COMPAQ
Technical Guide

April 2001
14MM-0501A-WWEN
Prepared by:
Industry Standard Server Division
Compaq Computer Corporation

Contents

Compaq TaskSmart N-Series Appliance Network Attached Storage Deployment Guide

Abstract: This guide is provided to assist Compaq customers in executing Network Attached Storage (NAS) deployments using Compaq TaskSmart N-Series appliances. It is intended to assist customers to do the following:

- Understand basic setup and configuration
- Integrate NFS, CIFS and NCP clients into a single storage-based architecture
- Address performance concerns as they relate to deployment

Introduction

Often times, one of the most time-consuming issues associated with new server and storage equipment is the deployment, especially if the new equipment is also a new product on the market. Planning issues are usually the most complex, but sometimes the sheer volume of equipment that is planned for can require a large amount of resources to deploy. The Compaq *TaskSmart*™ N-Series appliance has been designed to help alleviate some of these deployment issues so that IT managers can focus the bulk of their time analyzing existing infrastructures and planning for new infrastructures.

Deployment Issues

Several issues are associated with any new server deployment.

- What specific tasks are assigned to the new servers?
- Where should the servers be placed physically?
- How should these new servers be configured?
- Will staff be familiar with the setup program(s)?
- Where are the integration points with the existing infrastructure and eBusiness architectures?
- How can the new servers best integrate disparate technologies?

There are other potential questions, but these can serve as a starting point for a deployment discussion. In any event the TaskSmart N-Series appliance has attempted to address these issues by leveraging an industry standard collection of hardware and software so that deployment is simple and easy to manage.

Appliance Setup and Configuration

Setup and configuration entail two steps. First, the hardware itself must be set up. Second, the software must be installed and configured. Setting up hardware for the TaskSmart N-Series appliance will be quite familiar to users of industry standard servers and storage devices. The server head is based on a Compaq *ProLiant*™ DL380 server. The external storage devices are Compaq *StorageWorks*™ enclosures. The appliance uses the Compaq Ultra3 Universal hot-pluggable LVD SCSI hard drive.

Thus, the hardware is similar to the most commonly deployed ProLiant and StorageWorks industry standard hardware. As such, it can even be leveraged for cross-deployments throughout the ProLiant, *AlphaServer*™, and StorageWorks product lines. Hardware deployment problems are minimized because the deployment techniques – rack mounting, cable management, and cross-compatibility – are the same for the TaskSmart N-Series as for other Compaq industry standard products.

The software, then, is where most deployment work will actually be done. The nice thing about the TaskSmart N-Series appliance, however, is that because it is dedicated to a single task, it is already pre-configured and pre-optimized for that task. The only configuration tasks that remain are those that are particular to a given customer's existing infrastructure:

- Network settings
- Disk carving and snapshot planning
- User and group account integration
- CIFS share and NFS export settings
- Novell Integration
- Remote server deployments

Since many of these issues are already covered in the associated white paper, *Planning for Network Attached Storage on Compaq TaskSmart N-Series Appliances*, this document will focus on the particulars of the actual deployment aspects, referring readers to the planning technical guide where appropriate.

TaskSmart Configuration Utility

Each TaskSmart N-Series appliance ships with a CD that contains the TaskSmart Configuration Utility. This utility allows administrators to go through a series of standard wizard screens, answering questions about the configuration of TCP/IP, DNS, WINS, SNMP, and Remote Insight Lights-Out Edition Board configuration. The TaskSmart Configuration Utility writes this information to a diskette, which is then inserted into the appliance during setup, so that the settings are automatically applied.

The TaskSmart Configuration Utility is a Win32 application designed to run on any standard Windows client, such as Windows 95, Windows 98, Windows NT, or Windows 2000. Each of the wizard screens has been designed to closely mimic standard Windows or Java configuration dialogs, so that users will have a short learning curve.

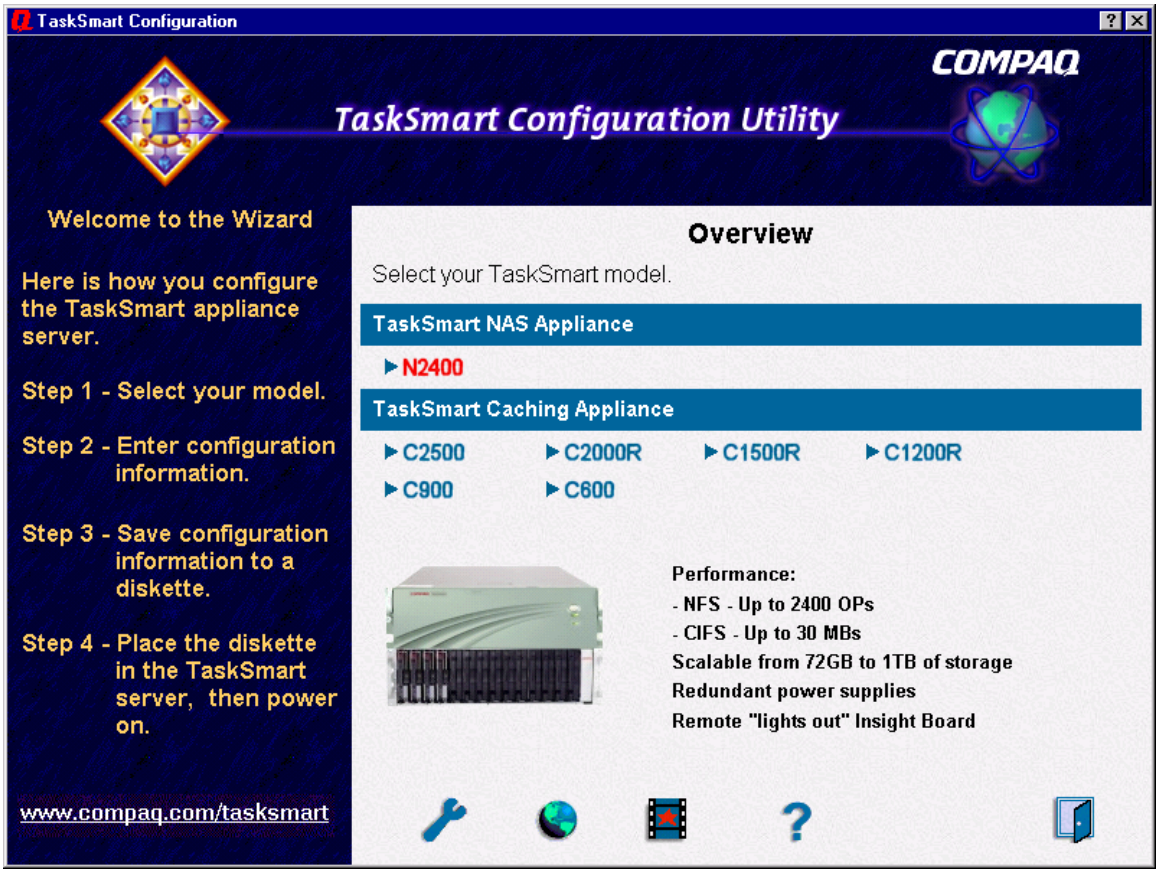

Figure 1: TaskSmart Configuration Utility initial screen

The TaskSmart Configuration Utility includes configuration paths for all TaskSmart appliances, including the C-Series of caching appliance servers. To configure a TaskSmart N2400, click **N2400** to display the following screen:

