Microsoft, Intel, Hewlett-Packard, Novell, Seagate, and other industry leaders work closely with Compaq to integrate their management solutions with Compaq products and initiatives, giving you, the Compaq customer, extraordinary flexibility and functionality in client management and PC ownership cost reduction.

Desktop Management Interface (DMI)

The Desktop Management Task Force (DMTF) is an industry body created in 1992 with the goal of standardizing systems manageability. DMTF established the Desktop Management Interface (DMI) framework to standardize access to PC configuration data. Compaq, as a Steering Committee and Technical Committee member of the DMTF, delivers hardware and software instrumentation that supports the DMI standard.

For more information on configuring the DMI software, refer to the online *Intelligent Manageability Guide*.

Wired for Management

Intel's Wired for Management initiative is focused on reducing the support and administration cost of Intel architecture-based systems without compromising their flexibility and performance. The Wired for Management guidelines provide a baseline set of building blocks that Compaq utilizes in Intelligent Manageability to provide standardized management of desktop inventories, remote system configuration, off-hours maintenance, and next generation power management. But Compaq doesn't stop with these baseline features. Additional capabilities have been incorporated into Intelligent Manageability to provide an extensive solution for managing networked computing environments.

Wired for Management technologies include:

- Desktop Management Interface (DMI) 2.0
- Remote System Installation
- Remote Wakeup and Remote Shutdown
- ACPI-Ready Hardware

Compaq Management Solutions Partners Program

Compaq delivers desktop management solutions through the Compaq Management Solutions Partners Program. This Compaq initiative ensures compatibility and integration of AssetControl features with leading PC LAN and enterprise management products. These products provide remote access to the AssetControl features so that LAN and PC administrators can manage the Compaq Family of Personal Computers information from a central location. The partnership ensures that the benefits of Intelligent Manageability are accessible through a broad range of vendors. This allows customers to use their tools of choice to remotely manage their Compaq computers and Internet Devices more confidently and cost effectively. For more information and a list of Compaq Management Solutions Partners and their products, visit www.compaq.com/im/partners/index.html on the Compaq Web site.

INDEX

W