COMPAQ

Technical Guide

May 2001
14MN-0501A-WWEN
Prepared by:
Industry Standard Server Division

Compaq Computer Corporation

Compaq TaskSmart N-Series Appliance Network Attached Storage Administration and Operations Guide

Contents

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

- Address cross-platform usability issues.
- Address ongoing performance and storage capacity planning issues.
- Understand how to effectively administer file serving in CIFS, NFS, and NCP environments.
- Understand how to set up and remotely manage Compaq TaskSmart N-Series appliances.
- Understand how to set up NIC teams.

Much of the information in this operations guide is adapted from the *Compaq TaskSmart N2400 Administration Guide* that is available with the purchase of each TaskSmart N-Series appliance.

Notice

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Introduction

The Compaq *TaskSmart*^{TM} N-Series appliance is an engineered solution designed to be used in many types of computing environments, from basic Microsoft Windows NT workgroups, to complicated Windows, UNIX, or Novell multiprotocol domains.

To effectively manage the TaskSmart N-Series appliance in these varied environments, the competent administrator must learn and understand the following concepts and procedures:

- Operations issues including the following concepts:
  - cross-platform management
  - data protection
  - backup and restoration of data
  - ongoing capacity planning
- Operations procedures including the setup and use of the following:
  - Compaq *SANworks*^{TM} Virtual Replicator
  - NTFS file system security
  - CIFS shares
  - UNIX network integration
  - Novell network integration
  - Remote administration
  - Ethernet teams

Each of these topics is discussed in the following sections of this document.

Operations Issues

Cross-Platform Management

One of the first questions that comes up with regard to a cross-platform file-serving appliance is how it deals with simultaneous access to files. The TaskSmart N-Series appliance handles this issue by accepting the control entities passed to it by clients and imposing those control entities at the file system level.

When a network client accesses data via CIFS, NFS, or NCP, that client makes a call similar to the POSIX Open() call. Windows clients actually use a low-level application programming interface (API) known as CreateFile(), but the effect is the same. Both Open() and CreateFile() allow for the application that opens an existing file (or creates a new one) to pass a desired file locking parameter to the file system.

Typically, this locking parameter takes one of the following forms, but there are other forms as well:

- Share read-write—Other applications can open the same file to read and write at the same time.
- Share read-only—Other applications can open the same file to read only. Writes to that file by other applications are denied.
- Share write-only—Other applications can open the same file to write only. Reads from that file by other applications are denied.
- Share exclusive—Other applications cannot open the file to read or to write. Any attempt to open this file by other applications is denied.

Essentially, the first application to open a file determines how that file is locked. When locked, the appropriate share parameter is enforced at the file system level, and subsequent attempts to open that file by other applications behave according to the lock parameter set by the initial application. For example, if a file is initially opened as share read-only, and a second application attempts to open that file to write to it, that attempt will fail because the file system will not allow it.

This same paradigm is enforced over network file systems like CIFS, NFS, or NCP. All three of these systems include protocol entities to pass along both the desired open mode (read, write, or read-write) and the desired file locking parameter [Open() or CreateFile()]. The CIFS, NFS, or NCP server resident on the TaskSmart N-Series appliance receives this locking parameter over the network and attempts to open the file in the manner specified, attempting also to apply the desired lock. If that client is the first to attempt to open the file, the open succeeds, and the specified lock is applied and enforced on the file system of the appliance. If that client is not the first to attempt to open the file, then another client (which file system is immaterial because locking parameters are enforced at the file system level) already has the file open and has already applied a locking parameter to it. The second (or any subsequent) client is then permitted access according to how the file was originally locked. Because CIFS, NFS, and NCP support locking entities at the network protocol level, it does not matter what protocol any of the clients use to attempt to access the file.

As long as a file remains open, the server enforces the locking parameter on other clients that attempt to open the same file. As soon as the file is closed by all accessing clients [the low-level API call is close() in POSIX and CloseHandle() in Windows], the file lock is released by the appliance file system.

Data Protection

The latest release of the TaskSmart N-Series appliance supports Advanced Data Guarding (ADG). This technology is incorporated into the Smart Array 5300 PCI controller.

ADG provides the highest level of data protection among RAID levels, while offering customers a high level of disk drive capacity utilization. ADG is a revolutionary RAID technology that provides the best combination of fault tolerance and disk space usage. ADG protects against multiple disk drive failures, while requiring the capacity of only two drives (in an array of up to 56 disk drives) to be set aside for dual sets of distributed parity data. This dual parity is spread across all of the disk drives in the system.

ADG can tolerate up to two simultaneous drive failures, giving administrators more flexibility in responding to drive failures without the fear of costly server downtime or data loss. Because a large capacity logical drive can have a lengthy rebuild time, this method of data protection is ideal for applications requiring large logical drives.

More information about ADG is available at the following website:

www.compaq.com/products/storageworks/smartarray-controllers/adg.html

Backup and Restoration of Data

The TaskSmart N-Series appliance is designed so that recoveries from certain kinds of disasters are less difficult than they might otherwise be. One of those quick recovery mechanisms involves running the QuickRestore program to reconnect to existing data if it is the operating system – rather than the data itself – which fails.

The first thing to observe is that the design of the appliance is such that a hard break exists between the data drives and the operating system (OS) drives. The data drives are located in external storage enclosures, and the OS drives are on a RAID 1 pair of drives located in the internal drive bays of the server. Three logical drives are located on the RAID 1 set. The first of these logical drives houses the actual OS. The remaining two logical drives are reserved for future use, allowing for flexibility in the ongoing design of the product. This design allows for a hard separation between the system and the data, thereby allowing a QuickRestore to reconnect reliably to the data, if the OS drives should fail.

There are two environments in which a QuickRestore to the TaskSmart N-Series appliance will take place: Domain and Workgroup. Where differences between the two arise, a note is entered into the text.

In addition, the NFS User Mapping service provides a mechanism by which user mappings can be saved to a text file. By having these user mappings saved on a regular basis to offline media, some manual recovery steps can be avoided at the time of a QuickRestore.

Using QuickRestore

The QuickRestore program itself includes two different restore methods: Quick and Full. The administrator selects the appropriate method from the TaskSmart N-Series appliance console when initiating the QuickRestore media.

- The “Quick” QuickRestore destroys and recreates only the OS disks.
- The “Full” QuickRestore destroys and recreates both the OS drives and the data drives, including RAID logical drives, SANworks Virtual Replicator (SWVR) virtualization metadata, and the data on the disk.

Note that the “Quick” process rebuilds only the OS drive. Thus, doing a “Quick” QuickRestore is the only supported method for reconnecting to existing data on the data drives. Reconnecting to data requires that the “Quick” method be chosen.

If used in conjunction with the TaskSmart Configuration diskette, the “Quick” QuickRestore process does not require any user input. The TaskSmart Configuration diskette provides initial networking settings to the QuickRestore process so that configuration difficulties are minimized. Use of the TaskSmart Configuration diskette is detailed in the companion paper entitled *Compaq TaskSmart N-Series Appliance Network Attached Storage Deployment Guide.* After the QuickRestore process is completed, a workgroup server is created. If the TaskSmart N-Series appliance is operating in a workgroup environment, then the administrator can immediately reconnect to the data, because SWVR reads the virtualization metadata from the data drives and automatically recreates storage pools and virtual disks within the newly created server environment. This setup can be verified by viewing the SWVR virtual disks and snapshots through the Windows Explorer interface or through the SWVR Snapshot Manager.

In this new environment, a new local system administrator and computer security ID (SID) will have been created. Therefore, the system administrator may not initially have access to the reconnected data, because that data was created using a system administrator or a computer with the new SID.

Restoring Previous System Settings

To restore all previous system settings in a workgroup environment, file permissions can either be reset manually, or an offline backup of registry settings can be used to restore these settings. Most backup and restore software packages support a mechanism for backing up and restoring the registry to offline media. This way, the restore process can be completed rather quickly, because only the settings are restored, not the data. If the file permissions are to be reset manually, it may first be necessary to change the ownership of all files and subdirectories to the new administrator. Then, user permissions can be manually applied.

To restore all previous system settings in a Domain environment, first reconnect to the shares following the QuickRestore, and then rejoin the Domain. Because a Domain environment stores the user account database on an external server (the Primary and Backup Domain Controllers), no user contexts are lost. The administrator simply needs to remove the old TaskSmart N-Series appliance from the Domain and add the new one. This last part is necessary because a new, unique SID was assigned to the computer during the QuickRestore process. Another option would be to use an offline backup program option to restore system registry settings, just as in the Workgroup model.

After the data reconnection is completed, a few server reconfiguration tasks are required. If the prior system configuration (registry data) is restored using an offline backup facility, this task should not be required. However, if the offline system backup does not provide such a facility or if a manual restore is chosen for another reason, the following items must all be reconfigured:

- CIFS shares, NCP shares, and NFS exports, including permissions
- NIS or passwd/group files—These files must be imported into the NFS Mapping Service anew.
- NFS user mappings—These mappings can be reconfigured by re-applying previously saved mappings as previously outlined and in the *Compaq TaskSmart N2400 Administration Guide*. This step is necessary only if system settings are not restored via some offline backup mechanism.