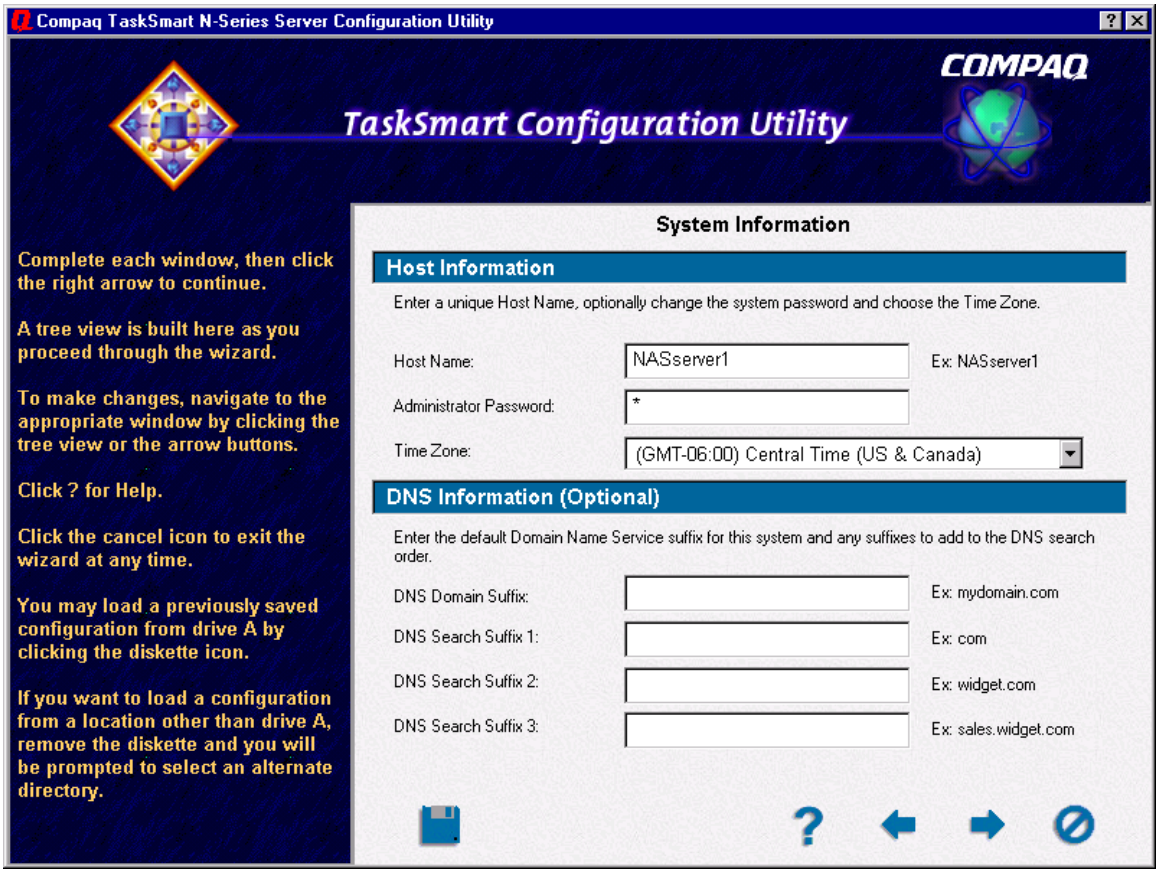

Figure 2: TaskSmart N2400 System Information screen

This initial screen allows the administrator to enter the Host Name, Administrator Password, Time Zone, and DNS Domain Information. The Administrator password is stored on the diskette in free text, so the recommended configuration setting is "*", which leaves a blank password on the appliance. The Administrator should then change this password immediately upon deploying the appliance. Help is available at any time by clicking the "?" button at the bottom of the screen. Once appropriate information is entered, the administrator can move to the next screen by clicking the right-arrow button. Click the left-arrow button to move to a previous screen.

