Compaq TaskSmartÔ N2400

Overview of the *TaskSmart N2400* 933MHz Server

The TaskSmart N2400 933MHz server is available with two Pentium III processors. This server includes all the features of the 733MHz server with the added features discussed in the following pages.

Table 1: System Part Numbers and Configuration Codes

Server Description	Part Number	Configuration Code
TaskSmart N2400 933/133-2TB (US)	221867-001	JJN1
TaskSmart N2400 933/133-2TB (Euro)	221867-421	JJN2
TaskSmart N2400 CHILLER JP	221867-291	JJN3

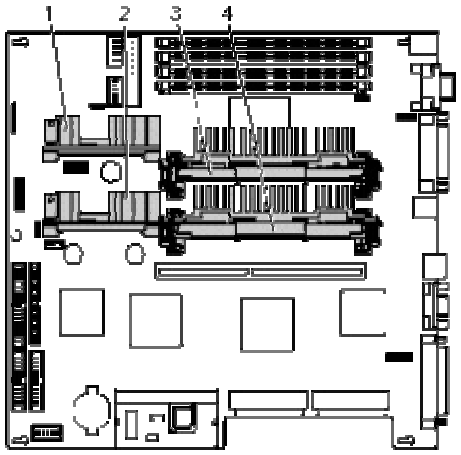
Distinctive Features of the Upgraded TaskSmart N2400

This new model brings the following changes to the TaskSmart N2400 line:

- Two (2), 933MHz processors with 256KB integrated Level 2 cache
- A 5300 Smart Array Controller - The Smart Array 5300 series of high performance Ultra3 array controllers provides improved flexibility and data protection by using an innovative modular design and new Advanced Data Guarding (RAID ADG) technology.
- Capable of using 18.2GB, 15,000 RPM Ultra3 drives in system drive bay (head).
- Capable of supporting up to four (4) external drive enclosures with 36.4GB, 10,000 RPM Ultra3 drives. When fully populated this provides fifty six (56), 36.4GB hot-pluggable hard drives.
- Uses Windows Powered OS and the operating system.
- Integrated web based user interface through the Lights Out Remote Insight Board (RIB).
- Implements NetWare support.

933MHz Processors

The TaskSmart N2400 933MHz system is populated with two (2), 933MHz processors with 133-MHz front side bus and 256KB integrated Level 2 cache. The system **must be populated with two processors** which operate in an associated mode. These processors are not hot-pluggable parts. The processors are keyed to ensure correct alignment. Align the pattern of pins on the processor with the pattern of holes in the slot to ensure proper installation. The pins and holes do not line up if the processor is misaligned.



Note:
Individual heatsinks may vary from the heatsink shown above

Table 2: Processor component locations

Item	Description
1	PPM Slot 1
2	PPM Slot 2
3	Processor slot 1
4	Processor slot 2

PPM

Every processor comes with a Processor Power Module (DC-to-DC converter) that provides power for the processor, it must be installed.

5300 Smart Array Controller

The TaskSmart N2400 comes with the Smart Array 5300 series of high performance Ultra3 array controller. This controller provides improved flexibility and data protection by using an innovative modular design and new Advanced Data Guarding (RAID ADG) technology. In addition, the Smart Array 5300 controller also provides higher levels of performance with several enhancements including a new memory architecture and new RAID engine.

The SA-5300 features complete data compatibility with previous generation's of Smart Array controllers for easy data migration from server to server and for controller upgradeability.

Features

- Higher performance architecture offers the new hardware RAID engine, and a new performance memory architecture to significantly improve performance over previous controllers
- Modular, easy-to-upgrade design lets you optimize performance and increase capacity as needed from two to four channels and with 32, 64 or 128MB battery-backed cache.
- New RAID ADG delivers high fault tolerance similar to RAID 1 while keeping capacity utilization high like RAID 5. RAID ADG protects data from multiple drive failures while only requiring the capacity of two drives to store parity information.
- RAID ADG can withstand two simultaneous hard drive failures without data loss or downtime this is twice as many as RAID 5
- High capacity utilization - the net capacity of two drives is reserved for parity information.
- Ultra3 SCSI technology delivers high performance and data bandwidth up to 160MB/s per channel bandwidth.
- Up to 4 channels provides the highest storage capacity per PCI slot in the industry.
- Mix-and-match LVD SCSI compatibility protects your investments and lets you deploy drives as needed.
- Battery-backed cache protects cached data in the event of a power outage, server failure or controller failure, and redundant batteries take that protection even further.
- A 64-bit, 66 MHz PCI interface boosts bandwidth up to a 533 MB/s total transfer rate.
- Online Management Features: Online Capacity Expansion, Online RAID Level Migration, Online Stripe Size Migration, Online Spares (Global), User Selectable Read/Write cache, User Selectable Expand and Rebuild Priority.

Raid ADG

RAID ADG is a new advanced RAID level that increases the number of sets of parity, creating multiple sets striped across the disks. ADG provides unparalleled fault tolerance, greater than RAID 1 or RAID 5, and at a lower cost implementation than RAID 1. Designed for support on the Smart Array 5300 Controller, RAID ADG is ideal for applications requiring large volumes. Available with the Smart Array 5300 Controller, RAID ADG can safely protect an array up to 56 total drives, ensuring a powerful solution with high fault tolerance.

System ROM

It is not necessary to modify any internal switch settings when implementing the 933MHz serve. During a system ROM upgrade of an existing N2400, the "Diskette drive power-up override" switch will need to be enabled (on) to allow for ROM upgrade.

The Compaq TaskSmart N2400 server has two switchbanks (SW1 and SW2) located on the system board. These switches are used to set the configuration of the server. The Diskette drive power-up override switch is located on Switchbank SW2 shown below.

System Configuration Switchbank (SW1)

SW1 is used as a system identification switch and the setting is pre-set in the factory. **Do not** change these settings. Incorrectly setting these switches may result in damage to the server.

System Configuration Switchbank (SW2)

The system configuration switchbank (SW2) is a six-position switch that is used for system configuration. The position of SW2 on the system board is shown below.

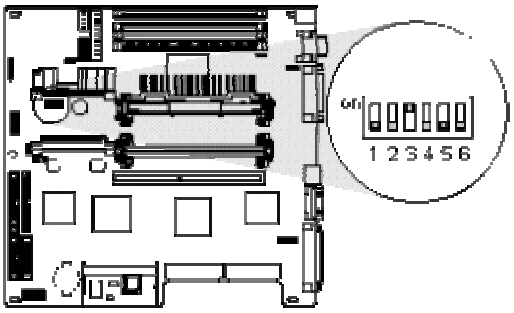


Table 3: Switchbank (SW2) Configuration Switch Settings

Item	Description	Default Setting
1	Embedded video disable	Off
2	Configuration lock	Off
3	Rack mount	On
4	Diskette drive power-up override	Off
5	Password disable	Off
6	Maintenance	Off

Windows Powered Operating System

The N2400 933MHZ appliance is powered by Microsoft Windows as a dedicated file servers. The Windows Powered operating system does not require any additional installation and setup instructions beyond what is already customary for Windows Advanced Server. The N2400 system powered by Windows supports heterogeneous environments, allowing clients running on Windows and other operating systems (including Unix) to share files and storage simultaneously on the LAN. N2400 systems powered by Windows incorporate the latest in server appliance technology to provide advanced features whose benefits include:

- Interoperable: Supports Windows and other operating systems
- Easy to Deploy
- Easy to Manage
- Highly Reliable
- Highly Scalable
- Optimized for High Performance
- Web User Interface

Interoperable

The N2400 powered by Windows support clients running Windows and other operating systems. No special configuration is required to support heterogeneous clients. The administrator deploys the N2400 appliance on the LAN, does basic configuration, and the server is ready to support the clients. The basic configuration takes about 15 minutes, as did the N2400 733MHz system.

Easy to Deploy

The N2400 powered by Windows has been specially designed to be easy to deploy: most basic deployments can be completed in 15 minutes. Key to the

streamlined deployment process are special tools and a simple Web user interface (UI) that administrators use to configure the appliance.

Easy to Manage

Microsoft has designed a Web-based (HTML) UI for configuration and management of the Windows Powered N2400. This easy-to-use UI allows an administrator to manage one or more N2400 appliances from a remote machine.

Highly Reliable/Available

The N2400 powered by Windows uses the best-of-breed technology of Windows 2000 to provide world-class reliability. The reliability of Windows Advanced Server 2000 is built into the Windows Powered N2400.

Highly Scalable

The N2400 powered by Windows uses best-of-breed technology to provide a highly scalable NAS server that can be scaled from GB to TB. The ability of administrators to add storage to existing NAS servers without having to bring the machines down adds convenience to scalability, allowing users to access their data while storage is being added.

Optimized for High Performance

NAS appliances powered by Windows have been optimized for performance, and supports industry-standard features including HTTP, NFS, CIFS, NW, Apple Talk, FTP, Kerberos, Fibre Channel, and SCSI.

Integrated Web Based User Interface

The Compaq Administration and Management Utility is a comprehensive management tool that allows administrators to access and manage all aspects of their TaskSmart N-series appliances.

The Compaq Administration and Management Utility is a Web-based user interface (UI) designed for the TaskSmart N-Series appliances. The Web-based UI allows system administrators to access and manage TaskSmart N-Series appliances via a Web browser on a remote Windows-based machine. The Compaq Administration and Management Utility is compatible with Web browsers that support HTML 4 or greater. Web browsers that meet this requirement are Microsoft Internet Explorer 4.0 and greater and Netscape 4.6 and greater.

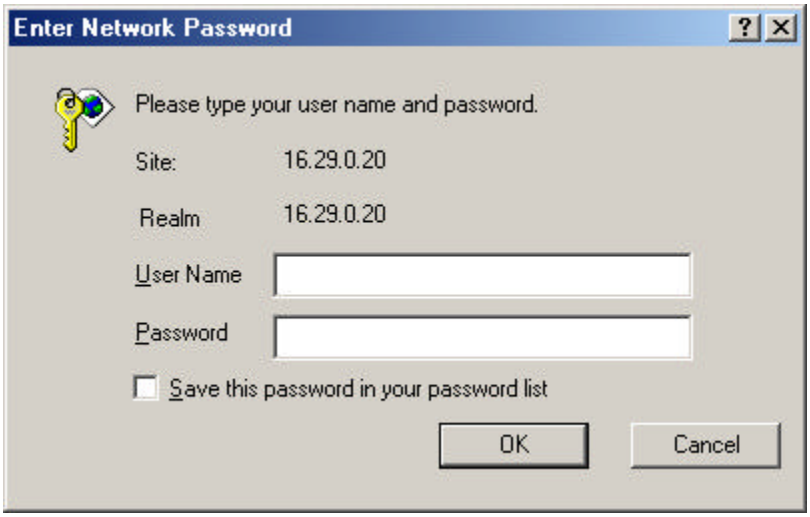
The following information provides an overview of the features and operation of the interface.

Accessing and Login

The User Interface is accessed using a standard browser pointed to the RIB IP address using socket 3201. If you assigned an address of 16.29.0.20 as the IP address for the RIB board, your user interface is accessed by entering the following address:

http://16.29.0.20:3201

Once this is entered you will be presented with a login dialog.

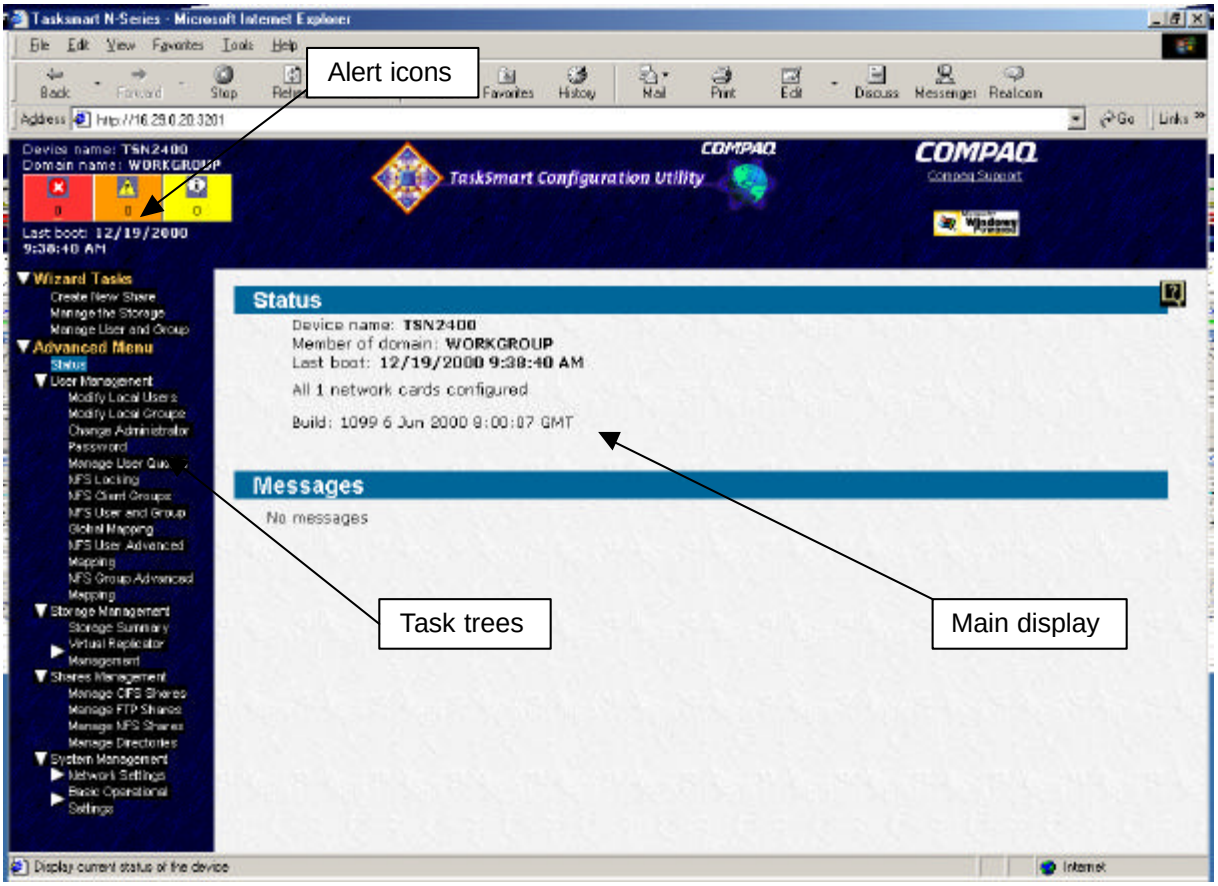


The user name and password is the administrator's user name and password. These are set using the configuration diskette during the standard installation of the N2400.

After entering the required information you will be presented with the user interface.

User Interface Window

The User Interface Window is used to access the various features of the N2400. There are three distinct areas of the user interface; Alert Icons, Task trees, and Main display. The illustration below shows the user interface with the task trees expanded to display all of the major functions and the Status item selected.



Alert Icons

Alert icons give immediate indication of the health and operation of the N2400. These icons are explained further later in this section.