Ongoing Capacity Planning

One of the most important operational tasks of an administrator in a file server environment is to adequately plan for increased storage capacity needs over time. The TaskSmart N-Series appliance currently has a total raw data capacity of two terabytes (2 TB) in a non-clustered configuration. This full capacity need not be deployed initially. Initial capacity requirements can be addressed, and then capacity can grow to meet future requirements over time. If performance is the concern, then growing drive capacity for optimized performance can also be addressed. For instance, additional drive spindles can be added in a specific manner to effectively increase real performance. Often, performance and capacity requirements grow together over time. In many cases, capacity needs to increase because more people are using the system, and as more people use the system, that system needs to be able to handle a larger amount of work.

Increasing Capacity to Address Performance Needs

From a strict performance standpoint, the best way to increase capacity is to add more disk drive spindles. Adding more spindles increases the number of simultaneous low-level disk I/Os that the system is capable of. The real issue is to add those spindles effectively.

One way to add spindles is to incorporate new spindles into an existing RAIDset. The *Compaq TaskSmart N2400 Administration Guide* provides details about how to do this procedure. After additional spindles have been incorporated into an existing RAIDset, additional logical drives can be carved across those spindles. Any existing logical drives get spread out across those additional spindles as well, so this arrangement can increase performance across the board. Because all logical drives in the RAIDset are spread across all spindles, the new logical drives can be added to an existing SWVR storage pool without concern for how they are used. SWVR concatenates rather than stripes the logical storage units in its pool. Thus, the new storage units will not be used until the existing units are full. However, because the drive spindles are already striped at a lower level, effective performance increases can be achieved.

There is one drawback to this strategy, however. When physical disks are added to an existing RAIDset, any data already present must be rewritten and striped across the additional disks. This process can take a significant amount of time, especially if there is a large amount of data already stored on the drives or if the system is typically under a heavy client load. Thus, this approach may be impractical for some deployed systems.

A second approach to increasing storage capacity is to add new drive spindles and create a new RAIDset. This method has the advantage of not affecting existing data on the system. New drives are added, and they are incorporated into a new RAIDset using the Compaq Array Configuration Utility (ACU). Then, one or more new logical drives are configured from this RAIDset. These logical drives can then be incorporated into new SWVR storage pools. New virtual disks can be created from these pools, and new data shares can be spread across the new storage capacity, effectively striping user reads and writes across all disk spindles in the system.

The disadvantage to this approach is that it requires the creation of new shares and exports, which in turn adds to the management tasks for the system administrator.

Increasing Capacity to Address Storage Needs

If storage capacity (total number of GB of storage available on a single system) is the paramount concern for capacity growth over time, then there are other ways to add new disk drive spindles to the system.

A third way to increase capacity is to add spindles, place the new spindles into new RAID logical drives, and incorporate them into existing SWVR storage pools. This method allows for each storage pool to have a larger available capacity. Then, existing virtual disks can be grown using the volume growth procedure outlined in the *Compaq TaskSmart N2400 Administration Guide* to increase the available capacity. This method has the distinct advantage of providing the best solution from an overall management perspective. The volumes can be grown quickly while they are online, because data is not restriped over the additional drive spindles. Moreover, it is unnecessary to create new shares and exports to use the new space, because the new space is logically incorporated into the old.

The disadvantage, however, is that this approach uses disk concatenation rather than disk striping to effect the growth. At the RAIDset level, the new drives are striped together. However, at the SWVR level – and by extension at the share and export level – they are not. Each individual RAIDset stripes data across its disks, but there is no striping across different RAIDsets.

This approach may or may not create a potential performance bottleneck. There are essentially two scenarios that could unfold. The first scenario is the simplest – the existing logical drives in a storage pool fill up with data that is no longer accessed, and all new reads and writes take place against the new logical drive(s) imported into the SWVR storage pool. In this case, there is no effective gain in available spindles and therefore little or no effective gain in performance.

In the second scenario, the existing logical drives in a storage pool fill up with data that continues to be accessed by users on the system, and new reads and writes take place against the new logical drive(s) imported into an SWVR storage pool. In this case, a significant increase in read performance can be realized, because reads get spread across all of the data in a storage pool. Some of that data is physically located on one logical drive; other data is physically located on other logical drives. This scenario allows for effective read performance to increase, because the dynamics of the system uses all available disk spindles. There will be a small increase in write performance, because all new writes will be physically written to the new logical drive(s) in the storage pool. The small potential increase in write performance is a direct corollary of the increase in read performance. Because read performance is spread across all spindles by the dynamics of the system, the actual number of physical reads across the new logical drive(s) is less than it otherwise would be. This configuration makes greater physical disk resources available for writes to the new logical drive(s), and a corresponding increase in performance can be realized.

Thus, growing capacity over time can be done in a number of different ways. The system administrator merely needs to be aware of the effects of different approaches to capacity growth, so that the best one for each system environment can be chosen.

Operations Procedures

Many of the procedures in this section are adapted from the C*ompaq TaskSmart N2400 Administration Guide*, which ships along with every TaskSmart N2400 appliance. Some of the information is reproduced here for the convenience of system administrators. In addition, some new and updated information is included.

Some of the included topics are as follows:

- Compaq SANworks Virtual Replicator
- Drive quotas
- NTFS file system security
- CIFS shares
- UNIX network integration
- Novell network integration
- Remote administration
- Ethernet teams

Compaq SANworks Virtual Replicator

The 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.

SWVR provides the following storage management units and tools:

- **Pools**

  Storage units formed from hardware arrays or physical drives. Can be of any size, up to 2 TB of raw data capacity.

- **Virtual disks**

  Storage units created by dividing pool space. Can be of any size, up to 1 TB.

- **Online volume growth**

  Ability to increase the size of a virtual disk, without user interruption.

- **Snapshots**

  Instant point-in-time copies of the virtual disks.

Pools

SWVR enables the grouping of RAID array storage (physical drives) into a logical pool of drive space. Any number of pools can be created, using industry-standard storage components and controller-based, fault-tolerant drive arrays, such as SANworks RAID arrays (referred to as storage units). The storage units provide drive space for the pool in the same way as the physical drives that make up a SANworks RAID array. These pools are then carved into separate units called virtual disks.

Virtual Disks

SWVR controls how data is stored on a virtual disk. Virtual disks perform and behave in exactly the same way as physical drives. Drive letters can be mapped to them, and read/write commands can be executed on them. Disk virtualization allows drive space to be optimally tailored to the size required by users and their applications, meaning virtual disk sizes can be made to match the requirements of applications and users. For example, if a user needs 650 MB of drive space, the administrator can create a 650-MB virtual disk. With a 1-TB database, several drives or RAID arrays can be combined in a single pool with a 1-TB virtual disk that spans that physical storage. The size of the virtual disks can range from 10 MB to 1 TB, depending on free pool space and other limits set at the time of pool creation. Refer to the chapter, "Advanced Administrative Procedures," in the *Compaq TaskSmart N2400 Administration Guide* for more information about virtual disks.

Online Volume Growth

SWVR provides the ability to increase storage capacity without disrupting operations. Normally, when a RAIDset is grown, the operating system does not recognize the size change until the system is restarted. The SWVR online volume growth feature directs the operating system to update the size of a physical drive or virtual disk, without requiring a system restart. Online volume growth can also instruct the operating system to grow the on-disk partition information for a volume. This feature allows a volume to grow into unused space. With online volume growth, storage capacity can increase as required by the users and applications, easily and with zero downtime.

The online volume growth feature operates only on basic and virtual disks formatted using the NTFS file system. It does not work with dynamic drives. Refer to the chapter, "Advanced Administrative Procedures," in the *Compaq TaskSmart N2400 Administration Guide* for additional information about online volume growth.

Snapshots

SWVR can make instant replicas, called snapshots, of virtual disks in a matter of seconds. Snapshots enable the instant creation of multipurpose virtual replicas of production data, without having to physically copy the data. Snapshots function in exactly the same way as ordinary physical drives, with read and write capabilities. Snapshots should be considered temporary in nature.

Snapshot Overview

Snapshots are copies of data on virtual disks. Snapshots initially take up very little space on the hard drive and can be created in mere seconds. Snapshots are extremely beneficial. They can be used to immediately recover a lost file or directory, to test a new application with important data without affecting the “real” data, and as a source of data for backups. Snapshots are a temporary backup of data and are not meant to be a permanent form of data backup.

Snapshots work by mapping blocks of virtual disks and intercepting virtual disk writes. Each initial write to a data block on the virtual disk causes that write to perform a copy of the original data before replacing it with the new data being written. This action is known as a copy-out and preserves a copy of the virtual disk as it was when the snapshot was created. The copy is available until the snapshot is deleted.

When using snapshots, performance of the virtual disk may be affected. Predicting the exact effect of snapshots on any particular virtual disk is difficult, because several variables are involved. These variables include the number of snapshots kept for each virtual disk, the type of the applications that are accessing the data, and the rate of change of the files on the virtual disk. When a high percentage of writes is made to the same area, as when a file is constantly rewritten, this is called write locality. Virtual disks with high write locality experience less performance degradation due to snapshots.

Read performance of the virtual disk remains constant, regardless of the presence of snapshots. Additionally, read performance of the snapshot is identical to that of the virtual disk. Write performance, however, may vary. Each initial write to a virtual disk area causes a copy-out to the snapshot, and the initial write is slower than if a snapshot is not being used. Copy-out is not performed on subsequent writes to the same virtual disk block, so write performance is unaffected after the initial write to each block.

Snapshot Facts

- Snapshots are on a per-virtual disk basis.
- Up to 12 snapshots per virtual disk can be created.
- Snapshots of snapshots can be created.
- Snapshots can be read-only or read-write.
- Snapshots must be assigned to a drive letter to be accessible.
- Snapshots can be shared in the same manner as virtual disks.
- Snapshots are automatically deleted if pool space becomes critical.