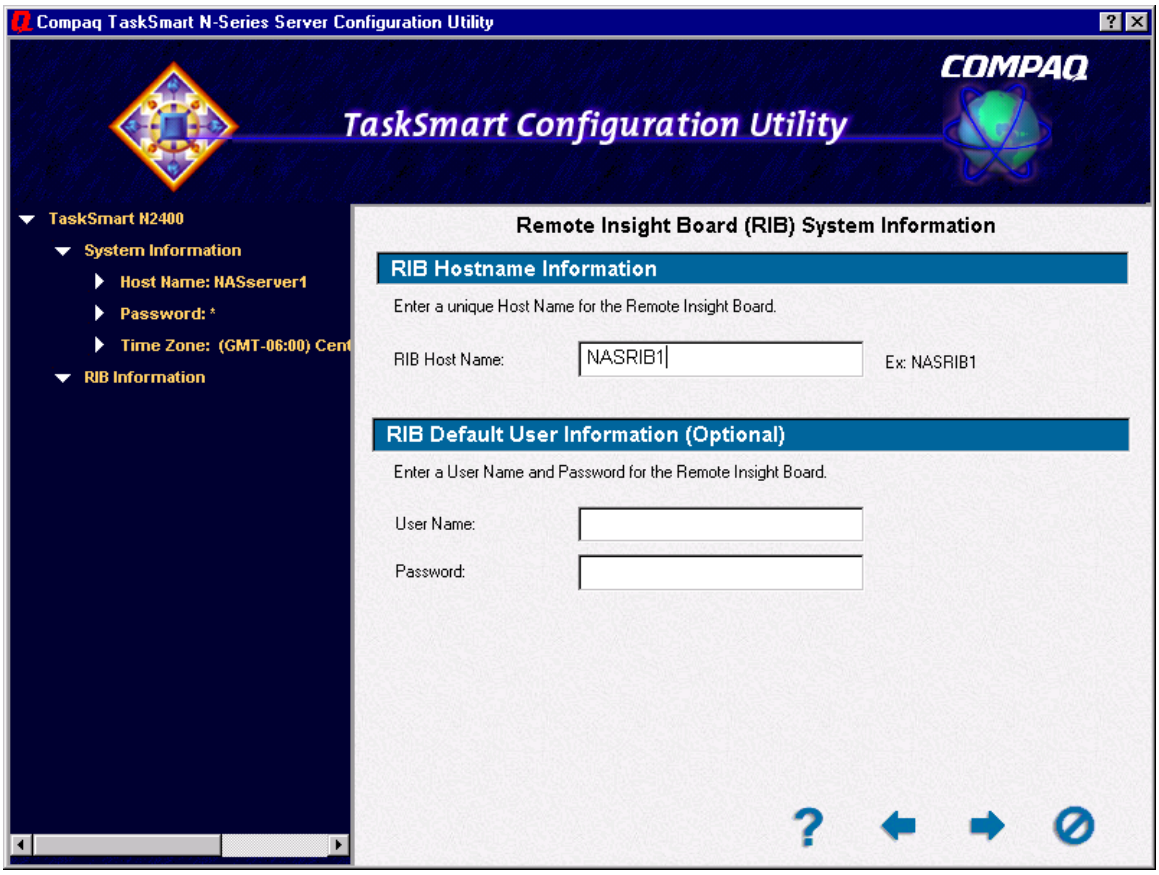

Figure 3: TaskSmart N2400 Remote Insight Board configuration screen

The Remote Insight Lights-Out Edition board is a standard feature of every TaskSmart N-Series appliance. The next screen that displays allows the administrator to enter basic Remote Insight Lights-Out Edition board configuration information, including the Host Name of the Remote Insight Lights-Out Edition board, and the Administrator's User Name and Password. Again, the password is stored in free text on the TaskSmart Configuration diskette, so it is best to enter a temporary or blank password here and then change that password on initial remote login to the Remote Insight Lights-Out Edition board. Additional information on the Remote Insight Board Lights-Out Edition board is available at the following URL:

www.compaq.com/manage/remote-lightsout.html

Note: The left-hand pane on the TaskSmart Configuration Utility stores summary information of the settings entered so far.

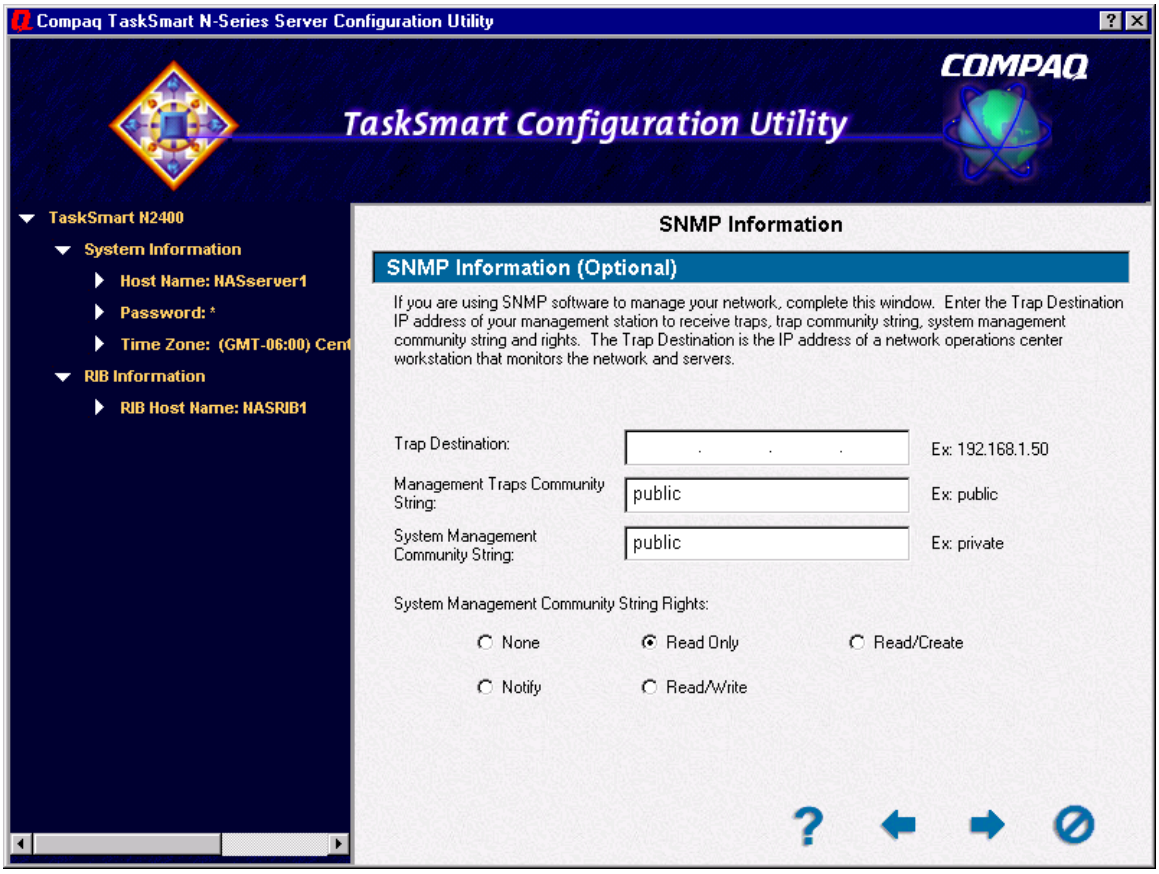

Figure 4: TaskSmart N2400 SNMP configuration screen

The next screen in the TaskSmart Configuration Utility allows the administrator to enter SNMP settings so that the TaskSmart N-Series appliance is immediately manageable from a remote Enterprise Management Workstation, such as a *Compaq Insight Manager*™ Console or an HP OpenView or Tivoli NetView management console. The Trap Destination is the IP address of the remote management console or the remote collection point for SNMP trap information. The two Community Strings are those used by the SNMP protocol to gain access to management data or to send SNMP write packets to the appliance. The System Management Community String Rights entail the access level that system management workstations have to the server. Read Only is required to view management data. Read/Write or Read/Create is required if remote SNMP interaction, such as when a remote restart is initiated. SNMP is a rather insecure protocol, so it may be most effective to leave the rights as Read Only, using the Remote Insight Lights-Out Edition board, which requires a secure authentication to gain access, for such remote tasks as resetting the server.