Task Tree

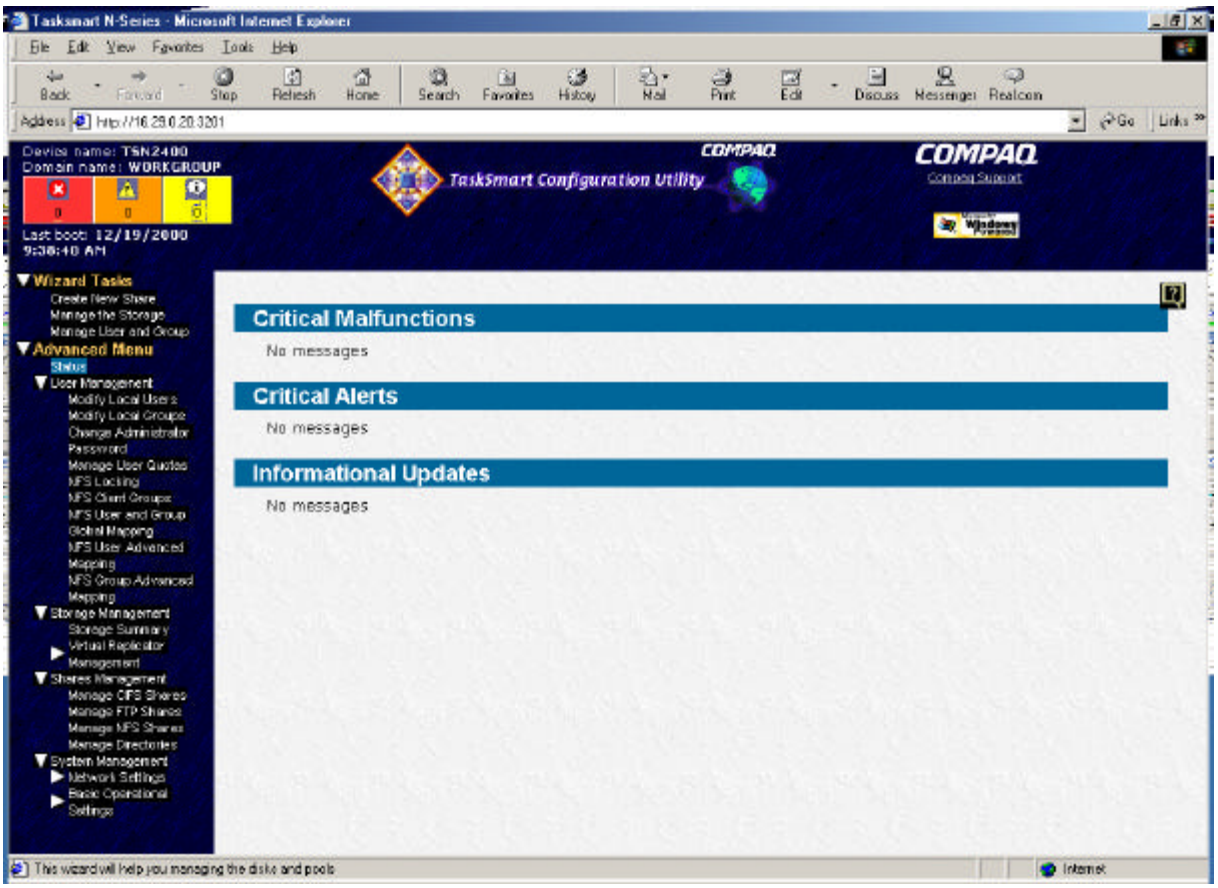
There are two main trunks of the task tree: Wizard tasks and Advanced menu. These allow the administrator to perform operations on the N2400. Each of these operations is described later in this section.

Main display

The main display is the area of the user interface where functions being performed will be displayed. Both informational and active operations will be displayed here.

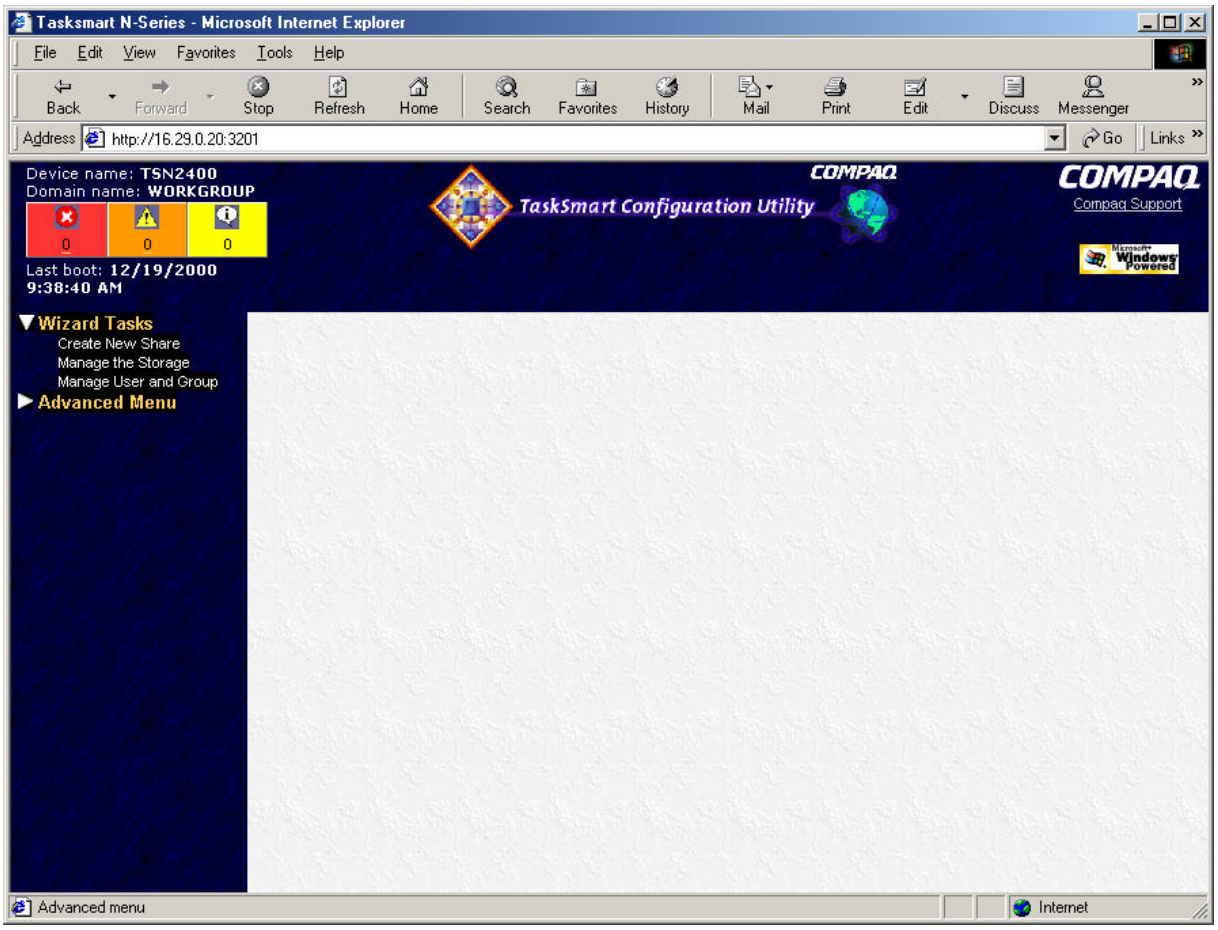
Alert Icons

The Alert Icons appear in the upper left hand of the user interface at all time. These icons give an immediate indication of the health of the N2400. This screen displays a list of critical errors, critical alerts and informational updates received during the current server session. The administrator can click on any of the events listed for detailed information on that event.



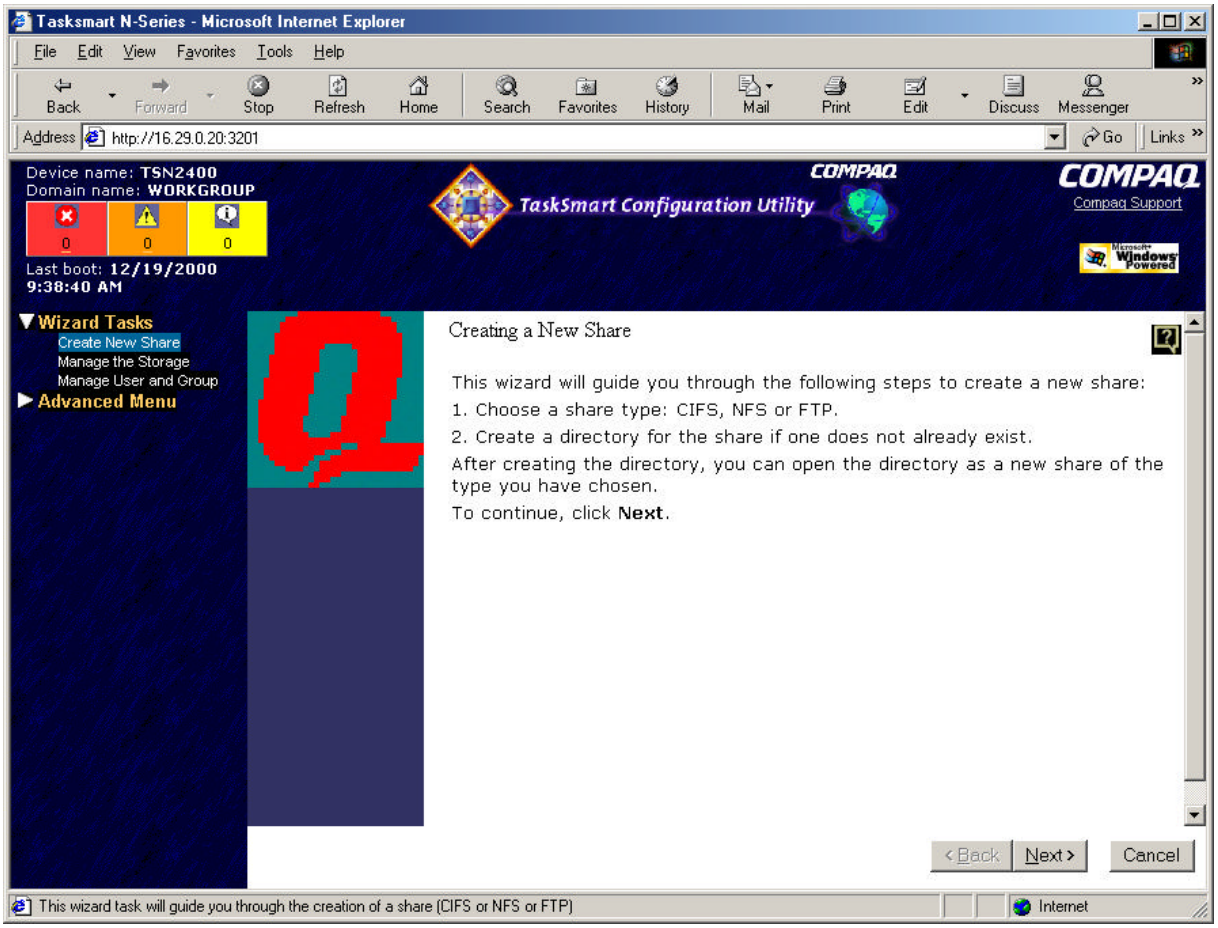
Wizard Tasks

Wizard Tasks are directed methods of, creating new stores, managing existing storage, and managing users and groups. Each of these items is accessed by selecting the desired operation under the Wizard Tasks menu item.



Create New Share

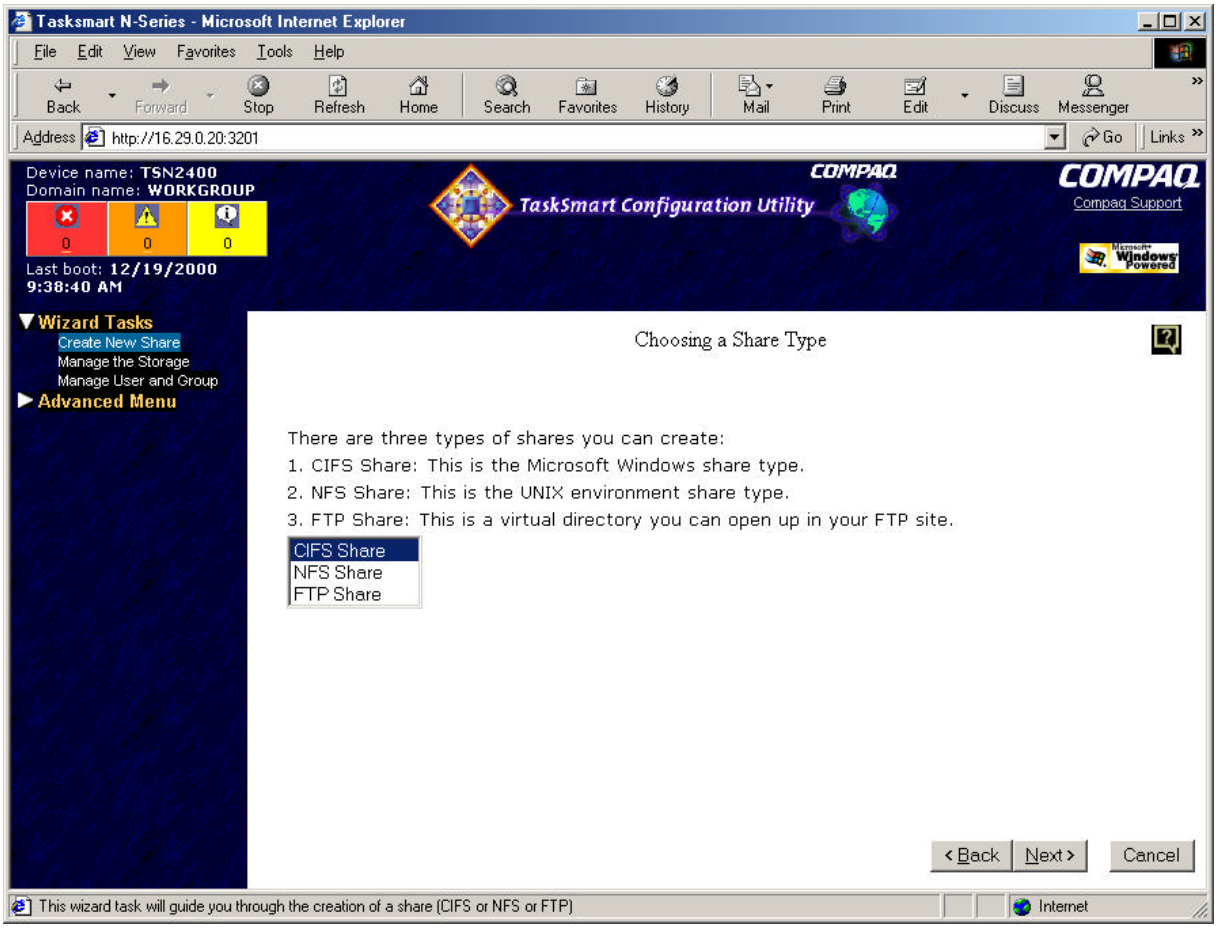
To create a new share select the Create New Share menu item. This wizard guides the user through the process of setting up shares on the TaskSmart N2400 appliance, including CIFS shares, NFS shares, and FTP shares. This functionality allows the administrator to create a directory on the local file system that can be shared by users and groups.



To create a new share, click on the Next button and follow the direction of the wizard screens.