Snapshots and Pool Sizing

When initially implementing snapshots, the first priority is to gain an understanding of the amount of additional pool space required by the snapshots. As described previously, this assessment is a function of the write activity, its locality, the projected lifetime of the snapshot, and number of snapshots per virtual disk. By default, 30 percent of the pool is reserved for snapshots.

To help plan for snapshot space allocation, SWVR includes a Snapshot Planner utility. The Snapshot Planner utility must be installed and run only on existing servers in the network. The utility must not be run on the TaskSmart N-Series server. The Snapshot Planner monitors all write activity to a selected volume, and reports the amount of pool space that a snapshot of the volume consumes. The Snapshot Planner provides complete pool and volume sizing information. The size of the virtual disks and the size of the pool are equally important.

Snapshot Access and Naming

Snapshots are read-write, and if snapshots are shared, they can be accessed and the data can be edited. If snapshots are shared with write access enabled, it is recommended that a snapshot of the original snapshot be created. There is no backup of the original snapshot unless a snapshot of it is taken. By controlling the share permissions, administrators can make snapshots read-only as an alternative to creating snapshots of snapshots.

Note: Snapshots of snapshots can impede performance when both snapshots are running on the same virtual disk.

The parent-child relationship of snapshots is not displayed in the Snapshot Manager. Therefore, appropriate snapshot naming and volume naming should be used to identify each snapshot individually. For example:

- Name the parent “Snapshot A”
- Name the child “Child of Snapshot A”

Snapshots and Backup

Snapshots are quick to create, and it is possible to capture a coherent view of the virtual disk data with little or no application downtime. Lack of application downtime removes the traditional backup window, or the amount of time taken to back up to offline media. While many applications must be shut down to capture an accurate backup, snapshots capture a point-in-time view of the data, which can be used as the source of the backup data. Applications can continue processing against the virtual disk data. Therefore, applications may have to be interrupted for only a few seconds during the snapshot process.

CAUTION: Snapshots are not a replacement for reliable, periodic data backup. If free pool space becomes critical, snapshots may be automatically deleted. See the section, “SWVR Lifeguard Service,” in the *Compaq TaskSmart N2400 Administration Guide* for additional information. Snapshots are a short-term convenience, and reside on the same physical drives as the data. If something happens to the data drives, the snapshots are also affected. Refer to the appendix, “Backup Utility Management,” in the *Compaq TaskSmart N2400 Administration Guide* for suggestions on how to back up the TaskSmart N2400 appliance.

Snapshot Restoration

Snapshots may be used as a highly efficient way to maintain online backups of a virtual disk, enabling immediate file and directory recovery. Snapshots are assigned to a drive letter and used exactly like virtual disks. If a file or directory is lost or corrupted, it can be recovered easily. The administrator can switch to the snapshot drive and copy the file or directory back to its original location on the virtual disk or an alternate location.

IMPORTANT: To preserve the integrity of a point-in-time snapshot of a virtual disk, ensure that it is exported as read-only.

Snapshots and Drive Defragmentation

A drive defragmenter consolidates files on a drive by reading various parts of the files and rewriting them to become contiguous on the drive. Contiguous files increase drive performance. When virtual disks are created from the drive space pool, the software makes them as contiguous as possible on the underlying storage units (logical drives and arrays).

CAUTION: Do not defragment a drive if there are snapshots on that drive. Because defragmenting a virtual disk causes files on the virtual disk to be rewritten, the snapshot is also rewritten, causing additional disk space to be used. To use a drive defragmenter, all snapshots on that drive must first be deleted.

IMPORTANT: Do not use the Windows 2000 operating system native defragmenter. It does not work on file allocations greater than 4K, and is therefore not applicable to the TaskSmart N-Series appliance.

Creating Snapshots

Snapshots are a daily maintenance tool for the TaskSmart N-Series appliance. Before creating a snapshot, the TaskSmart N-Series appliance must have a pool (or pools) of space and one or more virtual disks established. The TaskSmart N-Series appliance comes preconfigured with pools and virtual disks. Verify that there is adequate free pool space to support snapshots.

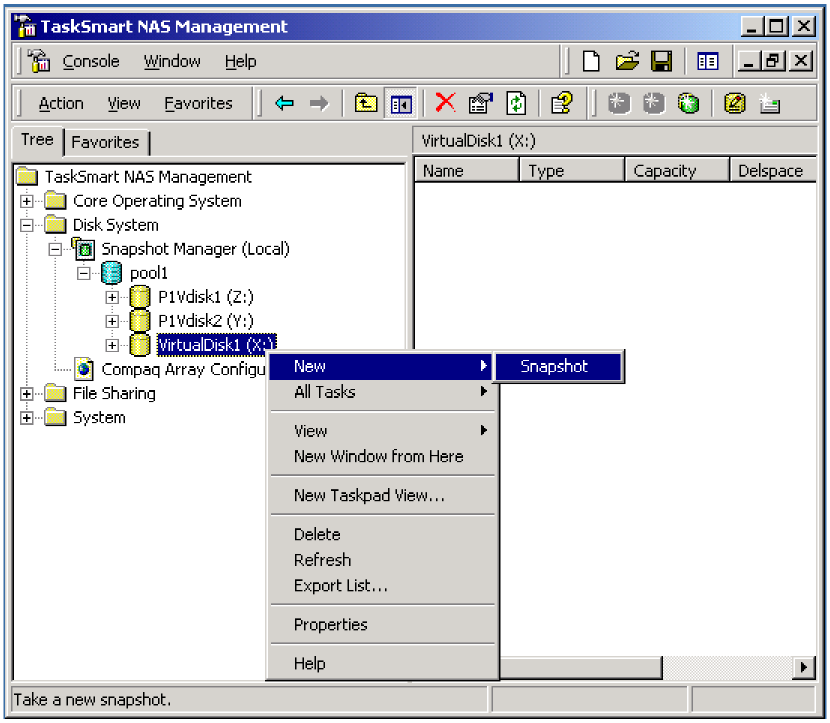
IMPORTANT: Snapshots are temporary in nature and are automatically deleted by the system if free pool space becomes critical. Snapshot data loss can occur.

The “Advanced Administrative Procedures” chapter of the *Compaq TaskSmart N2400 Administration Guide* provides instructions on how to alter the preconfigured snapshot layout for work environments. Instructions are also included for the procedures required to create pools and virtual disks.

After the pool (or pools) of space and one or more virtual disks are established, the process to create snapshots can begin.

1. From the TaskSmart Management Console, click **Microsoft Management Console (MMC)**. Then, click **Disk System**.
2. Click **Snapshot Manager**, and then click the desired pool.

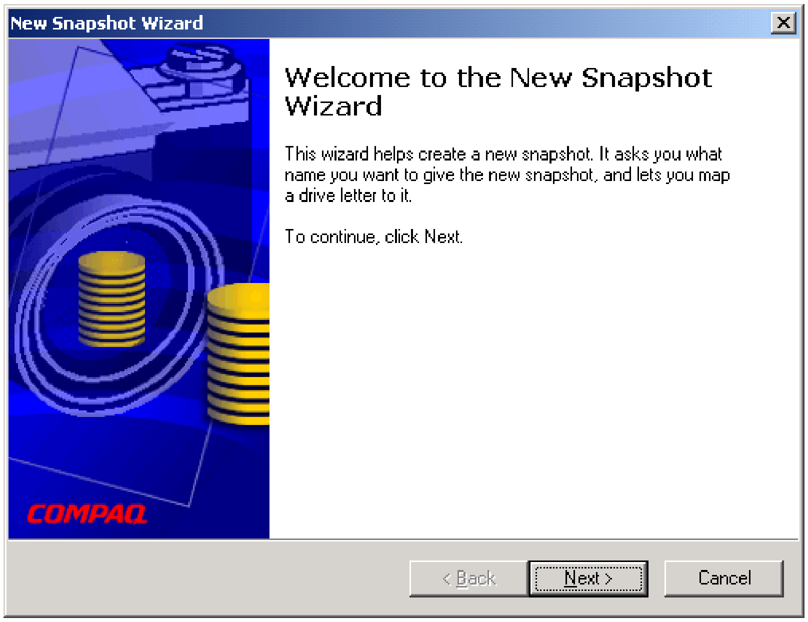
3. Select a virtual disk. Figure 1 illustrates the **Snapshot Manager** screen used during snapshot creation.



Take a new snapshot.

Figure 1: Snapshot Manager screen, creating snapshots

4. Right-click the virtual disk, click **New**, and then click **Snapshot**. The Snapshot wizard will open and display a series of questions. Figure 2 illustrates the **New Snapshot Wizard** dialog box.



Welcome to the New Snapshot Wizard

This wizard helps create a new snapshot. It asks you what name you want to give the new snapshot, and lets you map a drive letter to it.

To continue, click Next.

Figure 2: New Snapshot Wizard dialog box

5. Click **Next**. The **Snapshot Information** dialog box is displayed.
6. Enter a name for the snapshot. Appropriate snapshot naming and volume naming should be used to identify each snapshot individually.
7. Click **Next**. The **Drive Letter Assignment** dialog box is displayed.
8. Click **Map Drive Letter**, and then select a drive letter. Enter a volume label. The default is the same volume label as the virtual disk. Optionally, click **No Drive Letter**.