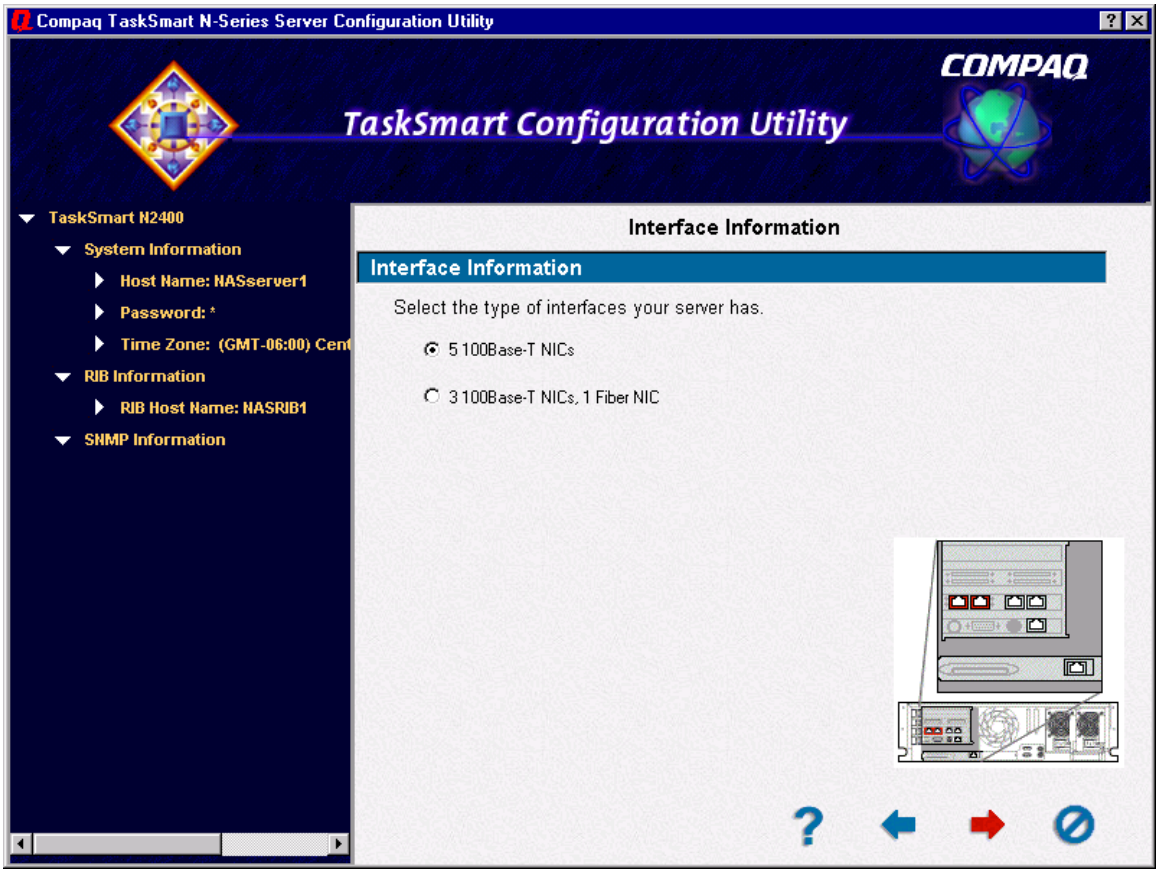

Figure 5: TaskSmart N2400 Interface Information screen

The next screen in the TaskSmart Configuration Utility allows the administrator to choose what type of network interface controllers (NIC) to configure. The choices are as follows:

- 5 100Base-T NICs
- 3 100Base-T NICs, 1 Fiber NIC

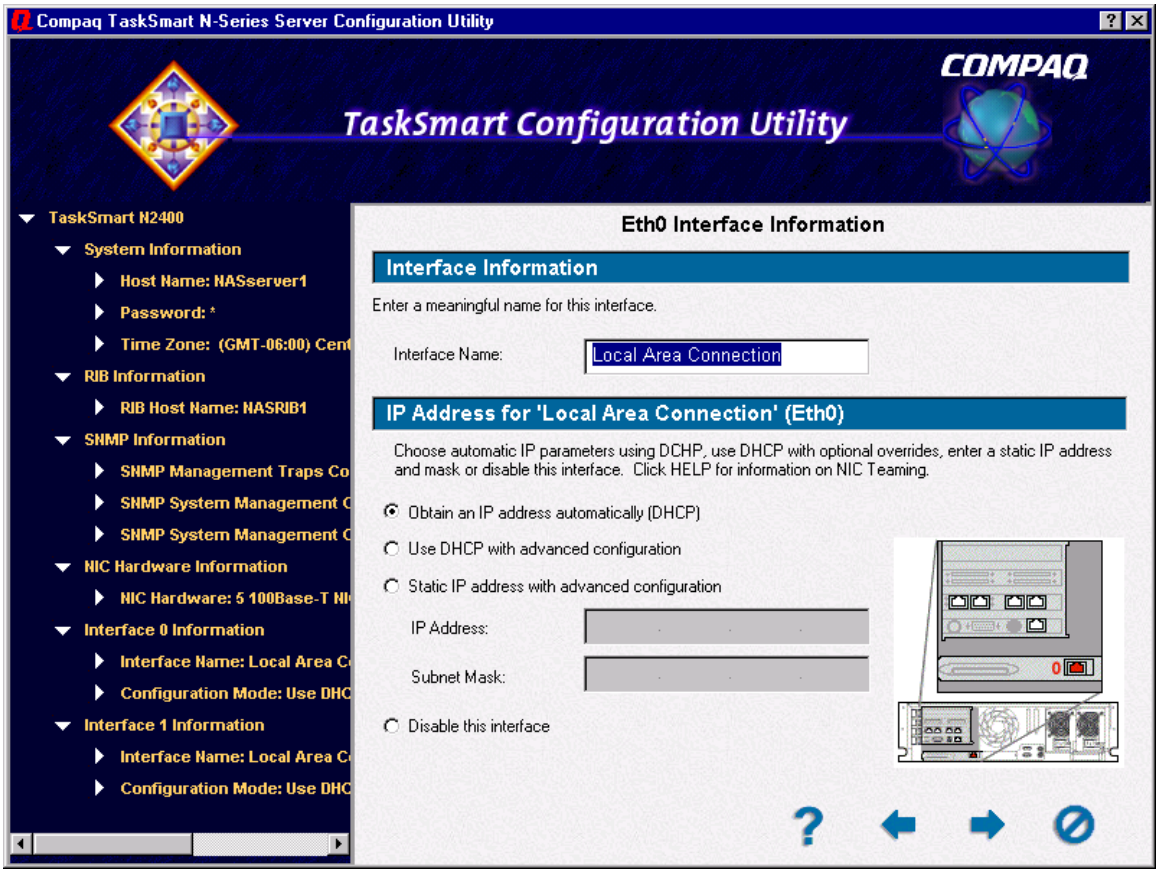

Figure 6: TaskSmart N2400 network configuration screen

The next six screens allow for offline configuration of the six network interfaces on the N2400 appliance, including the network interface used by the Remote Insight Lights-Out Edition board. Five of those interfaces are usable for server data traffic. The sixth screen, the Remote Insight Lights-Out Edition board interface, is only used to gain access to the Remote Insight Lights-Out Edition board, and thereby, gain access to the server remote console. Each of these interfaces can be given a logical name, such as "Local Area Connection *x*," and each can be configured with a static IP address or to obtain an IP address from a DHCP server. In addition, interfaces that will not initially be used can be disabled.