Choosing a Share Type

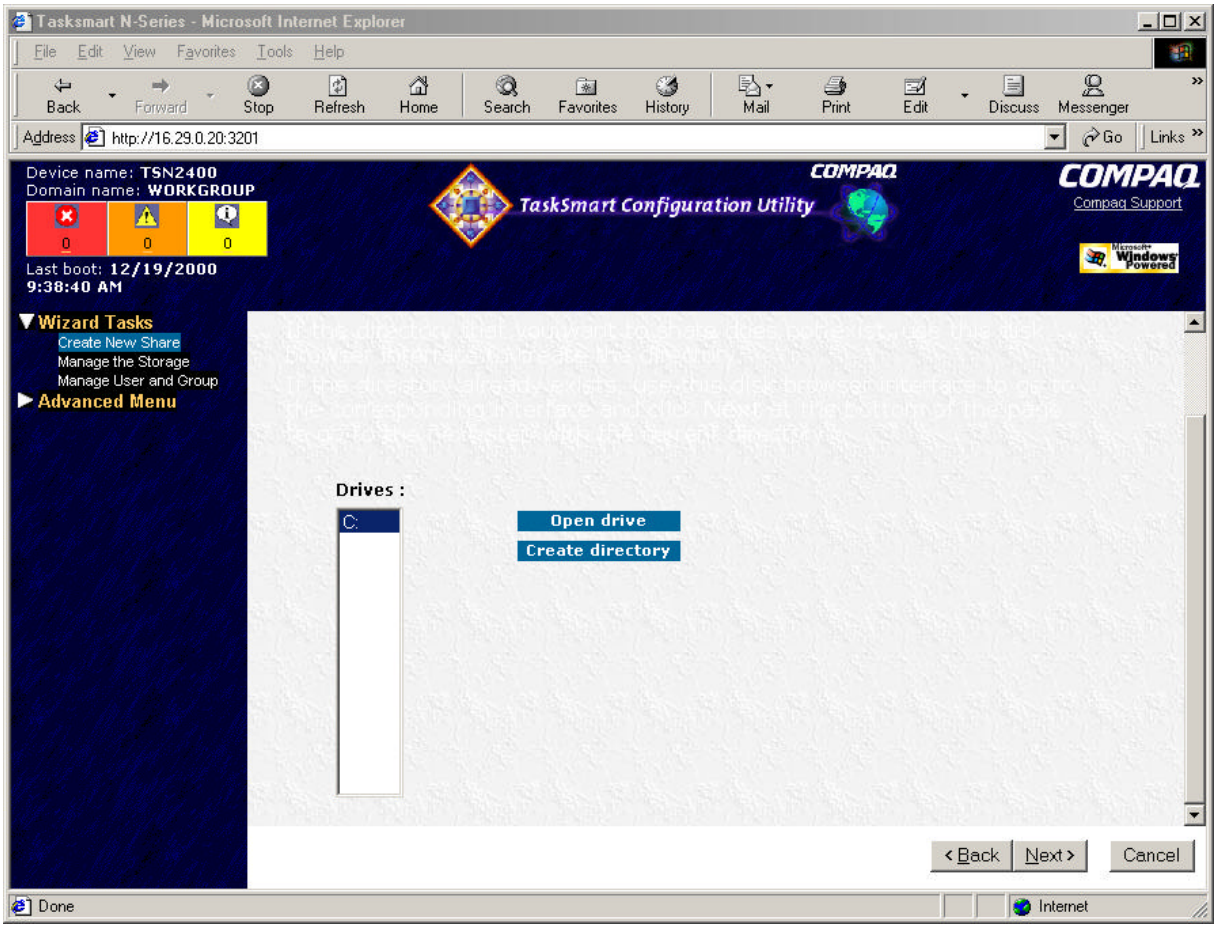
This screen allows the administrator to choose the type of share desired. The available choices are CIFS share, NFS share, and FTP share. CIFS shares are the Microsoft Windows share type. NFS shares are the UNIX environment share type. FTP shares are virtual directories that are opened up in a FTP site.



Select the desired share type and click on the Next button.

Open Drive/Create Directory Screen

This screen allows the user to select a local drive to browse to find a directory. It also gives the user the option to create a new directory. If a new directory is created, the user may define this as the share directory. If a local drive is opened, the user can browse it, searching for an existing directory or a place to add a new directory.



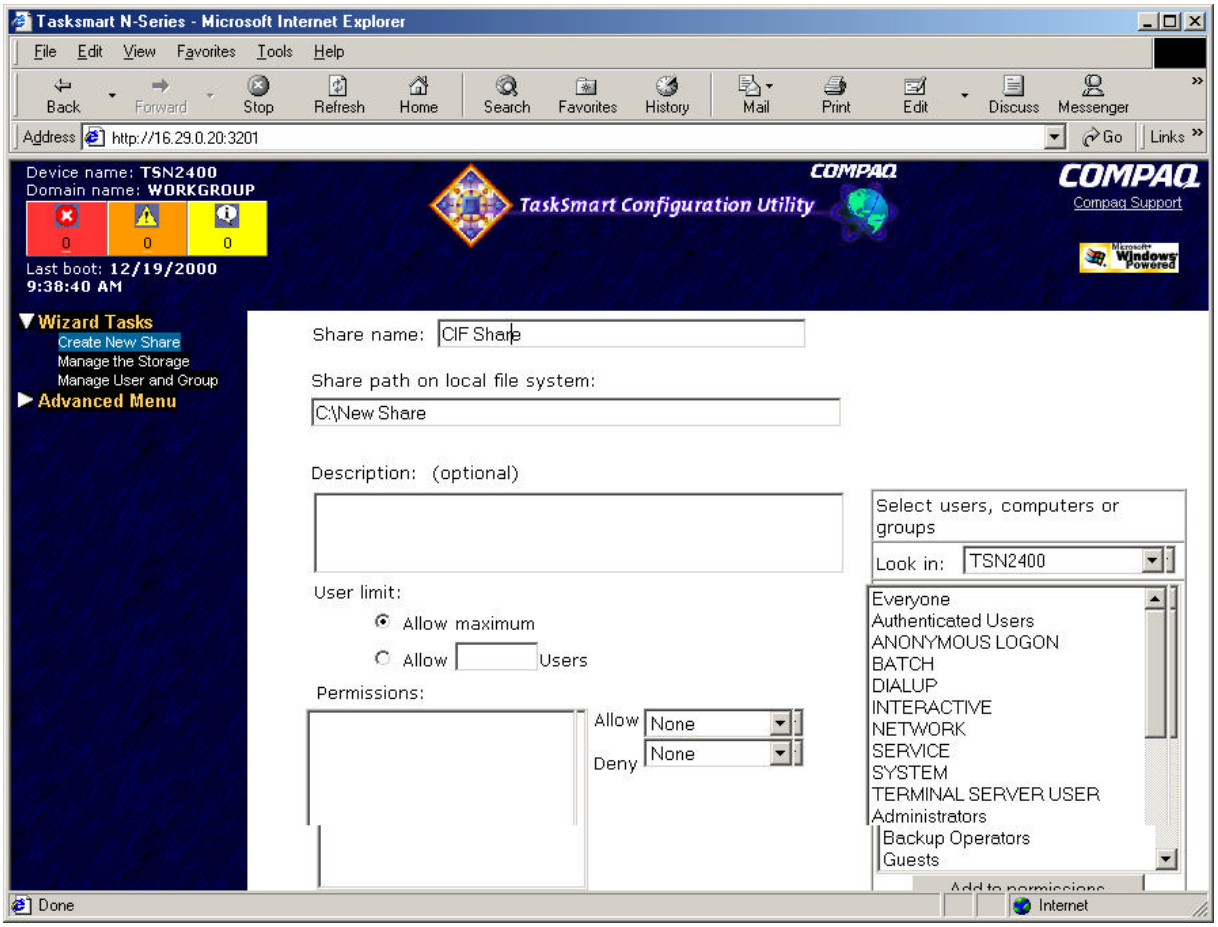
This screen is displayed regardless of the type of share being created. All of the available drives are displayed under the Drives heading. Select the desired drive and click on the Open Drives button. Next you can create a new directory or select and existing directory. After you have made your choices click on the Next button.

Create a CIFS Share

If the CIFS share type was selected, the next screen that is displayed is for defining CIFS properties. The first field that is defined is the share name. A description of the new share can be created next. The description is optional. This option simply provides other administrators with additional information regarding the share.

The administrator must then set the user limit for the new share. The administrator can either set the maximum number of users to no limit or to anything up to the total available.

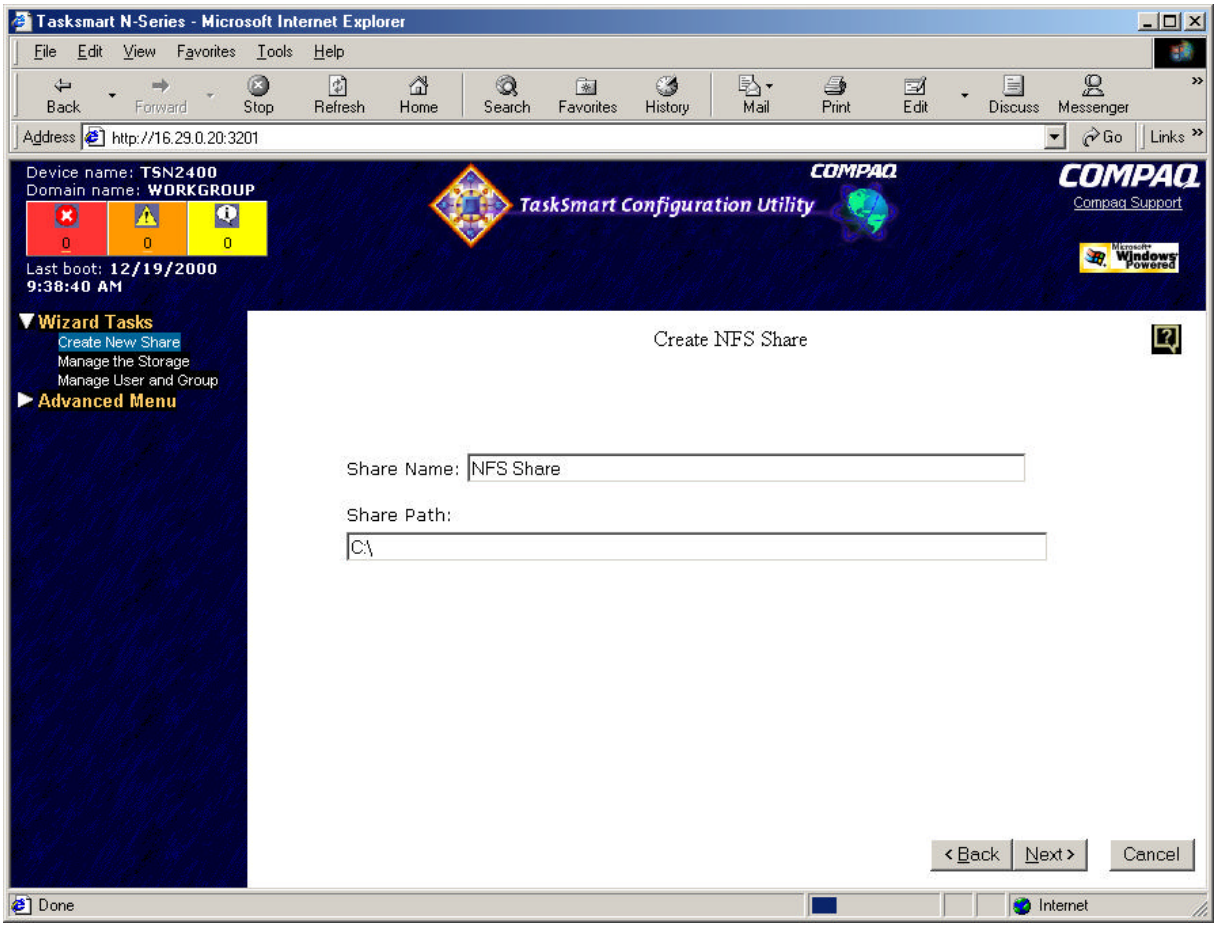
The final step in creating a new share is defining the permissions. The administrator selects any user, computer, or group from the list displayed on the right side of the frame and clicks the **Add To Permissions** button to include them in the permissions for the new share. When all the required permissions have been added to the new share, the rights must be set. To do this, the administrator selects the share in the permission box and then selects the desired rights in the **Allow** and **Deny** combo boxes. The available rights for each are Full Control, Read, Change, Read/Change and None.



Once the shares properties have been defined, click on the Next button to complete the share creation.

Create NSP Share

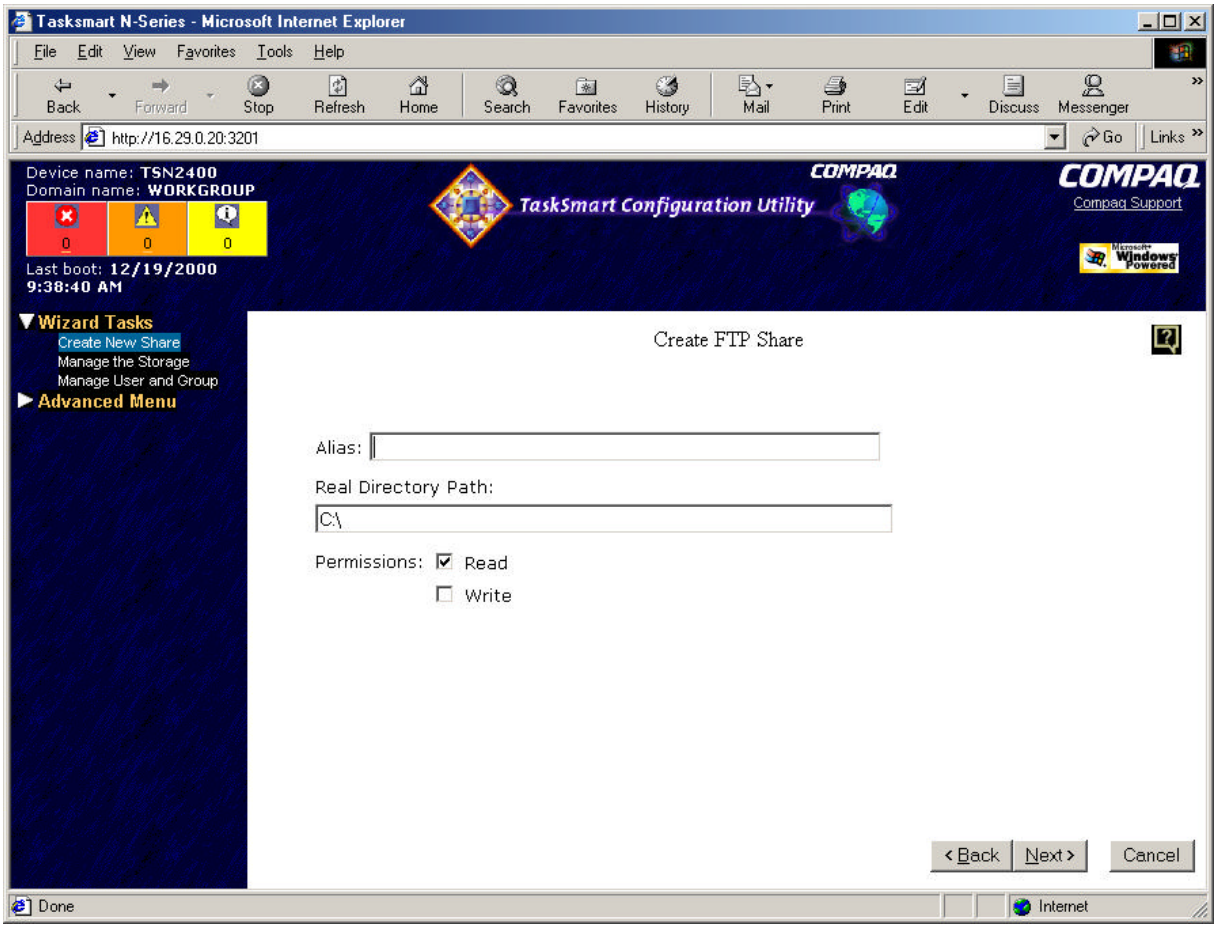
An NFS share has a share name and a share path.