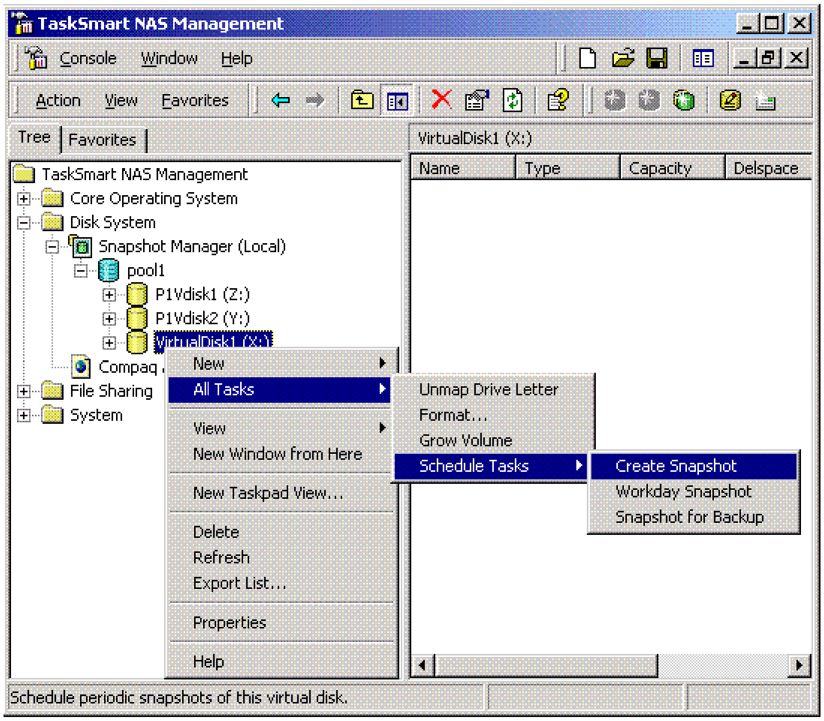
> **Note:** It is not necessary to assign a drive letter to the snapshot until access to the snapshot is needed. However, if only one snapshot per virtual disk will be created, it is advisable to assign a drive letter at this time.

9. Click **Next**, and then click **Finish**.

Scheduling Snapshots

Snapshots of a virtual disk can be scheduled for any arbitrary or regularly occurring date and time. The following steps outline the snapshot scheduling process. Recurring snapshot tasks can be configured so that a snapshot runs a backup command and automatically deletes itself when the backup completes.

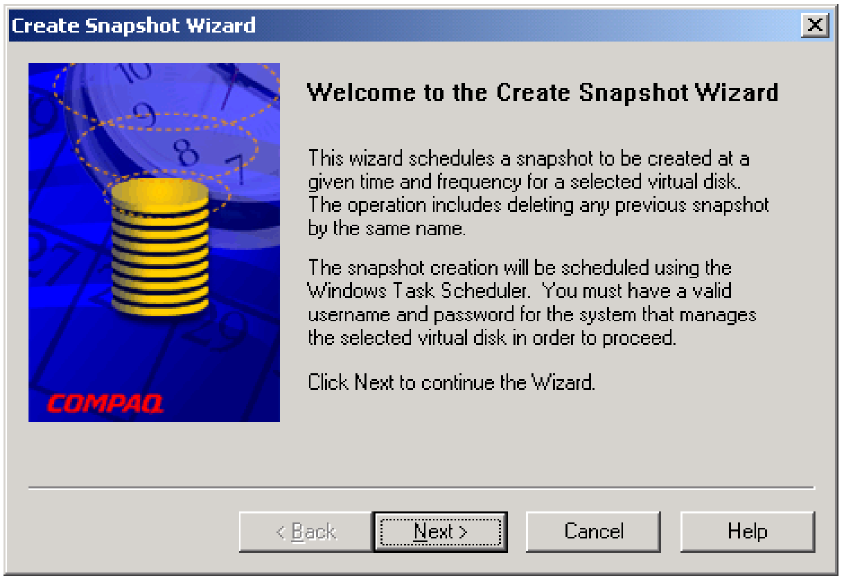
1. From the TaskSmart Management Console, click **Microsoft Management Console**, and then click **Disk System**.
2. Click **Snapshot Manager**, and then click the selected pool.
3. Right-click the selected virtual disk.
4. Click **All Tasks**, **Schedule Tasks**, and then click **Create Snapshot**.



Schedule periodic snapshots of this virtual disk.

Figure 3: Snapshot Manager screen, scheduling snapshots

5. The **Create Snapshot Wizard** dialog box is displayed. Click **Next**.



Create Snapshot Wizard

Welcome to the Create Snapshot Wizard

This wizard schedules a snapshot to be created at a given time and frequency for a selected virtual disk. The operation includes deleting any previous snapshot by the same name.

The snapshot creation will be scheduled using the Windows Task Scheduler. You must have a valid username and password for the system that manages the selected virtual disk in order to proceed.

Click Next to continue the Wizard.

Figure 4: Create Snapshot Wizard dialog box

6. Configure each screen of the wizard.
7. Click **Finish** when the last screen is completed.
8. To confirm the scheduled task:
   a. Right-click the virtual disk.
   b. Select **Properties**.
   c. Select the **Scheduled Task** tab. View the task listing for the task name and scheduled date and time.
   d. Click **OK**.

IMPORTANT: VERITAS Backup Exec does not allow snapshots to run a backup command to automatically delete themselves after the backup completes.

Restoring a Virtual Disk from a Snapshot

If data on a virtual disk becomes corrupted, the virtual disk can be restored from the normal tape backup. Alternatively, an existing and valid snapshot of the virtual disk can be used to restore the entire virtual disk from the existing snapshot.

Note: Snapshots are not a replacement for normal tape backup.

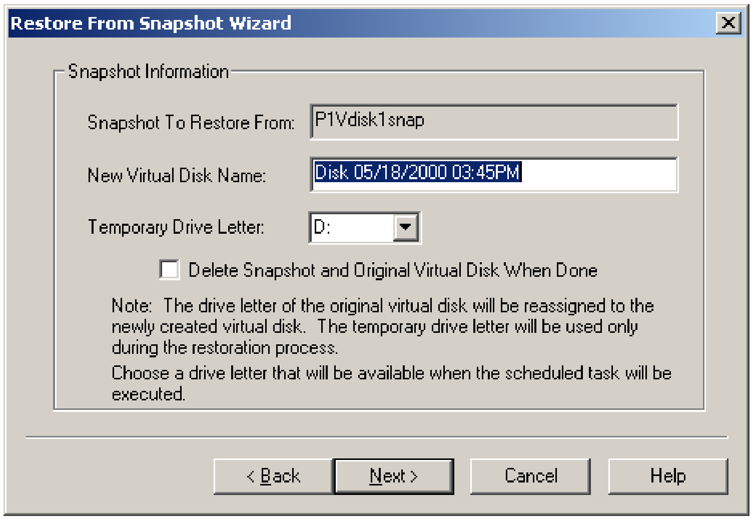
CAUTION: Snapshot recovery causes temporary pool space consumption because of the need to preallocate pool space for the newly recovered virtual disk. There must be sufficient free pool space, otherwise a pool-full condition may occur and the Lifeguard Service may delete the snapshot from which data is being read. If this snapshot is deleted, the data must then be restored from a tape backup.

The **Restore from Snapshot Wizard** schedules the recreation of a virtual disk from a snapshot. If specified, upon successful completion of the schedule, the previous virtual disk and snapshot are both deleted. Before using the wizard, execute the following steps to prepare the system:

1. Remove all shares associated with the virtual disk to be restored.
2. Delete all snapshots of the virtual disk to be recovered, except for the snapshot that will be used for the recovery. Additionally, in order to free up pool space, delete any other unnecessary snapshots of other virtual disks in the same pool.
3. Make sure that enough pool free space is available to accomplish the recovery, and if necessary, add logical disks to increase free pool space.
4. Typically, free pool space must equal the current size of the virtual disk to be recovered, plus the space currently used by the snapshot being used for the recovery. To determine the amount of space used by this snapshot, access the Snapshot Manager, and then select the virtual disk. Locate the snapshot name in the right-hand pane. The amount of the space used by the snapshot is in the **delspace** column.

After completing the preparatory steps, go to the TaskSmart Management Console and do the following:

1. Click **Microsoft Management Console**, and then click **Disk System**.
2. Click **Snapshot Manager**.
3. Right-click the appropriate snapshot to restore from, and select **All Tasks**, **Scheduled Tasks**. Then, select **Online Restore from a Snapshot**.
4. The **Restore from Snapshot Wizard** dialog box is displayed. Click **Next**.



Restore From Snapshot Wizard

Snapshot Information

Snapshot To Restore From: P1Vdisk1snap

New Virtual Disk Name: Disk 05/18/2000 03:45PM

Temporary Drive Letter: D:

□ Delete Snapshot and Original Virtual Disk When Done

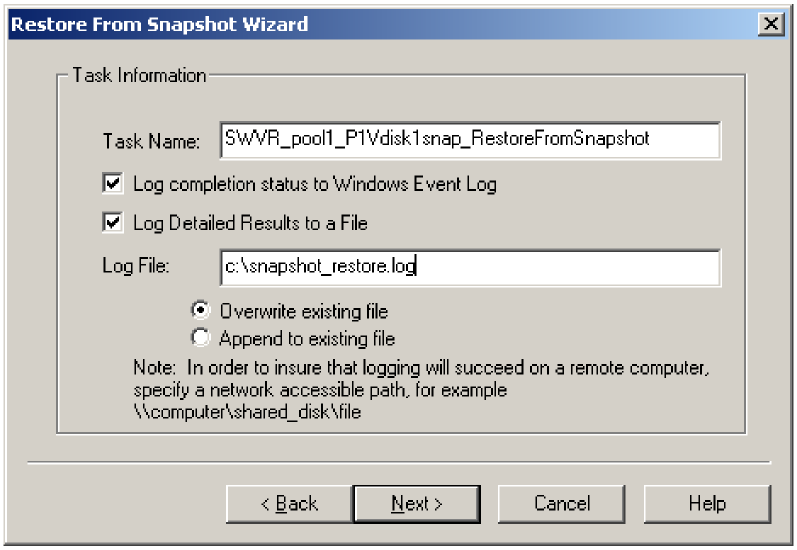
Note: The drive letter of the original virtual disk will be reassigned to the newly created virtual disk. The temporary drive letter will be used only during the restoration process.
Choose a drive letter that will be available when the scheduled task will be executed.