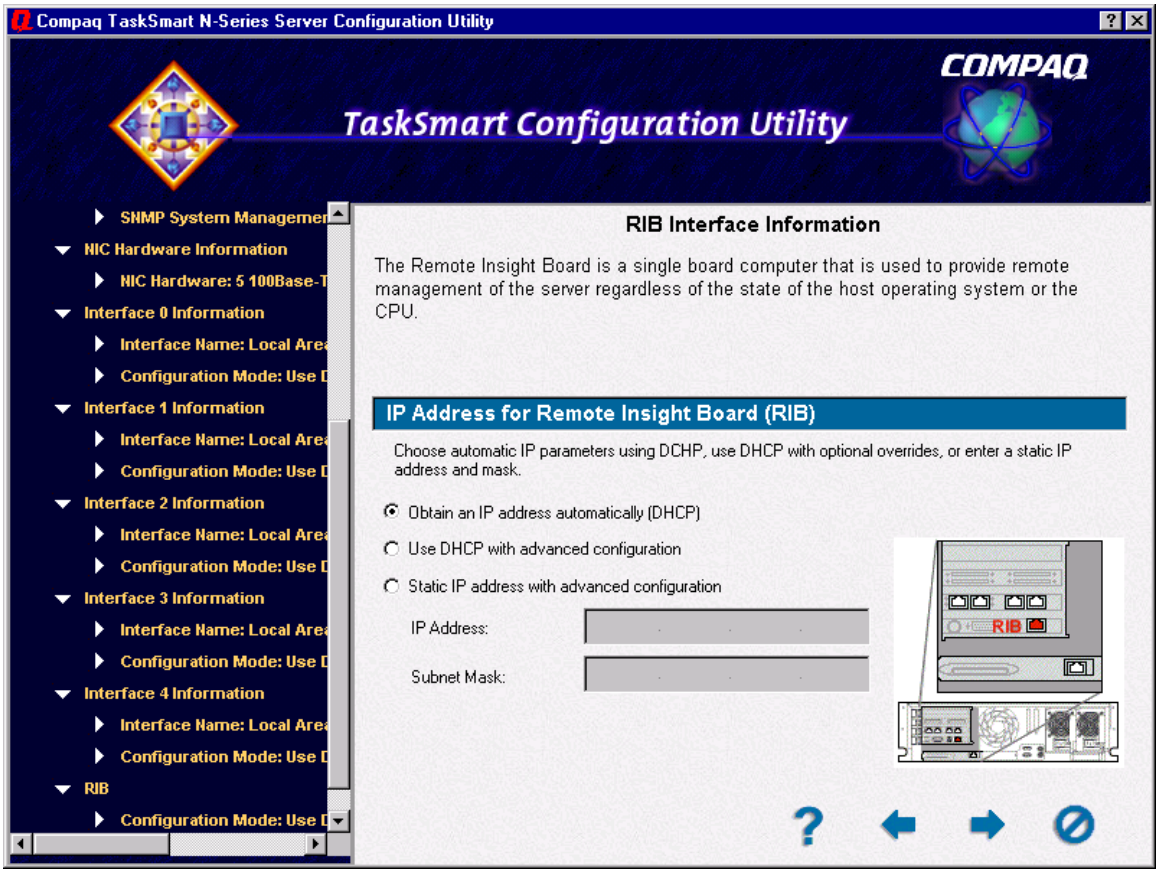

Figure 7: TaskSmart N2400 Remote Insight Lights-Out Edition Board Configuration screen

The Remote Insight Lights-Out Edition board interface cannot be disabled and no logical name (other than Remote Insight Lights-Out Edition board) is associated with it.

Note: There are no such options for disabling the Remote Insight Lights-Out Edition board on its configuration screen. However, it can be configured with a static or dynamic IP address.