Once the shares properties have been defined, click on the Next button to complete the share creation.

Create FTP Share Screen

When an FTP share has been defined, the share properties associated with it can be defined. The first field that must be defined is the alias. The final step is to enable or disable the read and write access for the share. This is done by clicking the corresponding check box.



Once the shares properties have been defined, click on the Next button to complete the share creation.

Create Other Shares Screen

When the properties of a share have been defined, the administrator is given the option to create other shares with the new directory created.

Shares Management Screen (CIFS/NFS only)

When all new shares have been added, the administrator can manage the existing shares. This screen allows the administrator to add, delete, or view the properties of a share.

Shares Management Screen (FTP only)

When all new shares have been added, the administrator can manage the existing shares. This screen allows the administrator to add or delete a FTP site, view the properties of a share, or define a new virtual directory.

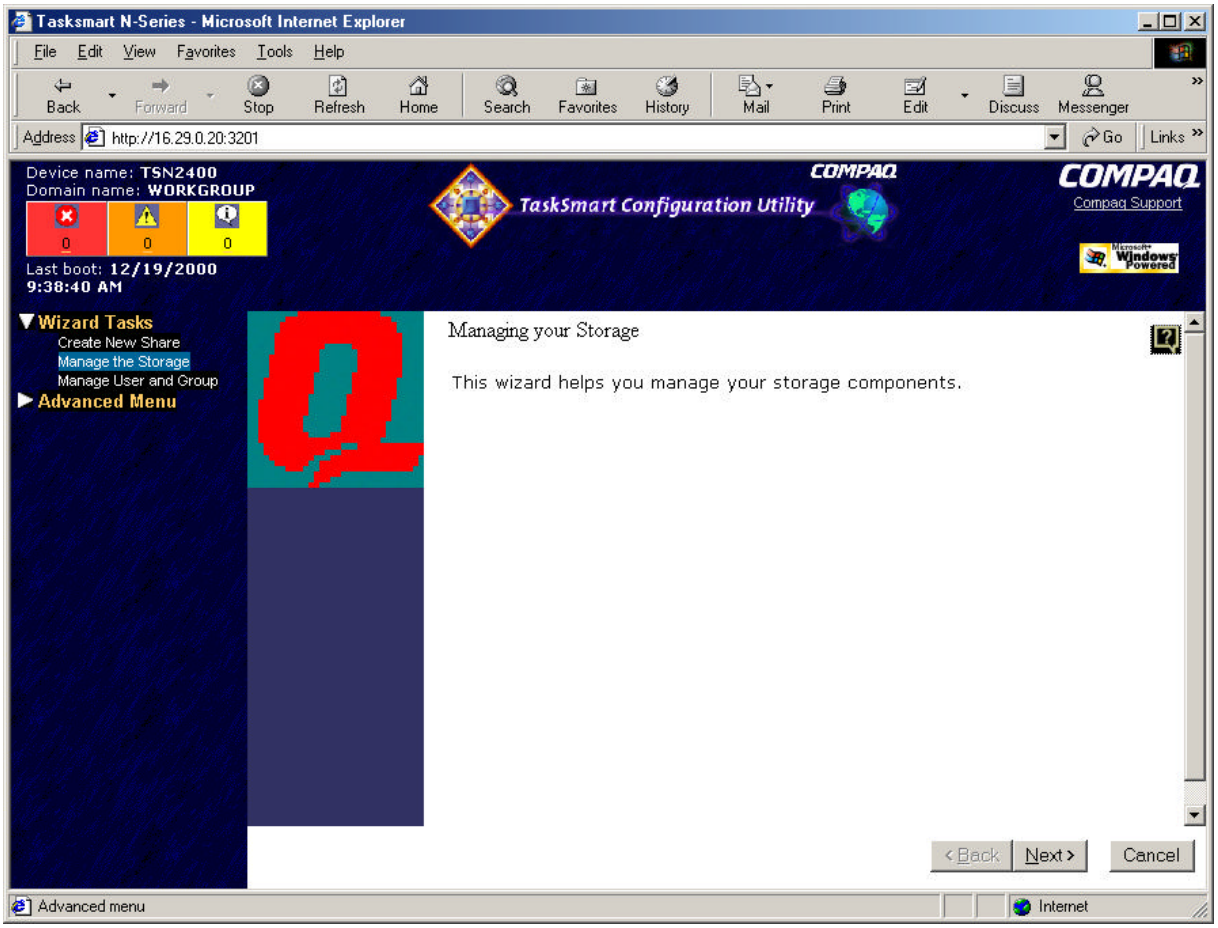
Shares Properties Screen (CIFS/NFS only)

This screen allows the administrator to modify the properties of the share. The share name and directory cannot be changed. The description of the share can be modified. The creation of a description is optional. This description simply provides other administrators with additional information regarding the share. The administrator must then set the user limit for the new share. The administrator can either set the maximum number of users to no limit or to anything up to the total available. The administrator can modify the permissions.

To add a new permission, the administrator selects any user, computer, or group from the list displayed on the right side of the frame and clicks the **Add To Permissions** button to include them in the permissions for the new share. When all the required permissions have been added to the new share, the rights must be set. To do this, the administrator selects the share in the permission box and then selects the desired rights in the **Allow** and **Deny** combo boxes. The available rights for each are Full Control, Read, Change, Read/Change and None.

Manage the Storage

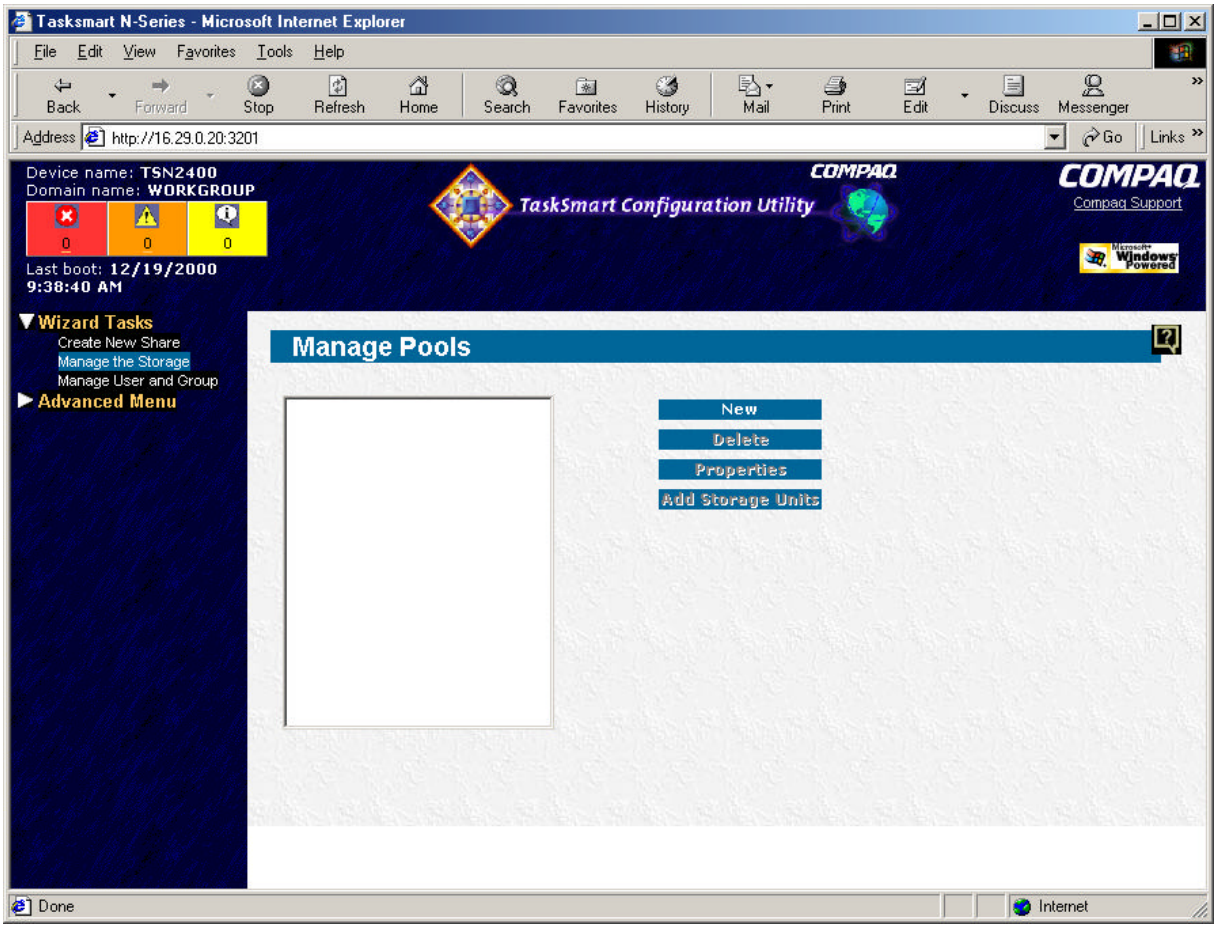
To use the Manage the Storage wizard, click on the Manage the Storage menu item. This wizard guides the user through the management of the storage on the TaskSmart N2400 appliance, including managing pools, virtual disks, and snapshots.



To start managing the desired storage component, click on the Next button and follow the direction of the wizard screens.

Manage Your Pools Screen

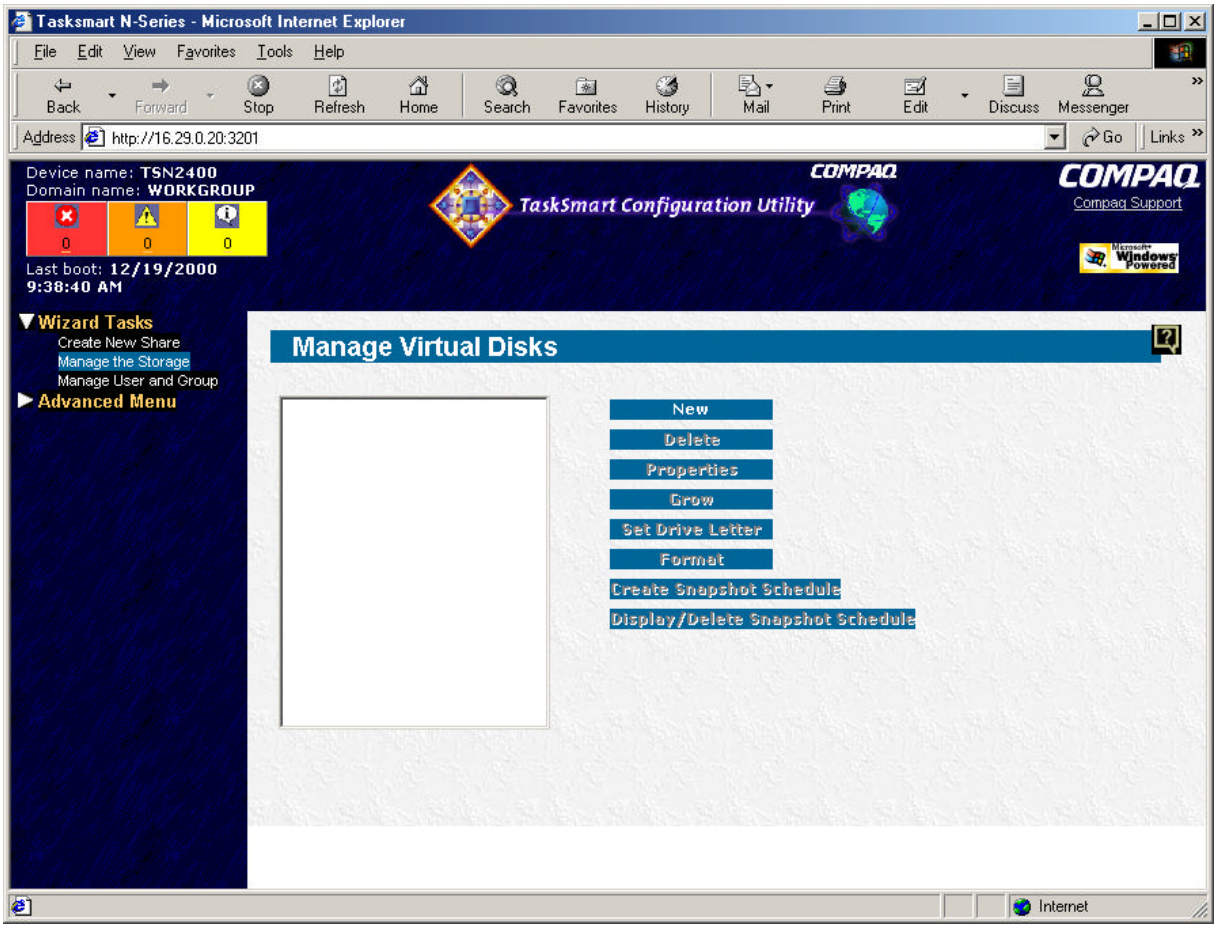
This screen allows the administrator to access the management tasks for the pools configured on the TaskSmart N2400 appliance. The available tasks include creating new pools, deleting pools, viewing pool properties, and adding storage units.