Figure 5: Restore from Snapshot Wizard, Snapshot Information dialog box

5. If desired, enter a new virtual disk name and drive letter. Then, select **Delete Snapshot and Original Virtual Disk When Done**.

6. Click **Next**. The **Task Information** dialog box is displayed. Figure 6 illustrates this next **Restore From Snapshot Wizard** dialog box.
7. Select **Log completion status to Windows Event Log**, select **Log Detailed Results to a File**, and then enter a log file path and filename. Then, select **Overwrite existing file**. When finished, click **Next**.

IMPORTANT: Step 8 must be completed to have a record of the transaction.



Restore From Snapshot Wizard

Task Information

Task Name: SWVR_pool1_P1Vdisk1snap_RestoreFromSnapshot

☑ Log completion status to Windows Event Log

☑ Log Detailed Results to a File

Log File: c:\snapshot_restore.log

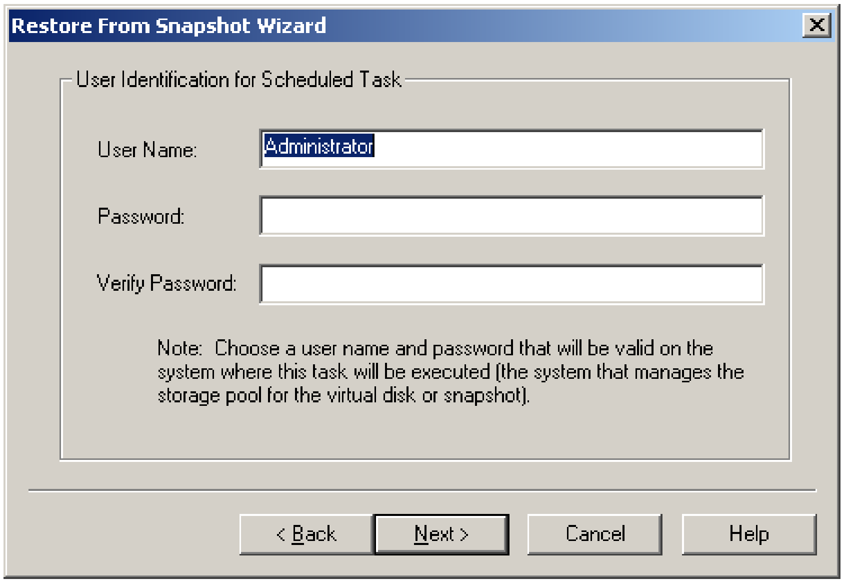
● Overwrite existing file

○ Append to existing file

Note: In order to insure that logging will succeed on a remote computer, specify a network accessible path, for example \\computer\shared_disk\file

Figure 6: Restore From Snapshot Wizard, Task Information dialog box

8. Enter the user name and password, and then click **Next**.



Restore From Snapshot Wizard

User Identification for Scheduled Task

User Name: Administrator

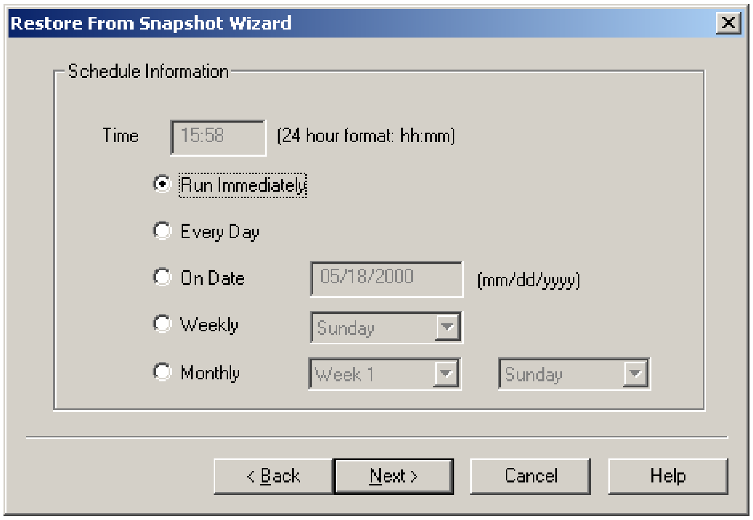
Password:

Verify Password:

Note: Choose a user name and password that will be valid on the system where this task will be executed (the system that manages the storage pool for the virtual disk or snapshot).

Figure 7: Restore From Snapshot Wizard, User Identification for Scheduled Task dialog box

9. Enter the schedule information. Enter the information for when the restore is to run. Then, click **Next**.



Restore From Snapshot Wizard

Schedule Information

Time 15:58 (24 hour format: hh:mm)

● Run Immediately

○ Every Day

○ On Date 05/18/2000 (mm/dd/yyyy)

○ Weekly Sunday

○ Monthly Week 1 Sunday

Figure 8: Restore From Snapshot Wizard, Schedule Information dialog box

10. When all screens have been completed, click **Next**, and then click **Finish**.

Modifying Reserved Pool Space for Snapshots

Although it is not recommended, the percentage of free pool space that is reserved for snapshots (30 percent) can be changed. If snapshots will not be used, removing this reserved space should not cause a problem.

CAUTION: It is possible for data corruption to occur if the percentage of free pool space is removed and snapshots are later used without adding back the 30 percent reserved space. There is a default minimum of 1056 MB of free space. It is not possible to set the reserved space less than this default without activating the Lifeguard service.

Increasing the percentage of free pool space poses no problem other than reserving a larger percentage of the pool.

To modify the percentage of free pool space:

1. Click **Command Prompt** on the TaskSmart N-Series Console.
2. On the command line, enter the command:

   `mfsppp` *`nn`* (*nn* represents the percentage of free pool space to reserve)

   For example:

   `mfsppp 10` — reserves 10 percent free pool space

   `mfsppp 0` — reserves 1056 MB – the minimum allowed

   `mfsppp 50` — reserves 50 percent free pool space

3. Enter `exit` to exit the command-line window.

For help with the mfsppp command, enter the `mfsppp help` in the command line.

IMPORTANT: Under no circumstances should Lifeguard functionality be disabled.

Drive Quotas

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, and administrators can then modify quotas as needed. By enabling and then disabling quotas, administrators take advantage of the auditing capabilities provided by quotas without reducing server performance. For more information about Quotas, refer to the online Help of the TaskSmart N2400 appliance.

To enable drive quotas:

1. Log on as an administrator on the TaskSmart N-Series appliance.
2. From the desktop, double-click the **My Computer** icon.
3. In the **My Computer** interface, right-click the selected virtual disk, and then select **Properties**.
4. In the **Properties** window, select the **Quotas** tab.
5. Select **Enable Quota Management**, and then click **OK**.

Note: If the volume is not formatted with the NTFS file system, or if the user is not a member of the administrators group, the **Quota** tab is not displayed in the **Properties** dialog box.

NTFS File System Security

The Compaq TaskSmart N2400 appliance uses NTFS, Version 5, as the underlying file system. The CIFS network file sharing protocol uses the NTFS file system security model as the basis for its own security model. To effectively administer CIFS shares, it is important to understand the fundamentals of NTFS security. This section documents the relationship between NTFS security and the CIFS file sharing protocol.

IMPORTANT: CIFS is a network file sharing protocol that resides on the file system. NTFS is a file system that resides on the drive subsystem, organizing and securing the data written to the drives.

When a CIFS client initiates a request over the network, the request is processed through the appliance CIFS service and is distributed throughout the file system to write the data onto the drive. When data is retrieved from the drive, it is distributed back through the file system and the appliance CIFS service, and then returned to the client.

More information about Windows file system security is available on the following Microsoft website:

www.microsoft.com/

Topics included in this section are as follows:

- Access Control Lists (ACLs)
- Local file system security integration into Windows Domain environments

Access Control Lists (ACLs)

The ACL contains the information that dictates which users and groups have access to a file, and the type of access that is permitted. Each file on an NTFS file system has one or more ACLs. For example, an ACL can define that User1 has read and write access to a file, User2 has read-only access, and User3 has no access to a particular file. The ACL also includes group access information that applies to every user in a configured group.