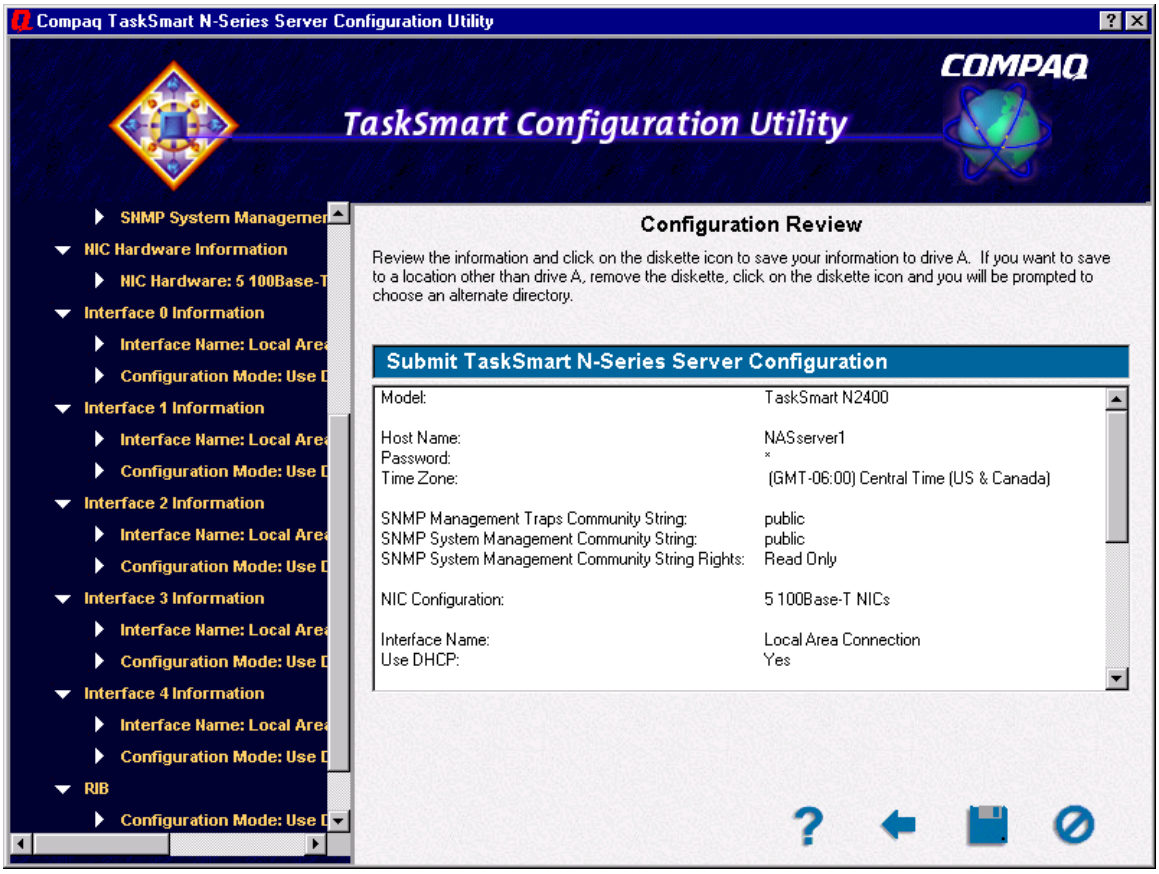

Figure 8: TaskSmart N2400 Summary screen

The final screen summarizes the information entered. To write it to any diskette, click the diskette icon. When complete, the diskette must be removed from the client machine and then inserted immediately into the diskette drive of the TaskSmart N2400. The diskette will not boot because the boot capability has been disabled on the system. For those occasions when a diskette boot is necessary (such as when applying a *ROMPaq*™), the appliance interface provides a mechanism to enable diskette boot once, after which it will be disabled again. See the *Compaq TaskSmart N2400 Administration Guide* for more details. Moreover, the Remote Insight Lights-Out Edition board included with each TaskSmart N-Series appliance allows for virtual diskette boot by uploading a raw diskette image to the board over the network. See the following URL for details:

www.compaq.com/manage/remote-lightsout.html

Usefulness of the TaskSmart Configuration Utility

Since the TaskSmart Configuration Utility can be run anywhere with data stored to any diskette, system administrators can control the often complex network and SNMP settings themselves in any deployment scenario. Then, should the scenario require deployment at a remote site, the administrator can ship the diskette along with the equipment that is sent to the remote site. Alternatively, the configuration files themselves can be emailed to the remote site for instantaneous delivery. The individual charged with remote site setup, then, is merely required to appropriately rack-mount the hardware and connect the Ethernet cables. The TaskSmart Configuration diskette is then inserted, and once complete – it takes about 10 to 20 minutes – the remote administrator can access the TaskSmart N-Series appliance over the appropriate network to complete configuration of disk carving, CIFS shares, NFS exports, and user and group account integration.

The TaskSmart Configuration Utility does not support initial configuration of Compaq NIC Teaming, a feature that allows for multiple NIC interfaces to be set up in a load-balancing or fail-over configuration. This feature can be installed by double-clicking on the icon on the desktop. After being installed, NIC Teaming can be configured after the initial setup runs by double clicking on the NIC Teaming configuration tool in the TaskSmart N-Series Control Panel. Further information is available in the appliance administration guide, which ships with each TaskSmart N-Series appliance.

Advanced Data Guarding

The Advanced Data Guarding technology is a revolutionary RAID technology that has been integrated into the Smart Array 5300 and in the new TaskSmart N2400.

Advanced Data Guarding technology offers the best combination of fault tolerance and usable disk space among RAID levels.

This patented Compaq technology allows customers to safely deploy large capacity disk drives and to create very large storage volumes without expensive overhead to protect their business critical data. This technology also gives customers more flexibility in responding to drive failures without the fear of costly server downtime.

Advanced Data Guarding provides the following benefits:

- Improved data protection over traditional RAID levels
- Lower cost to implement than RAID 1
- Ideal RAID level for large capacity disk drives
  - Longer rebuild times can leave an array exposed for lengthy period
  - 36-GB drive can take as long as 30 hours to rebuild depending upon rebuild priority (20MB/minute rebuild time)
- Density - greater usable capacity per U than RAID 1
  - Fewer drives that lower power consumption and heat
- Flexibility to respond to drive failures at remote sites

Advanced Data Guarding protects against multiple disk drive failures while only requiring the capacity of 2 drives in an array of up to 56 disk drives to be set aside for dual sets of distributed parity data. It provides data protection greater than RAID 0+1 or 10 while having the capacity utilization efficiency similar to RAID 5.

Advanced Data Guarding is a standard feature of the Smart Array 5304 controller and is compatible with Compaq Proliant servers and StorageWorks enclosures. It can support a maximum of 2TB of data utilizing 36-GB Ultra3 SCSI disk drives from a single PCI slot.

The Smart Array 5300 controller with Advanced Data Guarding is also integrated into the new Task Smart N2400 NAS appliance.

Disk Carving

The planning guide goes over several disk carving issues, noting relative drive size and performance scalability potential of different carving schemes. This guide does not repeat that. Instead it goes over specifically how disk carving affects deployment. And the good news is that it really has little effect at all.

Specifically, the TaskSmart N-Series appliance will automatically carve up its attached storage at the time it is deployed. First, it creates RAID 5 arrays out of the physical hard drives. Depending on the number of physical hard drives available, up to four 14-drive RAID arrays are created. If an odd number of drives are present, for example, a number of drives not evenly divisible by 14, such as 52 – then 14-drive arrays are created for each RAID array for the first 14, 28, 42, or 56 drives available. Then, the remaining drives are placed into a single RAID 5 array. If there are not enough remaining drives available to create a full RAID 5 set, then they are left unconfigured. The TaskSmart N-Series appliance defines four as the minimum number of drives necessary to create a RAID 5 array. Even though three drives are the practical minimum, it is recommended that at least four drives be deployed per RAID 5 array so that the disk space lost to parity is minimized. Thus, the automatic configuration tool also reflects this recommendation.

Table 1 documents some samples:

Table 1. Disk carving examples

Number of Physical Disks	RAID Array Topology
4	1x4-drive RAID 5 Array
7	1x7-drive RAID 5 Array
10	1x10-drive RAID 5 Array
14	1x14-drive RAID 5 Array
16	1x14-drive RAID 5 Array with 2 drives left unconfigured because a minimum of 4 drives is required for effective RAID 5
17	1x14-drive RAID 5 Array with 3 drives left unconfigured because a minimum of 4 drives is required for effective RAID 5
18	1x14-drive RAID 5 Array 1x4-drive RAID 5 Array
24	1x14-drive RAID 5 Array 1x10-drive RAID 5 Array
28	2x14-drive RAID 5 Arrays
32	2x14-drive RAID 5 Arrays 1x4-drive RAID 5 Array
38	2x14-drive RAID 5 Arrays 1x10-drive RAID 5 Array
42	3x14-drive RAID 5 Arrays
46	3x14-drive RAID 5 Arrays 1x4-drive RAID 5 Array
52	3x14-drive RAID 5 Arrays 1x10-drive RAID 5 Array
56	4x14-drive RAID 5 Arrays

Depending on specific drive configurations, other default disk carving setups are possible, but these samples offer a sketch of the likely possibilities for a few specific configurations.