Manage Your Virtual Disks Screen

This screen allows the administrator to perform various management functions on virtual disks. These include:

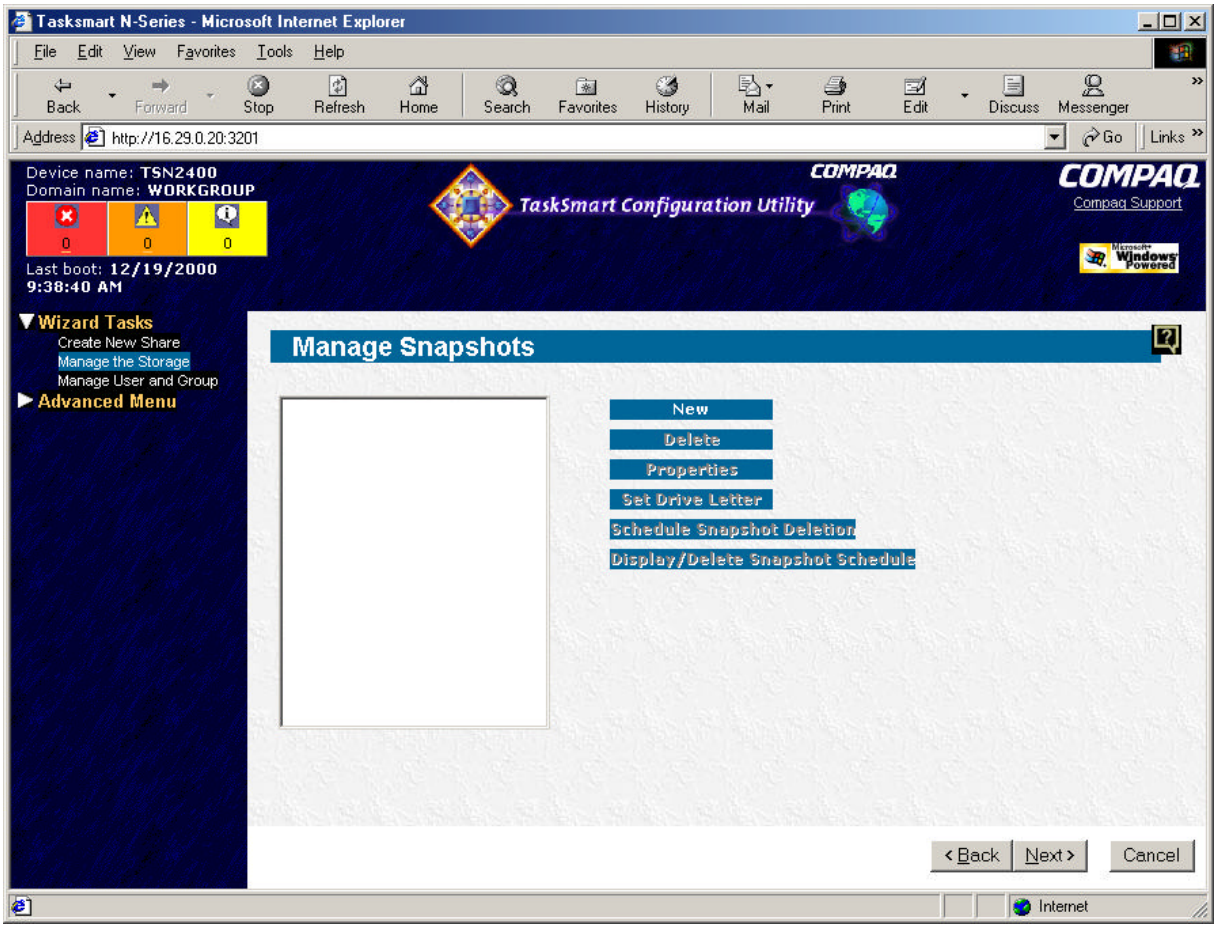
- Adding new virtual disks
- Deleting virtual disks
- Viewing virtual disk properties
- Growing a virtual disk
- Setting the drive letter
- Formatting virtual disks
- Creating snapshot schedules



Manage Your Snapshots Screen

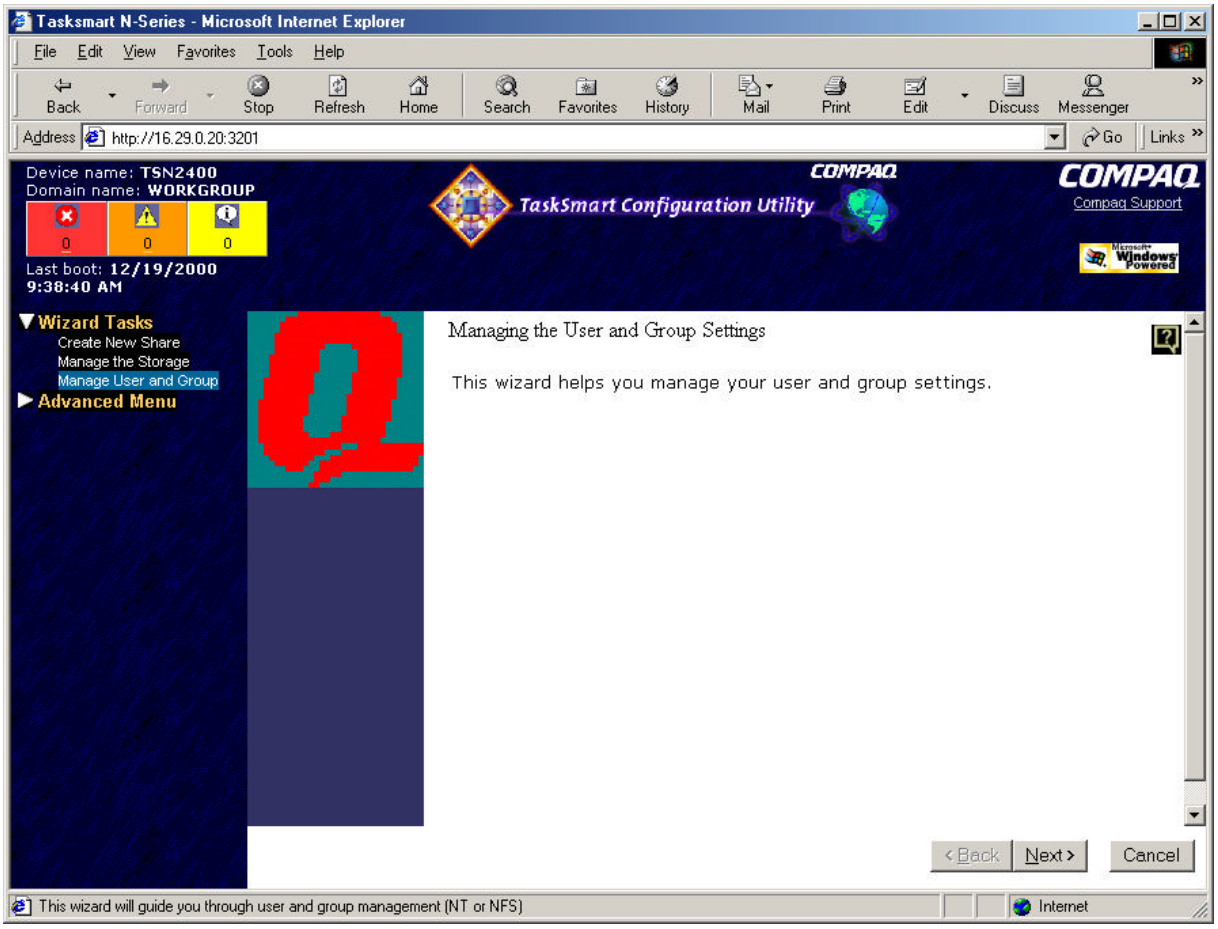
This screen allows the administrator to manage the snapshots on the server. The available tasks are:

- Adding new snapshots
- Deleting snapshots
- Viewing snapshot properties
- Setting the drive letter
- Scheduling snapshot deletion
- Displaying and deleting snapshot schedules



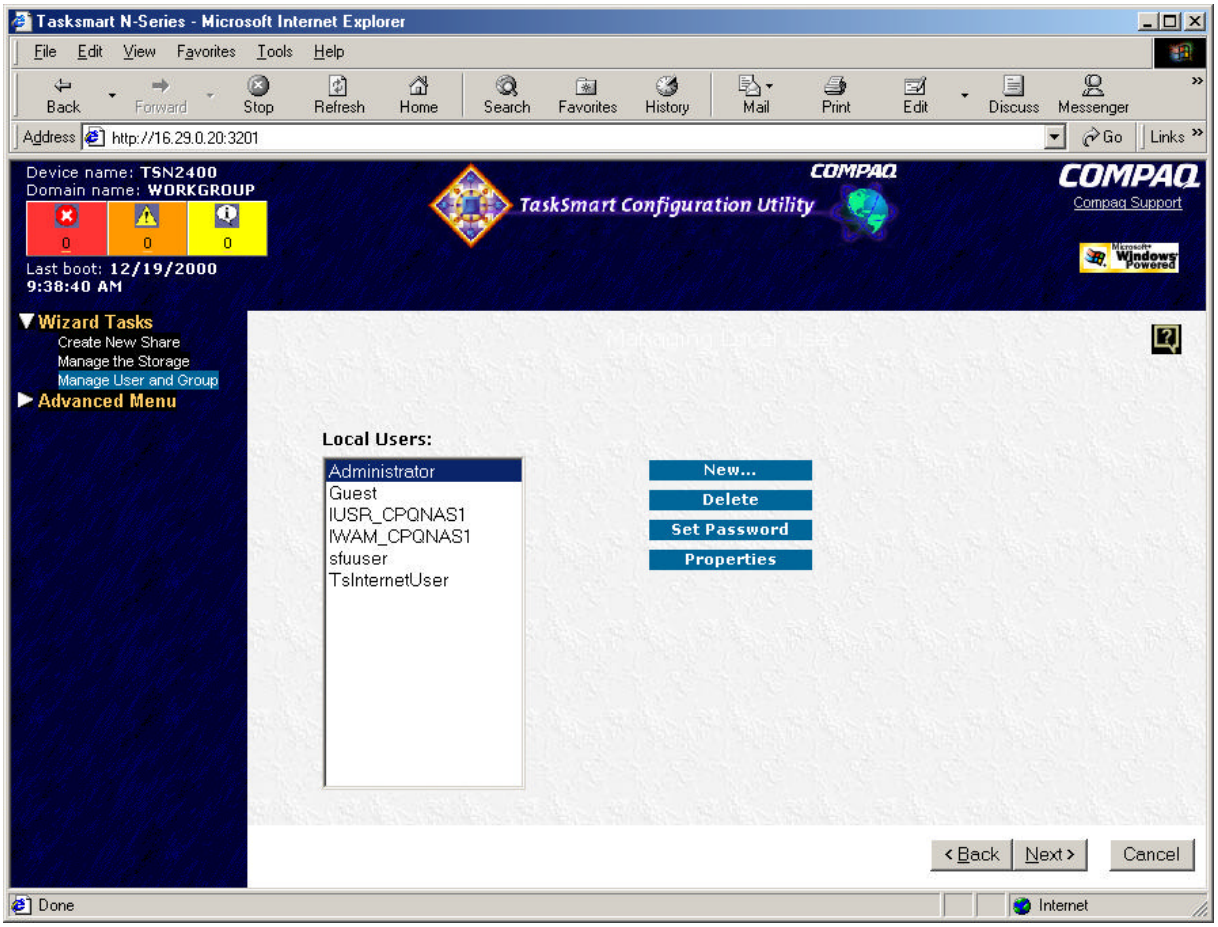
Manage User and Group

This wizard guides the user through the management of the users and groups on the TaskSmart N2400 appliance. This includes local user settings, local group settings, user quotas, and NFS mapping.



Manage Local User Settings Screen

This screen allows the administrator to define settings for local users. The available tasks are creating new users, deleting users, setting passwords, and modifying user properties.



Add New User Screen

This screen allows the administrator to create a new user account on the device. The administrator can enter a new valid username, user account full name, description of the user account, and account password. A valid username cannot be blank, contain the special characters / * ? "<> | + = , ; : [ ] \, or duplicate an existing username. The administrator can also disable the user account using this page.

Delete User Screen

This screen asks the administrator to confirm that they want to delete the user account. The user account will not be deleted until the administrator clicks **OK**. Built-in user accounts cannot be deleted.

Set Password Screen

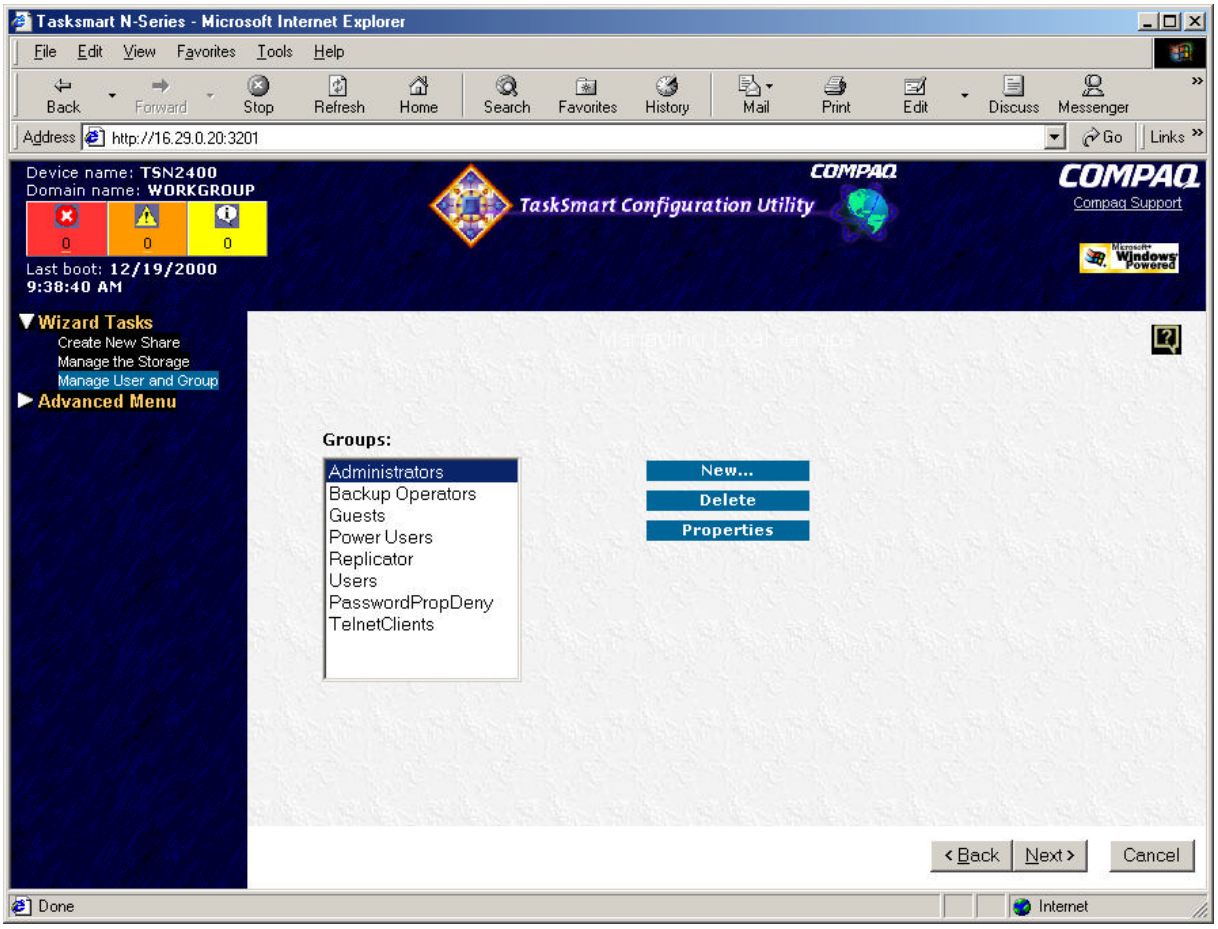
This screen allows the administrator to set a new password to a user account. The password cannot be blank.

User Properties Screen

This screen allows the administrator to modify the current username, user account full name, and description of the user account. A valid username cannot be blank, contain the special characters / * ? "<> | + = , ; : [ ] \, or duplicate an existing username. The administrator can also disable the user account using this page.

Manage Local Group Settings Screen

This screen lists the current local user groups and allows the administrator to manage the local user group settings. The administrator can create a new user group, delete an existing user group, or edit the properties of an existing user group.