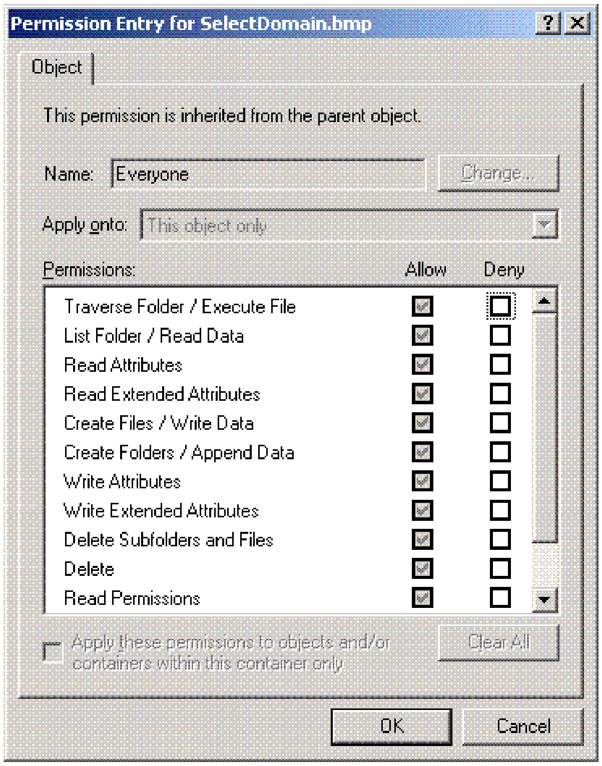
There are several permissions available for selection for any file or folder on an NTFS file system. These permissions are listed in Table 1.

Viewing File or Folder Security Properties

The following steps outline the process to view these permissions:

1. From either the client machine or the TaskSmart N-Series appliance, open the **Windows Explorer** interface, and then right-click the NTFS file or folder.
2. Select **Properties**.
3. Select the **Security** tab.
4. Click **Advanced**.
5. Select one of the users or groups in the list.
6. Click **View/Edit**. A screen displays a list of all the available permissions. Figure 9 illustrates the **Permission Entry** screen for a file.

Note: Additional permissions are available, but are not displayed in Figure 9.



This permission is inherited from the parent object.

Name: Everyone

Apply onto: This object only

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	☐
List Folder / Read Data	☑	☐
Read Attributes	☑	☐
Read Extended Attributes	☑	☐
Create Files / Write Data	☑	☐
Create Folders / Append Data	☑	☐
Write Attributes	☑	☐
Write Extended Attributes	☑	☐
Delete Subfolders and Files	☑	☐
Delete	☑	☐
Read Permissions	☑	☐

☐ Apply these permissions to objects and/or containers within this container only

Figure 9: Permission Entry dialog box, for file named SelectDomain.bmp

It is possible to configure different combinations of ACL permissions.

Table 1 provides a list of available access-level permissions and a description of the permission when enabled.

Note: If the permission is not enabled, the access level is denied.

Table 1. Access-Level Permissions

Permission	Description
Traverse Folder / Execute File	Users can open the folder or execute the file.
List Folder / Read Data	Users can list the contents of a folder or read data from a file.
Read Attributes	Users can read the core attributes from a file or folder (read-only, hidden, archive).
Read Extended Attributes	Users can read the extended attributes from a file or folder (compressed or encrypted).
Create Files / Write Data	Users can create files within a folder, or write data to a file.
Create Folders / Append Data	Users can create folders within a folder or attach data to an existing file.
Write Attributes	Users can write core attributes to a file.
Write Extended Attributes	Users can write extended attributes to a file.
Delete Subfolders and Files	Users can delete folders, and files within a folder.
Delete	Users can delete a file or folder.
Read Permissions	Users can read the permissions for all configured users and groups.
Change Permissions	Users can change permissions for all configured users and groups.
Take Ownership	Users can take ownership of the affected files or folders from another user.

Common access-level combinations have logical names that describe the access level. Table 2 describes the access-level descriptions.

Table 2. Access-Level Description

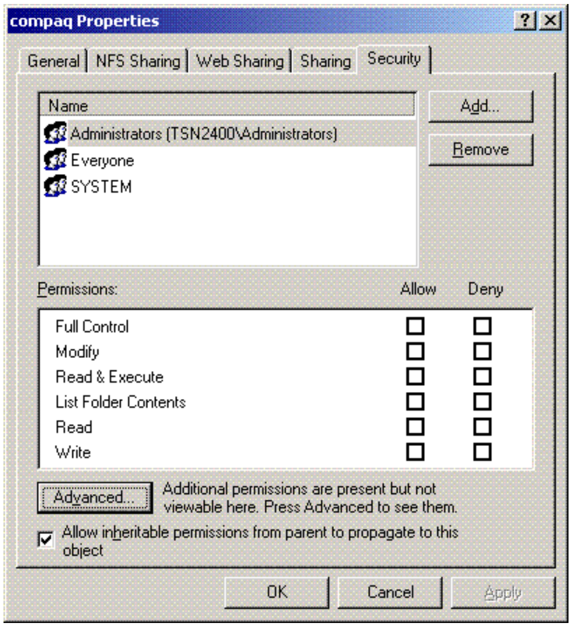
Access level	Description
Full Control	Allows complete access to all access-level permissions. Includes Modify, Read & Execute, Read, and Write access levels.
Modify	Includes all advanced access properties except: • Delete Subfolders and Files • Change Permissions • Take Ownership
Read & Execute	Includes all advanced access permissions except: • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership
List Folder Contents	Includes the following access permissions only: • Traverse Folder / Execute File • List Folder / Read Data • Read Attributes • Read Extended Attributes • Read Permissions
Read	Includes the following access permissions only: • List Folder / Read Data • Read Attributes • Read Extended Attributes • Read Permissions
Write	Includes the following access permissions only: • Create Files / Write Data • Create Folders / Append Data • Write Attributes • Write Extended Attributes

Note: These access levels can be combined, for example, Read and Write.

Managing File or Folder Security Properties

File system security can be managed locally using the TaskSmart N-Series console, or remotely with the Remote Insight Lights-Out Edition board. The necessary steps are outlined below.

1. From the **Windows Explorer** interface, right-click the file or folder to change.
2. Select **Properties**.
3. Select the **Security** tab.



Name
Administrators (TSN2400\Administrators)
Everyone
SYSTEM

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	□	□

Additional permissions are present but not viewable here. Press Advanced to see them.

☑ Allow inheritable permissions from parent to propagate to this object

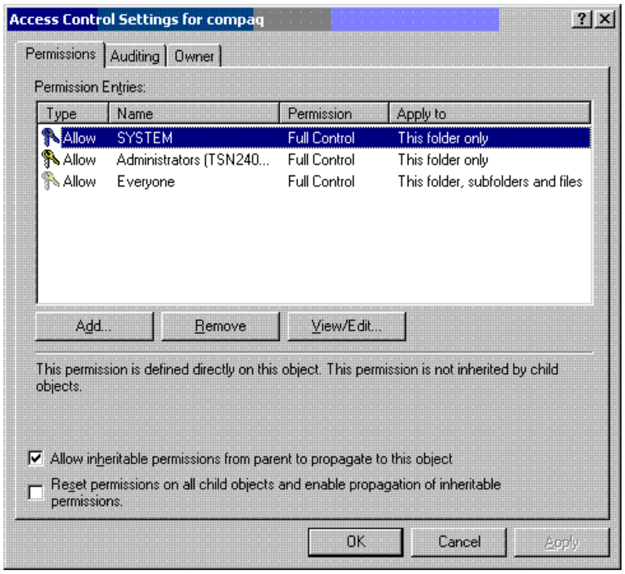
Figure 10: Security Properties dialog box for folder name of compaq

Several options are available on the **Security** tab:

- Users and groups can be added to the permissions list by clicking **Add**.
- Users and groups can be removed from the permissions list by highlighting the desired user or group and clicking **Remove**.
- If **Allow inheritable permissions from parent to propagate to this object**, at the bottom of the screen, is selected, the file or directory inherits permissions from the parent directory. If this check box is enabled, existing user and group permissions cannot be changed; however, additional users or groups may be added.
- The center section of the **Security** tab provides a listing of permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file access levels.

Note: Selections can be made only when **Allow inheritable permissions from parent to propagate to this object** is disabled.

- The **Advanced** button is used to modify ownership of files or to modify individual file access-level permissions. Figure 11 illustrates the **Access Control Settings** dialog box that is displayed when **Advanced** is clicked.



Permission Entries:

Type	Name	Permission	Apply to
Allow	SYSTEM	Full Control	This folder only
Allow	Administrators (TSN240...	Full Control	This folder only
Allow	Everyone	Full Control	This folder, subfolders and files

This permission is defined directly on this object. This permission is not inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

☐ Reset permissions on all child objects and enable propagation of inheritable permissions.

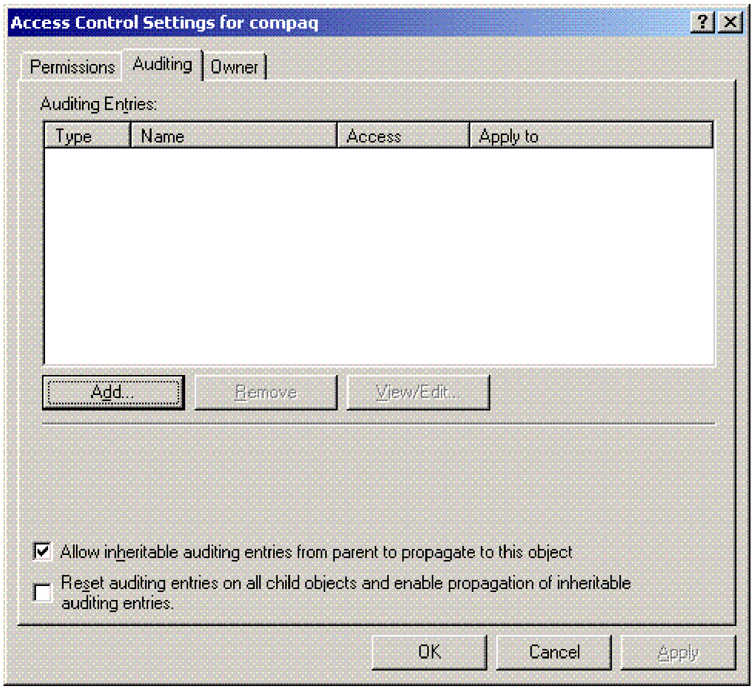
Figure 11: Access Control Settings dialog box, Permissions tab, for file name of compaq

Additional functionality is available in the **Access Control Settings** dialog box. Within the **Access Control Settings** dialog box are three tabs: the **Permissions** tab, the **Auditing** tab, and the **Owner** tab.