Note: The administrator can manually carve up RAID logical drives, using some of the ideas presented in the planning guide, but these are the default automatic setups.

After the RAID arrays are built, automatic disk carving continues. Each RAID 5 array is presented as a single logical drive. Then, the automatic disk-carving tool creates a single *SANworks*™ Virtual Replicator (SWVR) storage pool from each logical drive. Finally, 70% of the available pool storage space in each pool is presented to the operating system as an SWVR virtual disk. The remaining 30% of drive space in each pool is reserved by default for snapshots.

Disk carving at deployment can, in fact, be quite simple, if the default settings are adequate for the requirements of a particular customer. If not, then the planning guide provides a detailed discussion of alternate carving strategies that can be set up manually by the administrator.

Users and Groups

Once network settings are applied and disk carving completed, the next step is to integrate the TaskSmart N-Series appliance into user and group account database(s), or alternately, set up a Workgroup environment where the TaskSmart N-Series appliance maintains its own account database.

The TaskSmart N2400 supports Network File System (NFS), Network Core Protocol (NCP) and Common Internet File System (CIFS) protocols for file access over a network. CIFS is the standard network file sharing mechanism used by Microsoft Windows NT clients and servers. It is a superset of the Server Message Blocks (SMB) network file sharing protocol.

Access to CIFS shares requires a network login, providing username and password. A fundamental part of managing CIFS shares involves managing the users and groups that have access. Access to NCP shares also requires the use of a network login. This login can be accomplished using a Novell or Microsoft redirecter. The user account on the TaskSmart N2400 will be Netware-enabled, allowing the TaskSmart N2400 to emulate a Novell bindery server. Access to NFS shares does not require a username or password. However, NFS clients pass user ID (UID) and group ID (GID) information in their NFS requests. If nothing is done to integrate these UIDs and GIDs into the appliance, then all NFS clients will view file permissions as if they were user **nobody** in group **nogroup**. Moreover, there would be no translation of user and group access rights to files if a CIFS client subsequently accessed the NFS files. Thus, user and group setup is an important part of deployment.

Since the TaskSmart N-Series appliance is based on a core Windows 2000 operating system, there are two administration environments for native users and groups:

- **Workgroup.** All account information is stored locally.
- **Domain.** All account information is stored on a separate Windows NT or Active Directory Domain Controller.

Note: The appliance is not a domain controller for other servers. If user and group account information is stored locally, those accounts may be used only to authenticate logins to the appliance, resulting in a workgroup configuration.

In addition, the TaskSmart N-Series appliance will integrate into two UNIX user and group account models. Each of these account models is mapped to native accounts, resident in either a Windows Domain Controller (Domain environment) or the TaskSmart N-Series appliance (Workgroup environment):

- **passwd and group Files**: In this setup, a single pair of UNIX passwd and group files is uploaded to the TaskSmart N-Series appliance. The appliance is configured to use Personal Computer Network File System (PCNFS) as its user mapping model in the User Mapping configuration screens. The UIDs in the passwd file, with corresponding usernames, and the GIDs in the group file, with corresponding group names, are then mapped to native Windows user and group accounts. These password and group files must be updated periodically to keep them synchronized with the rest of the UNIX environment. For example, the files should be updated when new groups are added.
- **Network Information System (NIS)**: In this setup, the appliance is configured to use NIS as its user mapping model in the User Mapping configuration screens. The UIDs, with corresponding usernames, and the GIDs in the group file, with corresponding group names, are periodically and automatically downloaded from the NIS server. These users and groups are then mapped to appropriate Windows native user and group accounts.

The planning guide goes into additional detail of how to address the two different security models of Windows (and CIFS) and UNIX (and NFS). The operations guide white paper and the *Compaq TaskSmart N2400 Administration Guide* go into additional detail about the mechanics of configuring user name mapping. From a strict deployment perspective, the most important issue is knowing that the TaskSmart N-Series appliance will fit in with a particular infrastructure.

Domain Compared to Workgroup

TaskSmart appliances can be deployed in a workgroup environment or in a domain environment. As mentioned previously, CIFS is a session-based, stateful network file sharing protocol. When mapping a network drive or a client machine, a user sends a login credential to the server. This credential includes the username, password, and if appropriate, domain information. Using the credential, the server authenticates and provides the corresponding access to the user. When a TaskSmart appliance is deployed into a workgroup environment, all user and group account access permissions to file resources are stored locally on the appliance. By contrast, an appliance deployed into a domain environment uses the account database from the domain controller, with user and group accounts stored outside the appliance. The appliance integrates with the domain controller infrastructure as a member server.

IMPORTANT: The TaskSmart N2400 cannot act as a domain controller for other systems on the network.

Managing Users and Groups Effectively

Effective user and group management is dependent on how well users and groups are organized. Administrators typically create a small number of groups on the network, and then assign users to the appropriate group or groups. File system and share permissions can be applied at the group level, rather than at the user level. Since the number of groups is small, assigning the appropriate permissions to all users in a selected group, or groups, is more efficient.

Although each organization has specific conventions, following certain general guidelines makes administration simpler and more efficient. Since CIFS is dependent on users and groups to grant appropriate access levels to file shares, CIFS administration also benefits from a consistent user and group administration strategy.

Managing Usernames

Usernames should reflect a logical relationship between the username and the user who uses the account. It is important that rules are established to ensure usernames are as follows:

- Systematic
- Easy to follow and implement
- Similar (that is, the user's account name corresponds with the user's actual name)

Using a combination of the user's first name, middle initial, and last name results in systematic usernames for every member of a particular organization. Common examples include the following:

- First initial followed by last name (jdoe for John Doe)
- First initial followed by middle initial and last name (jqpublic for John Q. Public)
- Last name followed by first initial (DoeJ for Jane Doe)

When two users have the same initials or name, several alternatives can be used to create unique names. For example, a number can be added to the end of the username (jdoe1 and jdoe2). You can also apply a system of systematic naming rules (jdoe=John Doe and doej=Jane Doe).

Other conventions can be applied, however, it is important that conventions are both systematic and consistent.