New User Group Screen

This screen allows the administrator to create a new user group on the device. The administrator can enter a new valid user group name and description of the user group. A valid user group name cannot be blank, contain the special characters / * ? "<> | + = , ; : [ ] \, or duplicate an existing user group name. The administrator can also add local users to the user group.

Delete User Group Screen

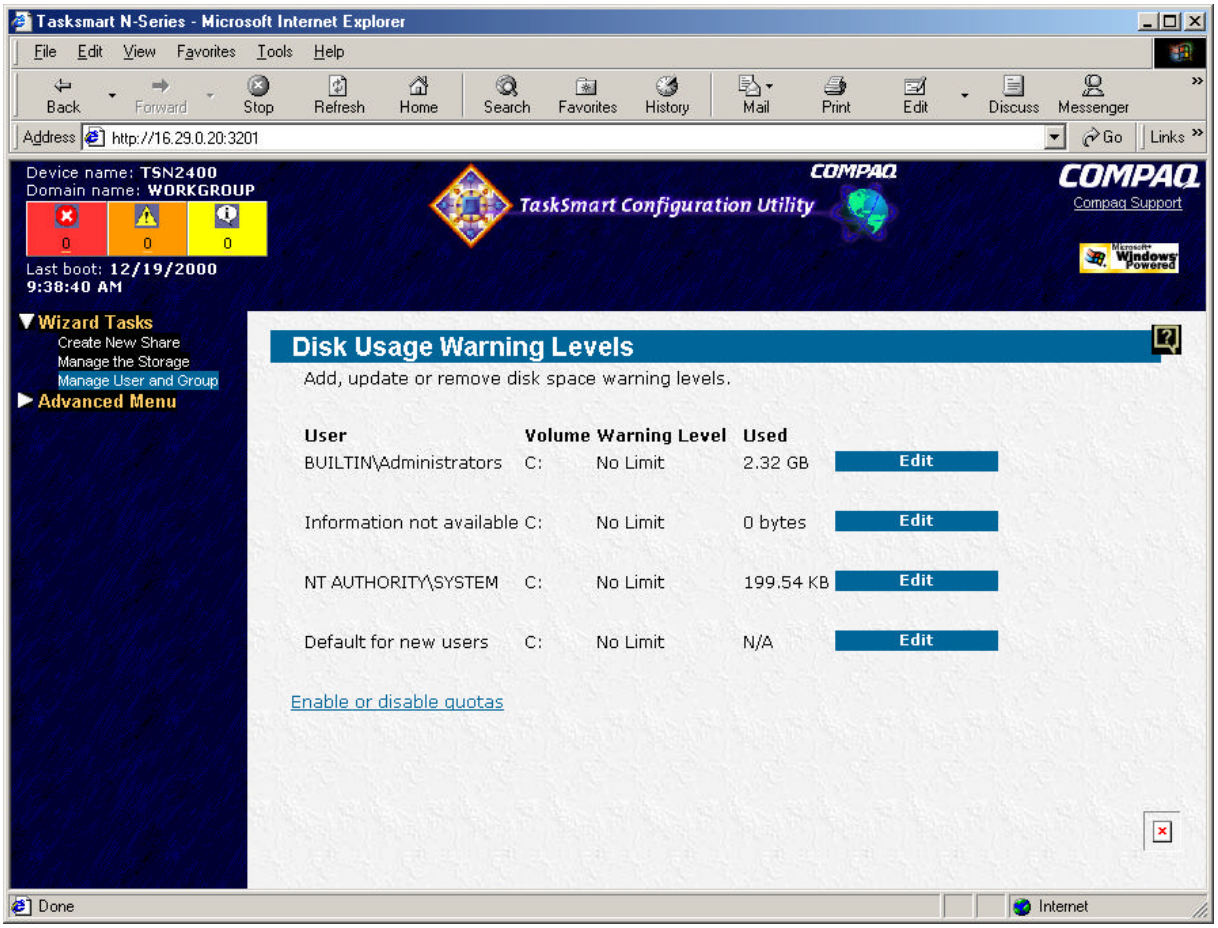
This screen asks the administrator to confirm that they want to delete the user group. The built-in user groups cannot be deleted. The user group will not be deleted until the administrator clicks **OK**.

User Group Properties Screen

This screen allows the administrator to modify the current user group name and the description of the user group. A valid user group name cannot be blank, contain the special characters / * ? "<> | + = , ; : [ ] \, or duplicate an existing user group name. The administrator can also add new users to the user group or remove local user accounts from the user group.

Manage Disk Usage Warning Levels

Drive quotas enable administrators to control the allocation of drive space to individual users or groups of users. When quotas are enabled and properly configured, it is impossible for one person or group to consume all of the available space on a disk. When quotas are enabled on a volume that already contains files, Windows calculates the drive space used by all users on the volume. The quota limit and warning level are then applied to all current users. Administrators can then modify quotas as needed. The drive quota must be enabled on the device through the console UI before this page is functional.



Edit Quota Screen

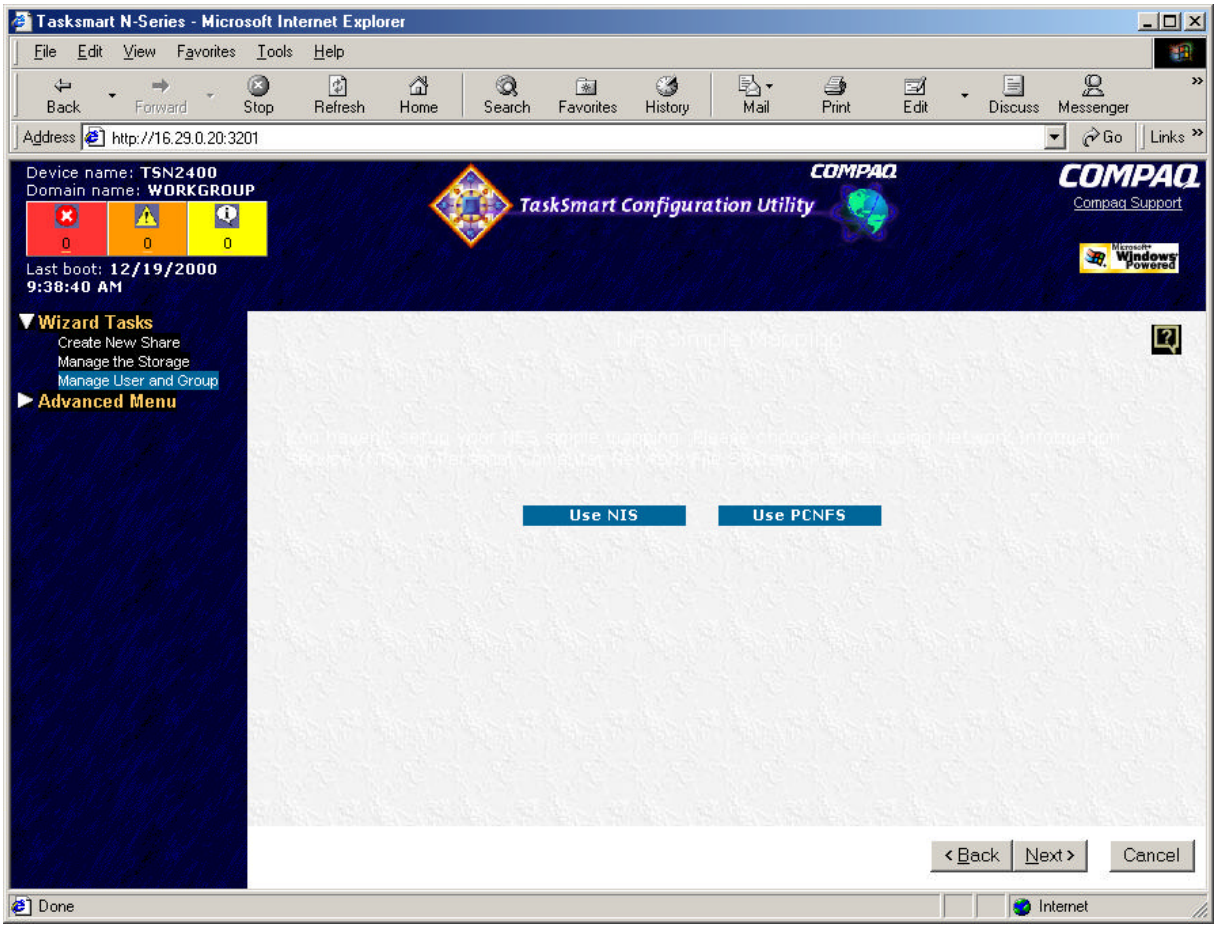
This screen allows the administrator to set the disk space warning level for a user. The administrator can either set the quota to have no limit or can set the warning level to anything up to the total available.

Manage NFS Mapping Screen

This screen allows the administrator to manage the various aspects of NFS mapping, including simple user and group mapping and advanced user and group mapping. User name mapping is the process of taking user and group identification from one environment and translating it into user identification in another environment.

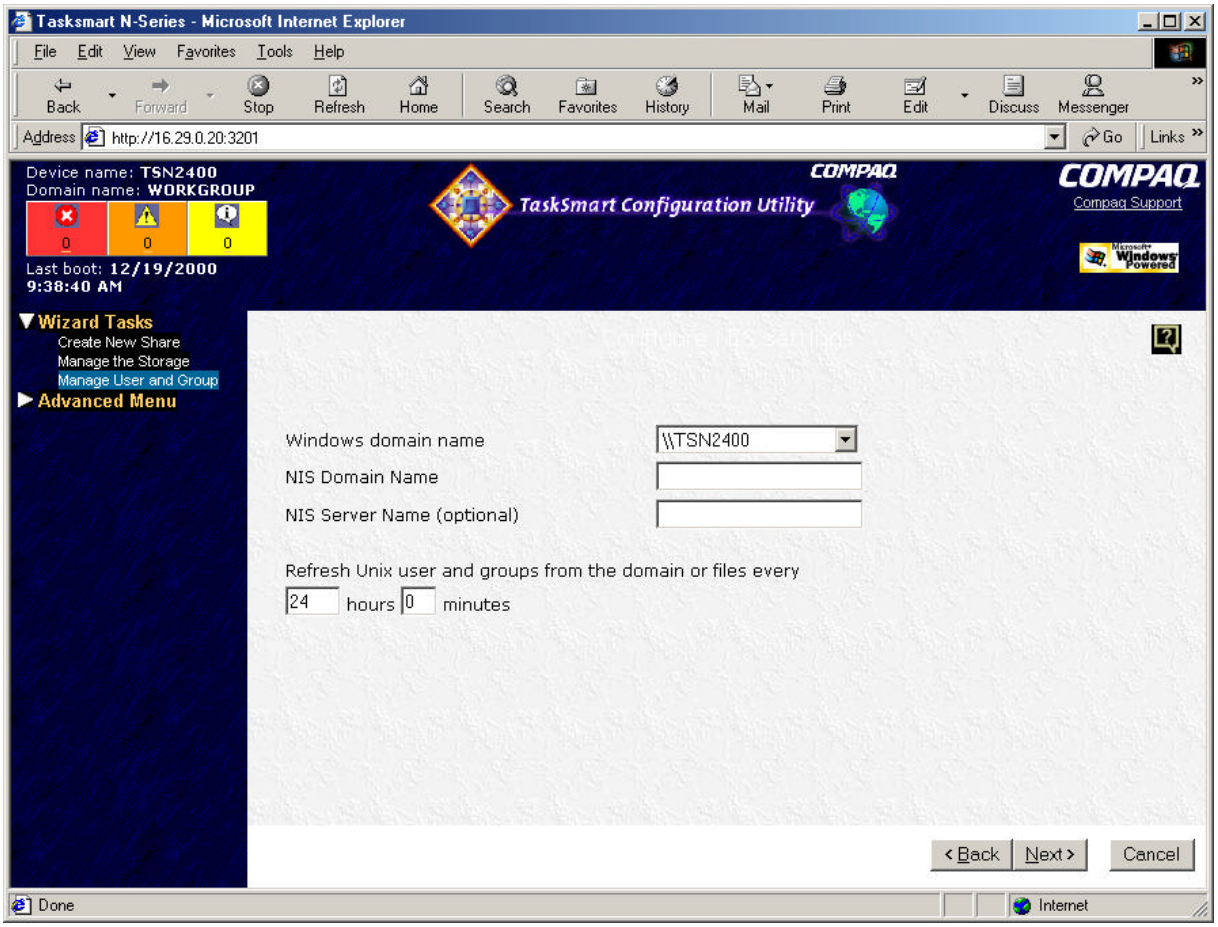
Manage Simple Maps Settings Screen

If the **Simple Maps** field is not checked on the NFS User and Group Global Mapping screen, this screen will be displayed and the **Simple Maps** field will be checked. This screen allows the administrator to choose the type of simple maps used by the server. The available choices are Network Information Services (NIS) and Personal Computer Network File System (PCNFS).



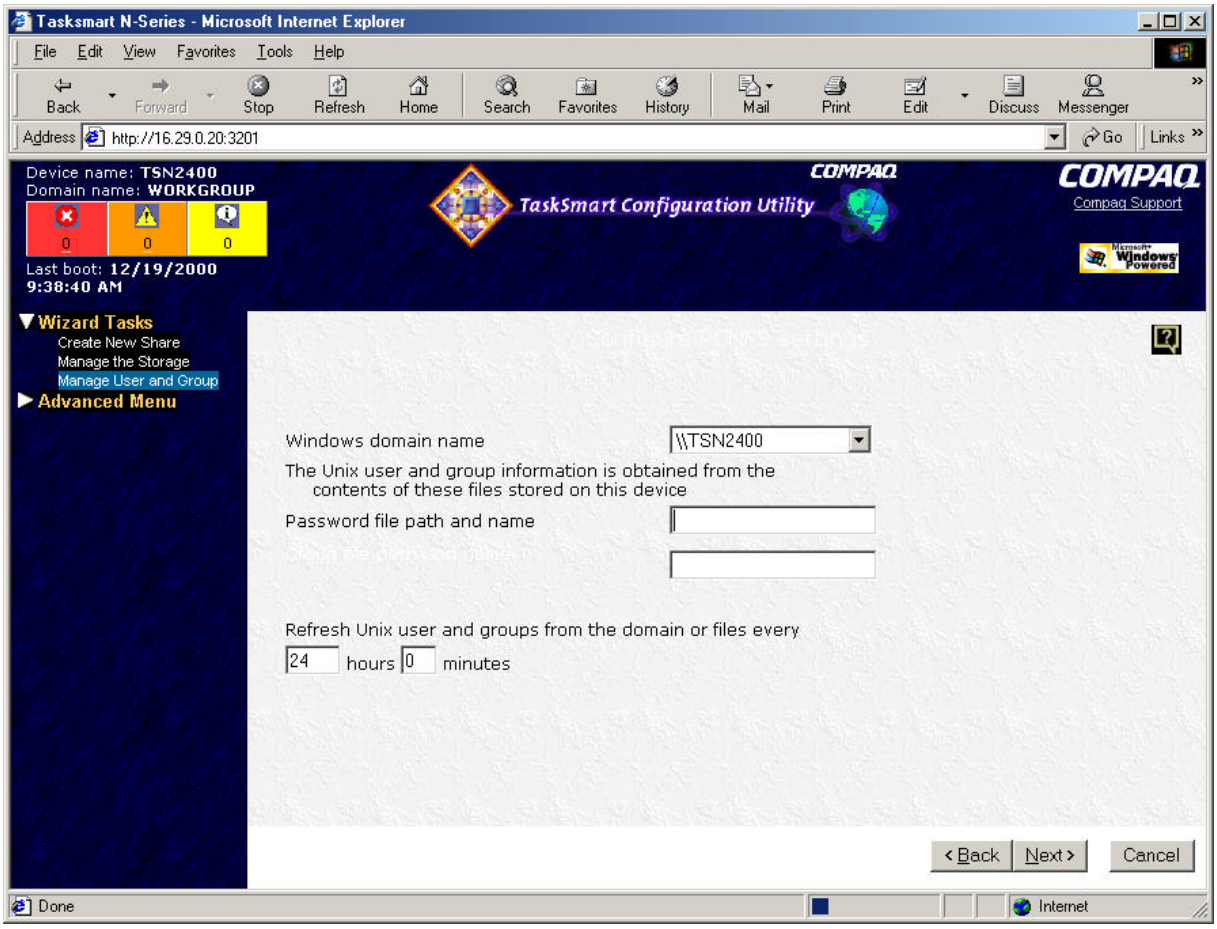
NIS mapping screen

This screen allows the administrator to define the Network Information Services (NIS) mapping settings. The administrator must supply the NIS Domain Name. They can also provide the NIS Server Name.