Options within the **Permissions** tab include:

- New users or groups can be added to the permissions list by clicking **Add**, and then following the dialog box instructions.
- Users or groups can be removed from the permission list by highlighting the user or group to remove, and then clicking **Remove**.
- Permissions for a user or group are viewed and edited by highlighting the user or group, and then clicking **View/Edit**.
- Permissions can be passed from a parent file to a child file by selecting **Allow inheritable permissions from parent to propagate to this object**. If this option is enabled, existing user and group permissions cannot be changed. However, additional users or groups may be added.
- If the object being configured is a folder, select **Reset permissions on all child objects and enable propagation of inheritable permissions**. This option allows all child folders and files to inherit the current folder permissions by default.

Another area of the **Access Control Settings** dialog box is the **Auditing** tab. This tab sets the rules for the auditing of access, or attempted access, to files or folders. The monitoring of users or groups can be established and maintained though the advanced **Access Control Settings Auditing** tab. The **Auditing** tab dialog box is illustrated in Figure 12.


Access Control Settings for compaq

Auditing Entries:

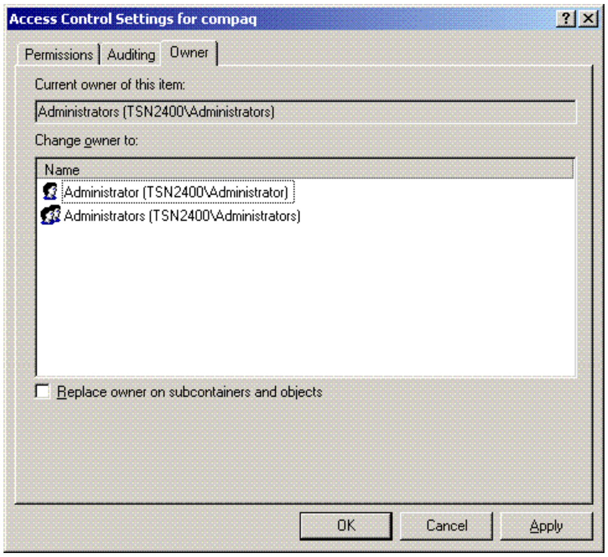
Type	Name	Access	Apply to

☑ Allow inheritable auditing entries from parent to propagate to this object

☐ Reset auditing entries on all child objects and enable propagation of inheritable auditing entries.

Figure 12: Access Control Settings, Auditing tab dialog box for folder name of compaq

The final tab in the advanced **Access Control Settings** dialog box is the **Owner** tab. The **Owner** tab allows for taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, the administrator gains access to the files and then manually applies the appropriate security configurations. Figure 13 illustrates the **Owner** tab.


Access Control Settings for compaq

Current owner of this item:

Administrators (TSN2400\Administrators)

Change owner to:

Name
Administrator (TSN2400\Administrator)
Administrators (TSN2400\Administrators)

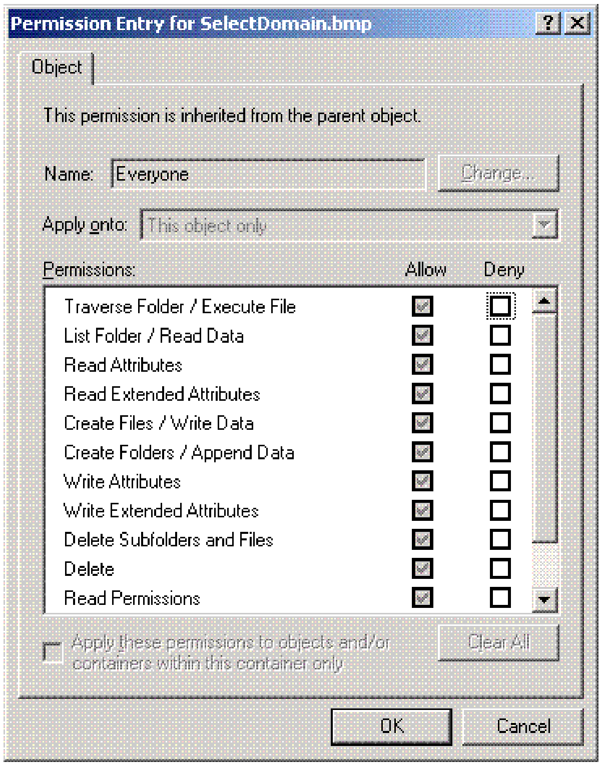
☐ Replace owner on subcontainers and objects

Figure 13: Access Control Settings, Owner tab dialog box for folder name of compaq

Modifying Permissions

To modify specific permissions assigned to a particular user or group for a selected file or folder:

1. From the **Security** tab of the **Properties** dialog box, click **Advanced**. The **Access Control Settings** dialog box is displayed. See Figure 11 for an example of this screen display.
2. Select the **Permissions** tab.
3. Select the desired user or group.
4. Click **View/Edit**. The **Permission Entry** dialog box is displayed.
5. Check all of the permissions to enable, and uncheck the permissions to disable. Select **Allow** to enable permission, or **Deny** to disable permission. If neither box is selected, permission is disabled. Figure 14 illustrates the **View/Edit** dialog box that specifies permissions.



Permission Entry for SelectDomain.bmp

Object

This permission is inherited from the parent object.

Name: Everyone

Apply onto: This object only

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□

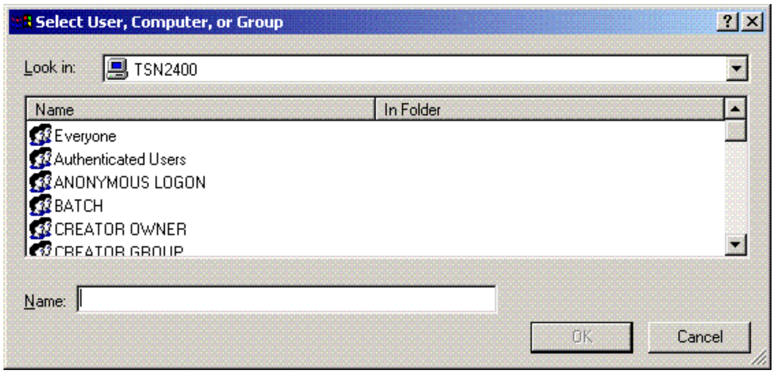
□ Apply these permissions to objects and/or containers within this container only

Figure 14: Permission Entry dialog box, for file name of SelectDomain.bmp

Adding a User or Group To Be Audited

To add a user or group to be audited:

1. From the **Auditing** tab of the **Access Control Settings** dialog box, click **Add**. Then, select the appropriate domain or machine name from the **Look in:** drop-down list box.



Select User, Computer, or Group

Look in: TSN2400

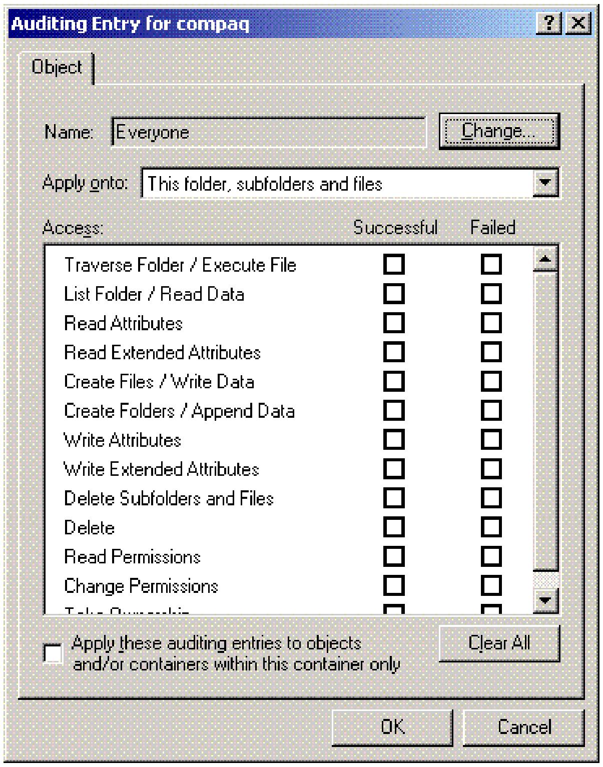
Name	In Folder
Everyone	
Authenticated Users	
ANONYMOUS LOGON	
BATCH	
CREATOR OWNER	
CREATOR GROUP	

Name:

Figure 15: Select User, Computer, or Group dialog box

> **Note:** A list of users and groups from the desired domain can be viewed only if the current user has permission to view the information on the domain.