Additional information is available in the TaskSmart N-Series operations guide and the administration guide for the appliance.

CIFS Shares and NFS Exports

CIFS and NFS are two distinct network file-sharing protocols. Where CIFS maintains the connection state between client and server and requires client user authentication in order to gain access, NFS is a stateless protocol that grants or denies access to network file resources based on the host name or IP address of the client machine. CIFS is the standard file sharing protocol for Windows clients; NFS is the standard file sharing protocol for UNIX clients.

The planning guide goes into extensive detail about how to integrate the two different file sharing mechanisms into a single, unified, heterogeneous file sharing environment. The important thing to consider from a deployment standpoint is how to set up shares and exports initially and how to migrate existing data to the TaskSmart N-Series appliance.

The simplest way to create CIFS shares is to use the NET SHARE command at the TaskSmart N-Series command prompt. Full help on how to use this command is available by typing NET HELP SHARE at the command prompt. That help is reproduced here so that an offline reference is readily available:

```
NET SHARE <share name>=<full path to folder>
```

For a command line interface, click **Command Prompt** on the NAS Console, or connect to the appliance through Telnet Server from a remote client.

For further help on the NET SHARE command, type NET HELP SHARE. The full text output of NET HELP SHARE follows:

```
NET SHARE sharename

    sharename=drive:path [/USERS:number | /UNLIMITED]

            [/REMARK:"text"]

            [/CACHE:Manual | Automatic | No ]

    sharename [/USERS:number | /UNLIMITED]

            [/REMARK:"text"]

            [/CACHE:Manual | Automatic | No ]

    sharename | devicename | drive:path} /DELETE
```

The NET SHARE command makes CIFS server resources available to network users. When used without options, it lists information about all resources being shared on the computer. For each resource, Windows reports the device name or names, or path name or names, and an associated descriptive comment. Table 2 illustrates NET SHARE resources.

Table 2. NET SHARE Resources

Device Name/Path Name	Description
Sharename	Provides the network name of the shared resource. Type **NET SHARE** with a sharename only to display

	information about that share.
drive:path	Specifies the absolute path of the directory to be shared.
/USERS:number	Sets the maximum number of users who can simultaneously access the shared resource.
/UNLIMITED	Specifies an unlimited number of users can simultaneously access the shared resource.
/REMARK:"text"	Adds a descriptive comment about the resource and encloses the text in quotation marks.
Devicename	Specifies one or more printers (LPT1: through LPT9:) shared by sharename.
/DELETE	Stops sharing the resource.
/CACHE:Automatic	Enables offline client caching with automatic reintegration.
/CACHE:Manual	Enables offline client caching with manual reintegration.
/CACHE:No	Advises client that offline caching is inappropriate.

A similar command line utility is available for creating NFS exports. This utility is called NFSSHARE. Help is available by typing NFSSHARE /? at the TaskSmart N-Series command prompt.

Note: The NET SHARE and NFSSHARE commands are **not** case sensitive. NFSSHARE and nfsshare are equivalent, as are NET SHARE and net share. The NFS shares created with NFSSHARE, of course, **are** case sensitive, as required by the NFS protocol, as are case-sensitive files and directories created by NFS clients. CIFS, by default, is **not** case sensitive, again as required by the protocol.

Again, for the sake of convenience, the help for NFSSHARE is reproduced here:

```
NFSSHARE <export name>=<full path to folder>
```

For a command line interface, click **Command Prompt** on the NAS Console, or connect to the appliance through Telnet Server from a remote client.

For further help on the NFSSHARE command, type NFSSHARE /?. The full text output of NFSSHARE /? follows:

```
NFSSHARE sharename=drive:path [-o RO[=client[:client ...]]
                              RW[=client[:client ...]]
                              ROOT=client[:client ...]
                              ANON
                              ENCODING=EUC-JP ]
```

where client can be either a host or a client group.

```
NFSSHARE {sharename | drive:path} /DELETE

NFSSHARE sharename
```

The NFSSHARE command makes NFS server resources available to network users. When used without options, it lists information about all resources being shared on the computer. For each resource, Windows reports the device name or names, or path name or names, and an associated descriptive comment. Table 3 illustrates NFSSHARE resources.

Table 3. NFS SHARE Resources

Device Name/Path Name	Description
Sharename	Provides the export name of the shared resource. Type **NFSSHARE** with a sharename only to display information about that export.
drive:path	Specifies the absolute path of the directory to be exported.
[-o …	The –o parameter indicates that machine-specific access privileges will be set.
RO[=client[:client ...]]	RO indicates that the list of client hosts or client group names is granted read-only access to the export.
RW[=client[:client ...]]	RW indicates that the list of client hosts or client group names is granted read-write access to the export.
ROOT=client[:client ...]	ROOT indicates that the list of client hosts or client group names is granted root level access to the export.
ANON	ANON indicates that the export is available to anonymous or squashed users.
ENCODING=EUC-JP]	This is a special setting that allows native support of Japanese character sets over the Network File System.

Once appropriate shares and exports are set up, clients can write files to the TaskSmart N-Series appliance. These clients can be existing NFS or CIFS servers whose data is to be consolidated on the appliance. In the ideal situation, the CIFS servers whose data is to be consolidated will be member servers of the same Windows Domain into which the TaskSmart N-Series appliance is incorporated. Likewise, the ideal migration scenario for NFS files is one in which the source server is a member of the same NIS environment into which the TaskSmart N-Series appliance is incorporated. If such is not the case, then appropriate user and group ACLs will have to be reproduced on the appliance based on the existing settings for the source servers. Of course, those same user and group names will also have to be re-created in the appliance's own local account database. This is more time consuming than simply getting the same user and group ACL information from a common Windows domain controller, but it can be managed for small deployments.

In the NFS case, NFS users and groups, whether they come from NIS or a passwd and group file pair, will have to be mapped to appropriate native Windows users and groups. This can be a time consuming and laborious process, but the nice thing is that once it's done, it need not be done again. User and group mappings can be exported from one TaskSmart N-Series appliance to another in case more than one needs to be deployed.

For additional information on planning for NFS, NCP, and CIFS integration onto a single appliance, including user and group mapping issues, see the TaskSmart N-Series planning guide. For information on the mechanics of configuring the user and group mapping service in particular, see the Task Smart N-Series administration guide or the Task Smart N-Series operations guide white paper.

Compaq Professional Service Offerings

Compaq Services offers complete services for the implementation, management and support of your environment:

- Warranty upgrades
- Installation and configuration
- Priority Service Plan
- Performance and Capacity Planning
- System Management and Monitoring
- For more information visit the Compaq website at

  www.compaq.com