PCNFS mapping screen

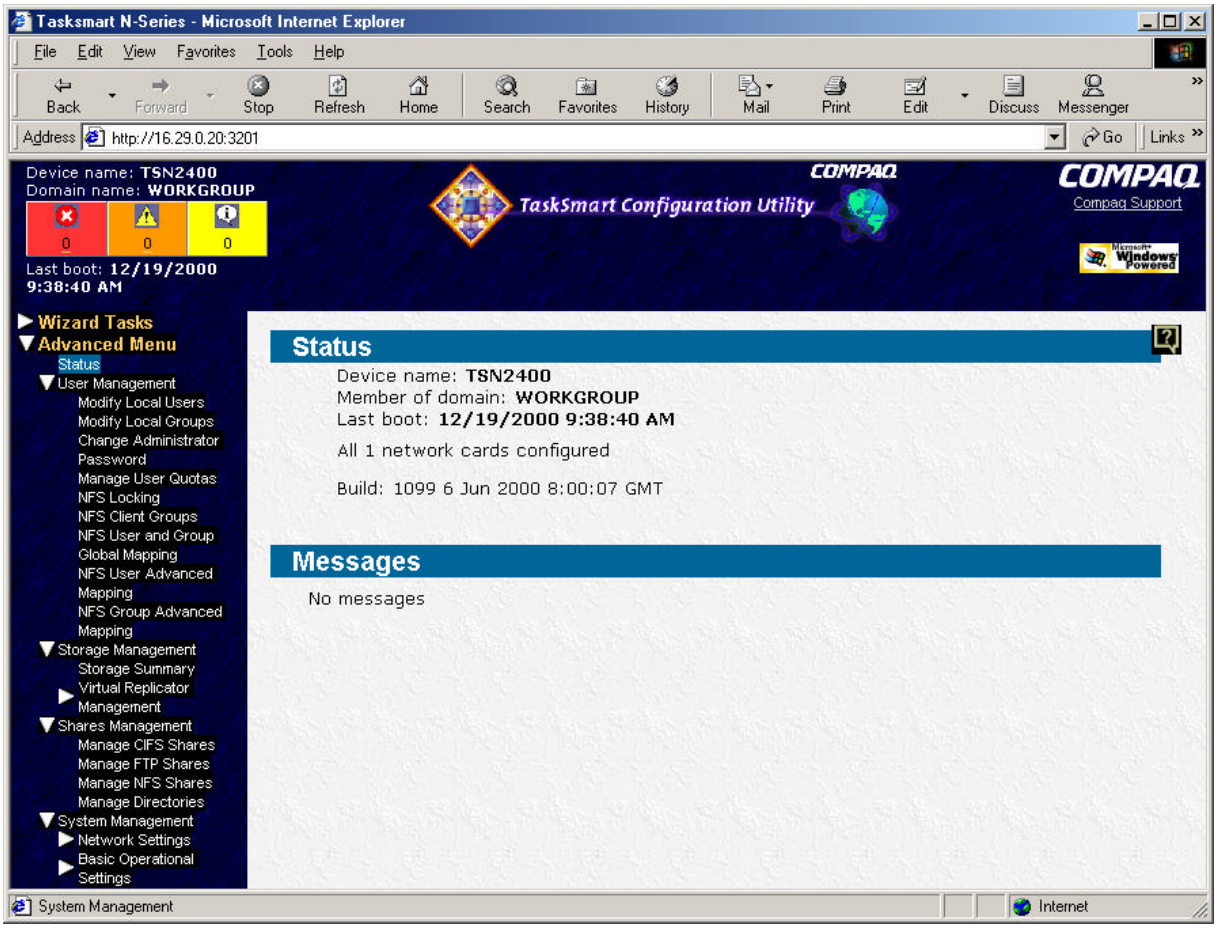
This screen allows the administrator to define the Personal Computer Network File System (PCNFS) mapping settings. The administrator must supply the password file path, password filename, group path, and group filename.



Advanced Menu

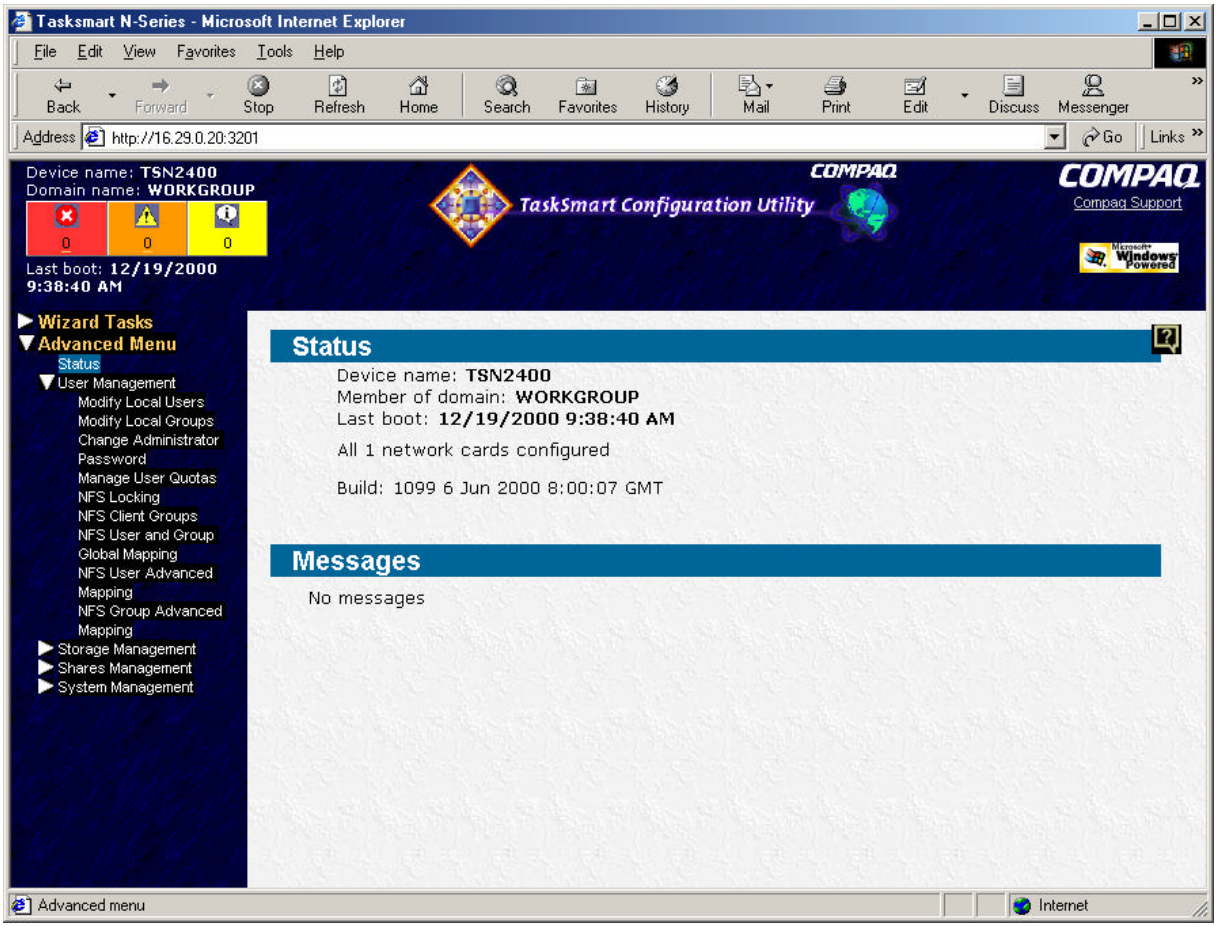
The Advanced Menu provides the tools necessary to perform advanced operations on the N2400. These incluse:

- Status - The **Status** page shows the current status of the appliance and includes the device name, domain name, last boot time, build version, network interface card information, and messages.
- User Management – Used to setup and manage user accounts.
- Storage Management - Used to setup and manage storage.
- Shares Management - Used to setup and manage shares.
- System Management – Used for general system manament.



User Management

The User Management options are used to perform the following:



Modify Local Users

The **Modify Local Users** page lists the current local user accounts and allows the system administrator to manage the local user account settings. The system administrator can create new user accounts, delete user accounts, set user account passwords, or edit user account properties.

Modify Local Groups

The **Modify Local Groups** page lists the current local user group and allows the system administrator to manage the local user group settings. The system administrator can create a new user group, delete an existing user group, or edit the properties of an existing user group.

Change Administrator Password

The **Change Administrator Password** page allows the system administrator to change the local administrator password. The system administrator must enter the current administrator password before the new password will be effective. The password cannot be blank.

Note: This page cannot be used to change the domain administrator password.

Manage User Quotas

Drive quotas enable system administrators to control the allocation of drive space to individual users or groups of users. When quotas are enabled and properly configured, it is impossible for one person or group to consume all the available space on a drive.

When quotas are enabled on a volume that already contains files, Windows calculates the drive space used by all users on the volume. The quota limit and warning level are then applied to all current users, and system administrators can modify quotas as needed.

NFS Locking

The Network File System (NFS) can lock access to files, preventing multiple users from editing the file simultaneously. The NFS has support for this action. NFS locking is optional.

NFS locking depends on the software application components to manage the locks. If an application does not lock a file, nothing prevents a user from overwriting it.

The waiting period setting determines how long the TaskSmart N2400 appliance allows the locks to be kept active after a client or server crash. The TaskSmart appliance will allow the locks to be active for the designated number of seconds, while querying the client to see if it wants to keep the lock. If the client responds within this timeframe, the lock will be kept active. Otherwise, the TaskSmart appliance clears the lock.

The locking user interface also allows the administrator to manually clear any locks that might remain open after a client or the TaskSmart N2400 appliance loses power.

Global Mapping

The NFS User and Group Global Mapping page allows the administrator to create general guidelines on how user and group identification from one environment is translated into another environment. The administrator can also enable advanced mapping (configured on the NFS User Advanced Mapping and NFS Group Advanced Mapping pages) by checking the Simple maps checkbox.

Choose the Windows domain from the Windows domain name drop-down menu. Multiple names will be listed only if domain trusts have been established. Choose either to set global mapping with the Network Information Service (NIS) or with the Personal Computer Network File System (PCNFS) by clicking the appropriate radio button. If NIS is selected, the NIS domain name should be typed by the administrator in the indicated space. The NIS server name can also be entered. If PCNFS is selected, the administrator should enter the password file path and name, and the group file path and name in the appropriate areas.

The device can be set to refresh UNIX user and group information on a cyclical basis by entering the desired time frame.

Note: All changes to this page must be followed by clicking OK before they become effective.

NFS User Advanced Mapping

Advanced (explicit) mapping allows the administrator to specifically decide how matching is accomplished. The administrator manually lines up the Windows NT and UNIX user names.

When multiple Windows users are mapped to a single UNIX user, advanced mapping requires a primary user to be selected. The primary user can be set by highlighting the selected user, clicking **Set Primary**, and then clicking **OK**. A primary user is indicated in the **Mapped users** window by an asterisk (*). If the administrator does not select a primary user, the map created first will be considered primary.

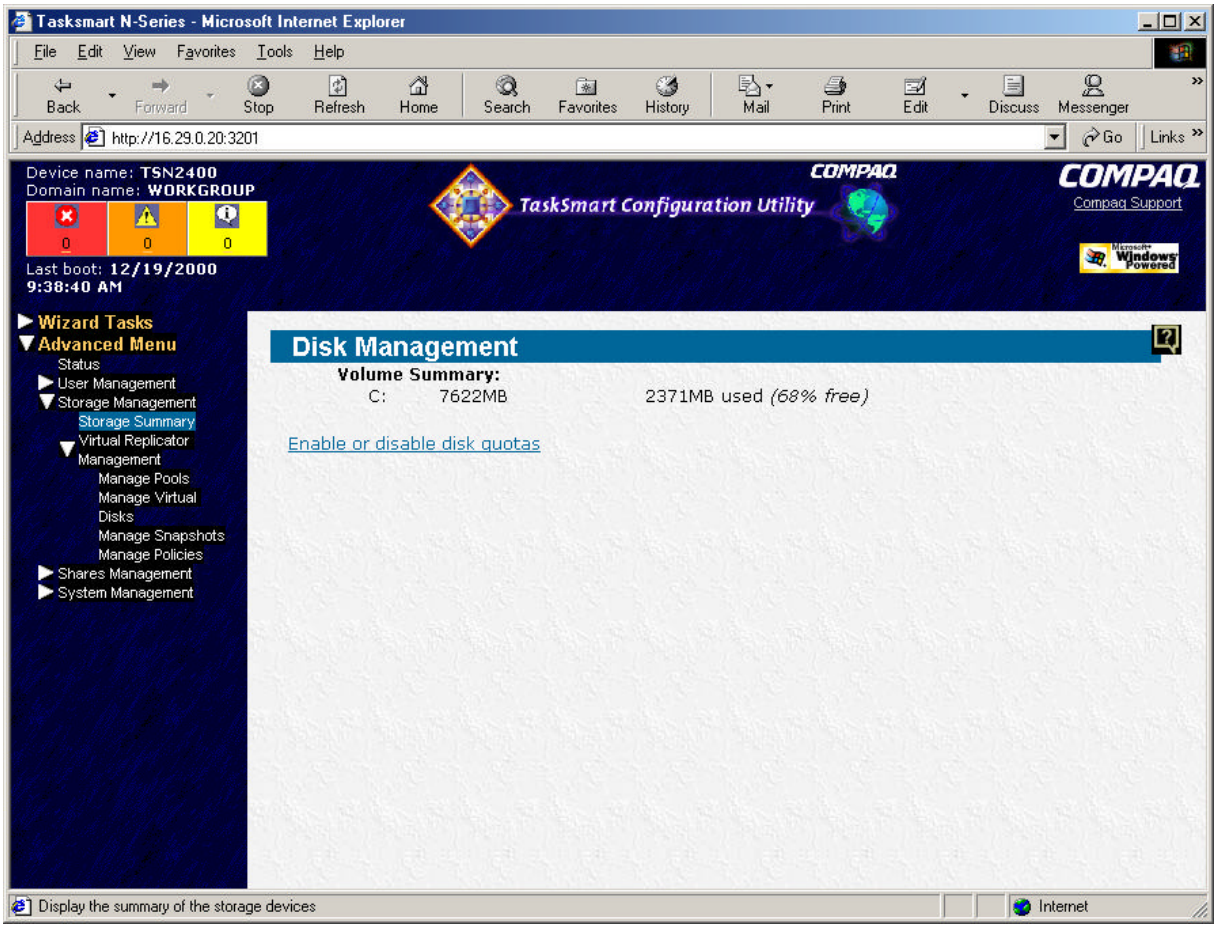
NFS Group Advanced Mapping

Advanced (explicit) mapping allows the administrator to specifically decide how matching is accomplished. The administrator manually lines up the Windows NT and UNIX group names.

When multiple Windows groups are mapped to a single UNIX group, advanced mapping requires a primary group to be mapped. The primary group can be set by highlighting the group, clicking Set Primary, and then clicking OK. A primary group is indicated in the Mapped groups window by an asterisk (*). If the administrator does not select a primary group, the map created first will be considered primary.

Storage Management

The Storage Management options are used to perform the following:



Storage Summary

The **Storage Summary** page lists the volumes that are present on the device. It also shows both the amount (in megabytes) of storage that is being used on the volume and the percentage of free space that is available on the volume.

When Enable or disable disk quotas is clicked, the Enabling quotas screen is displayed. Check the boxes in front of the drives on which you want to enable quotas. Click **OK** to have the device carry out the operation.

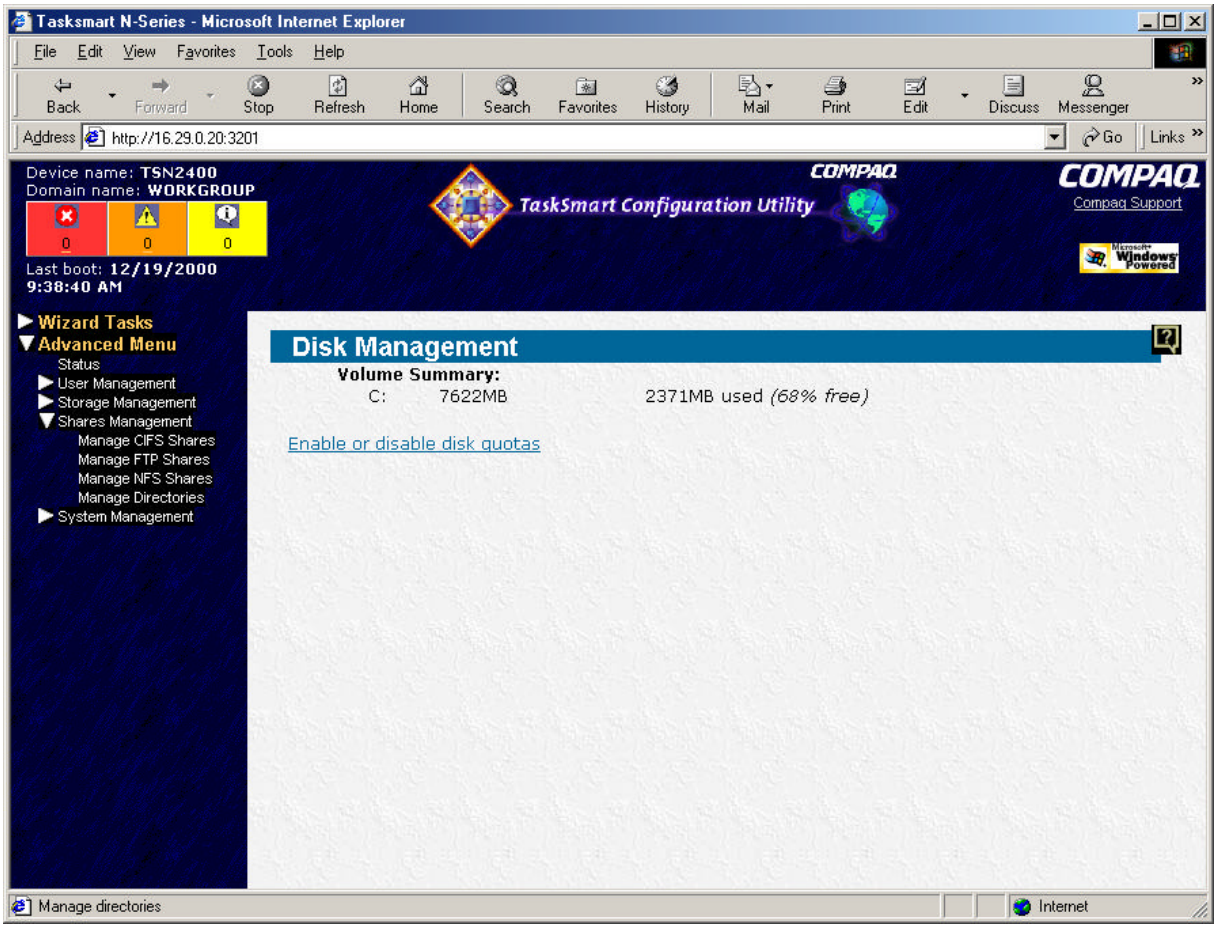
To disable quotas uncheck the boxes in front of the drives on which you want to disable quotas. Click **OK** to have the device carry out the operation.

Virtual Replicator Management

Compaq SANworks Virtual Replicator (SWVR) provides advanced, centralized storage management capabilities in Microsoft Windows NT and Windows 2000 computing environments. Innovative storage management features simplify storage configuration and management, and enhance availability and scalability.

Storage Management

The Storage Management options are used to perform the following:



Manage CIFS Shares

The **Manage CIFS Shares** page lists current CIFS shares and allows the system administrator to manage the CIFS shares on the device. The system administrator can create new shares, delete existing shares, or modify properties of an existing share.

Manage FTP Shares

The **Manage FTP Shares** page lists current FTP shares and allows the system administrator to manage the FTP shares on the device. The system administrator can create new FTP sites, create new virtual directories, delete existing FTP sites or virtual directories, or modify properties of existing FTP sites or virtual directories.

Manage NFS Shares

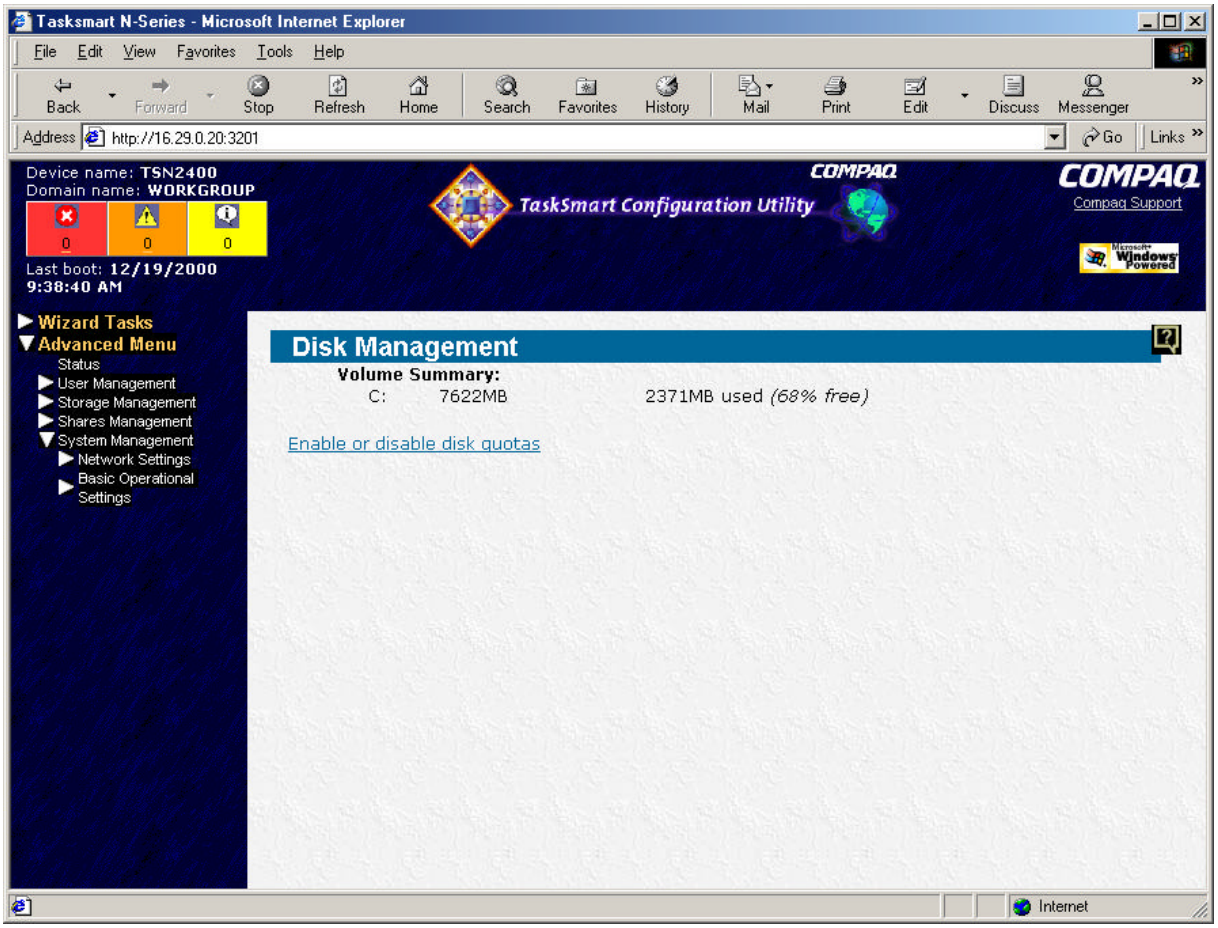
The **Manage NFS Shares** page lists current NFS shares and allows the system administrator to manage the NFS shares on the device. The system administrator can create new NFS shares, delete existing NFS shares, or modify properties of an existing NFS share.

Manage Directories

The **Manage Directories** page lists the directories in the file system and allows the system administrator to manage the file system on the device. On first entry to this page, the drive letters of the fixed drives on the device are listed. The system administrator can open a selected directory, create new directories, delete existing directories, and modify properties of an existing directory.

System Management

The System Management options are used to perform the following:



Change Device Identity

The **Change Device Identity** page allows the system administrator to set up the device name, the domain or workgroup name in which the device resides, the default DNS suffix, and the domain username and password. The changes will not be applied until the user clicks the **OK** button at the bottom of the screen. If the changes are applied successfully, a restart page will be loaded. The changes will not be effective until the device is restarted.

A legal device name can only contain letters (A-Z, a-z), digits (0-9), and hyphens (-). The device name cannot be a number (e.g., 43820).

If the device is joining a new domain, a valid domain username and password must be entered.

Network Configuration

The **Network Configuration** page allows the system administrator to set up the global network configuration that applies to all network adapters. The system administrator can set up the DNS suffixes and the host file.

The system administrator can choose either to append the primary DNS suffix or to append the primary DNS suffix and parent suffixes. The system administrator can also choose to append specific DNS suffixes included in the textbox. If **Append Specific DNS Suffixes** is chosen, at least one valid DNS suffix must be entered in the textbox.

The system administrator can also edit the host file on the device. The host file is located in the following path: %Windows System Path%\drivers\etc\hosts. The file contains static mapping of IP address to the host name. There are instructions in the default host file on how to add new mapping to the host file.

Configure SNMP Service

The **Configure SNMP Service** page allows the system administrator to set up the Simple Network Management Protocol (SNMP) service on the device. SNMP service must be installed before this page can be used. The system administrator can specify the device contact, location, community name, and trap destination.

The system administrator can also specify an accepted community name. Each community will have its own community rights setting. There are five different community rights settings: Read Create, Read-Write, Read Only, Notify, and None.

The system administrator can set the network to accept SNMP packets from any host, or from specified hosts only.

The Web user interface has no support for the following: multiple community names, different service types, and send authentication traps.

(These are supported by the Microsoft Management Console (MMC) User Interface.)

Web Access Restrictions

The **Web Access Restrictions** page allows the system administrator to specify which clients can access the Web user interface on the device. The system administrator can either enable all network adapters, or choose just the network adapters that have static IP addresses. The system administrator cannot set Web access restrictions to network adapters that use dynamic IP addresses.

View Event Logs

The **View Event Logs** page allows the system administrator to read and manage the system log, the application log, and the security log on the device. The system administrator can read the details of an individual event log by selecting the log and clicking the **Properties** button. The system administrator can also clear all event logs.

After clicking **Properties** on a selected log, a new page with details of the log will be shown. The date, time, type, source, category, ID, and description of the log are shown. The information shown is not editable. The user can click the **Close** button to go back to the **View Event Logs** page.

After clicking the Clear All Events button, a confirmation message will appear, asking the user to confirm the action. After **OK** is clicked, all the event logs will be cleared.

NFS & IIS Logs

The **NFS & IIS Logs** page allows the system administrator to read and manage the NFS and IIS logs. A drop-down menu allows the system administrator to choose between the NFS log and the IIS log. Before this page can be used NFS logging and IIS logging must be turned on.

When the NFS log is selected in the drop-down menu, the system administrator can read the NFS log or clear the log file. Only the most recent 300 lines from the log file are shown. If the NFS logging option is not turned on, an error message is shown. After clicking the **Clear** button, a confirmation page will be displayed. The device will not clear the logs until the system administrator clicks **OK** on the confirmation page.

When the IIS log is selected in the drop-down menu, another window is displayed. It lists existing IIS logs. The system administrator can read the IIS log, download log files, and delete log files. By highlighting any existing log, the system administrator can view the details of that log. The IIS logging settings must be configured to start a new log file when the file exceeds a certain size. The suggested setting is 1 MB. If the IIS logging settings are not configured correctly, an error message is shown. If the IIS logging settings are configured correctly, the IIS log page will show all existing log files and the top 300 lines in the files.

Unwanted individual logs can be deleted. Highlight the unwanted file, and click **Delete**. After clicking **Delete**, a confirmation page will be displayed. The device will not delete the logs until the system administrator clicks **OK** in the confirmation page.

Set Date and Time

The **Set Date and Time** page allows the system administrator to set the date, time, and time zone of the device. Daylight Saving Time is automatically calculated.

Shut Down or Restart Device

The **Shut Down or Restart Device** page allows the system administrator to shut down or restart the device. By marking the corresponding radio button and clicking **OK**. After **OK** is clicked, no confirmation page appears. The device shuts down or restarts without any further input from the administrator.

Upgrade Options

Table 2: Options and Spare Part Numbers

Description	Part Number
NC6132 Gigabit Ethernet Fiber Network Interface Card	TBS

Service Considerations

- The Pentium III processor cannot be down-clocked; therefore, all processors must use the same frequency. Compaq does not support mixing processor frequencies.
- During POST, each processor and its initialization frequency is displayed. If POST detects processors of unlike frequency, ROM halts the system.

Important Notes

! **Important**

Class B Regulatory Information—Your server currently complies with the FCC Class B requirements for digital devices. To maintain compliance with Class B regulations, you must install the enclosed material according to the instructions for this upgrade kit. Failure to follow these instructions may void the user's authority to operate the equipment.