2. Select the user or group, and then click **OK**. The **Auditing Entry** dialog box is displayed.



Auditing Entry for compaq

Object

Name: Everyone

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Traverse Folder / Execute File	□	□
List Folder / Read Data	□	□
Read Attributes	□	□
Read Extended Attributes	□	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	□	□
Change Permissions	□	□
Take Ownership	□	□

□ Apply these auditing entries to objects and/or containers within this container only

Figure 16: Auditing Entry dialog box for folder name of compaq

3. Select the desired audits for successful and failed attempts for the user or group, and then click **OK**.

Taking Ownership of a File or Folder

The current owner of the file or folder is listed at the top of the screen. To take ownership:

1. From the **Owner** tab of the **Access Control Settings** dialog box, select the appropriate user or group from the **Change owner to** list.
2. If it is also necessary to take ownership of subfolders and files, select **Replace owner on subcontainers and objects**.
3. Click **OK** to execute the commands.

Local File System Security Integration into Windows Domain Environments

All file ACLs include properties specific to users and groups from a particular Workgroup or Domain environment. In a multi-Domain environment, user and group permissions from several Domains can apply to files stored on the same appliance. Users and groups local to the TaskSmart N-Series appliance can be given access permissions to files and folders on the appliance. The Domain name of the TaskSmart N-Series appliance supplies the context in which the user or group is understood. The file level permission configuration depends on the network and Domain infrastructure where the appliance resides.

Because the CIFS network file sharing protocol supplies a user and group context for all connections over the network, appropriate default ACLs are applied to the file system when new files are created. CIFS configuration tools provide the ability to share permissions out to clients. These shared permissions are then propagated into a file system ACL, and when new files are created over the network, the user creating the file becomes the file owner. In cases where a specific subdirectory of a share has different permissions from the share itself, the NTFS permissions on the subdirectory apply instead. This policy results in a hierarchical security model where the CIFS network protocol permissions and the file permissions work together to provide appropriate security for CIFS shares on the appliance.

Note the following considerations when CIFS permissions and NTFS file system permissions are stored in the associated ACL of a file:

- CIFS permissions and NTFS file system permissions are implemented separately. It is possible for files in a file system to have different permissions from those applied to a CIFS share. When files have both CIFS and NTFS permissions, the most restrictive of the permissions takes precedence. This policy is useful when a single CIFS share is shared out to a large community of users, but contains several folders, each with access to a subset of the larger user community.
- The CIFS and NTFS security models are designed to integrate seamlessly. This integration provides the ability for one security model to be applied to the other security model.

CIFS Shares

As noted in the previous discussion about file system permissions and ACLs, the CIFS file security model is based on the NTFS file security model, and seamlessly integrates with NTFS files security. This section documents how to manage CIFS shares, and discusses CIFS security and other topics.

There are several ways to set up a CIFS share. The first and simplest way is to open a command-line interface. Alternatively, CIFS share creation and management can be accomplished through the Microsoft Management Console or through Windows Explorer in the TaskSmart N-Series appliance GUI interface.

Therefore, the topics included in this section are as follows:

- Administrative shares compared to standard shares
- Share management using the command-line interface
- Share management using the TaskSmart Microsoft Management Console
- Share management using Windows Explorer

Administrative Shares Compared to Standard Shares

CIFS supports both administrative shares and standard shares. Administrative shares are not included in the list of shares when a client browses for available shares on a CIFS server. Administrative shares are shares whose last character is a “$” character. Standard shares are listed whenever a CIFS client browses for available shares on a CIFS server. Standard shares are shares that do not end in a “$” character.

The TaskSmart N-Series appliance supports both administrative and standard CIFS shares. To create an administrative share, input a “$” character at the end of the share name when setting up the share. To create a standard share, do not input a “$” character at the end of the share name.

Share Management Using the Command-Line Interface

The simplest way to set up a CIFS share is to open a command-line interface to the TaskSmart N-Series appliance.

Setting up a Share Using the Command-Line Interface

To get a command-line interface and set up a share, use the following steps:

1. Click **Command Prompt** on the TaskSmart N-Series Console, or connect to the appliance from a remote client.
2. Enter the following command in the command-line interface:

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

3. For further help on the NET SHARE command, enter NET HELP SHARE. The full text output of the NET HELP SHARE command is listed as 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 3 illustrates NET SHARE resources.

Table 3. NET SHARE Resources

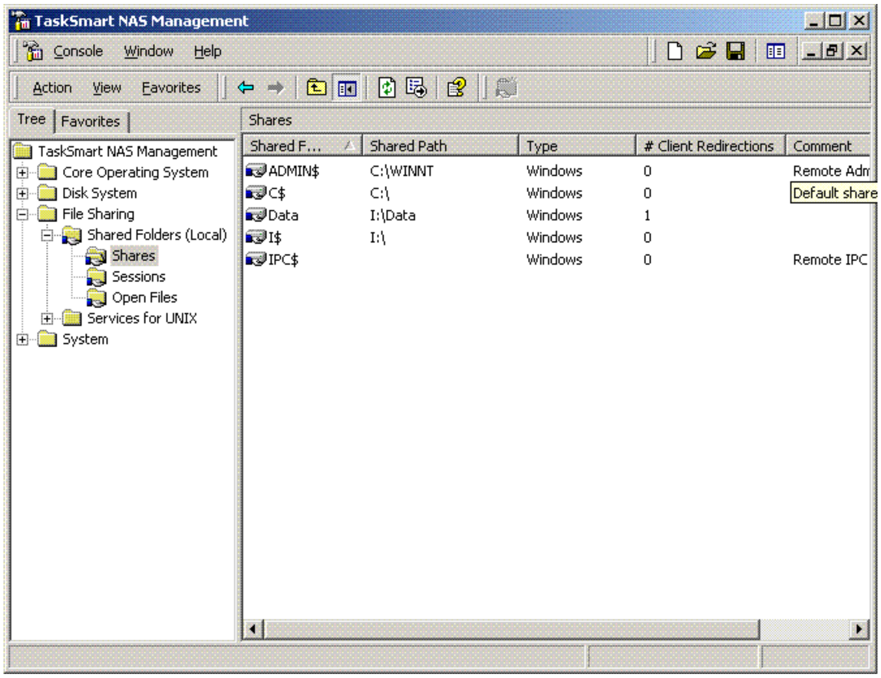
Device Name/Path Name	Description
Sharename	Provides the network name of the shared resource. Enter **NET SHARE** with a sharename only to display information about that share.
drive:path	Specifies the absolute path of the directory to be shared.
/USERS:number	Sets the maximum number of users who can simultaneously access the shared resource.
/UNLIMITED	Specifies an unlimited number of users who can simultaneously access the shared resource.
/REMARK:"text"	Adds a descriptive comment about the resource and encloses the text in quotation marks.
/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.

Share Management Using the Microsoft Management Console

Shares can be created, deleted, and modified from the Microsoft Management Console (MMC).

To invoke the MMC snap-in necessary to administer CIFS shares:

1. From the TaskSmart N-Series Console, click **Microsoft Management Console**.
2. Navigate to the **File Sharing** folder.
3. Open the **Shared Folders** subfolder. The MMC console for file sharing administration is displayed showing three additional subfolders, and all file shares, including administrative shares, are listed, along with summary data for each share.



Shared F...	Shared Path	Type	# Client Redirections	Comment
ADMIN$	C:\WINNT	Windows	0	Remote Adm
C$	C:\	Windows	0	Default share
Data	I:\Data	Windows	1	
I$	I:\	Windows	0	
IPC$		Windows	0	Remote IPC

Figure 17: TaskSmart NAS Management screen, (MMC), CIFS Shares manager

Note: CIFS shares can also be administered through remote MMC by pointing the remote **Shared Folders** snap-in on a client machine at the TaskSmart N-Series appliance. Either way, three subfolders are displayed.

The MMC subfolders are described in Table 4.

Table 4. MMC Subfolders

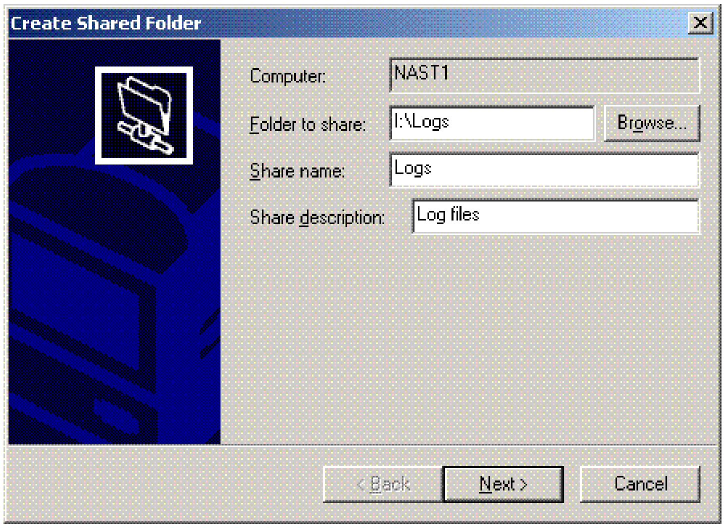
Subfolder Name	Description
Shares	Lists all shares on the appliance, including administrative shares. Shares can be added, removed, or modified in this subfolder. See the section, "Administrative Shares Compared to Standard Shares," previously in this document for details.
Sessions	Lists all current client sessions connected to the appliance. Client sessions can be managed in this subfolder.

Open Files	Lists all files currently open through shares on the appliance. Open files can be managed in this subfolder.

Creating a CIFS Share Using the MMC

To create a share using the MMC:

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Shares**. Then select **Action** form the toolbar. Select **New File Share**. The **Create Shared Folder** dialog box is displayed.



Computer: NAST1

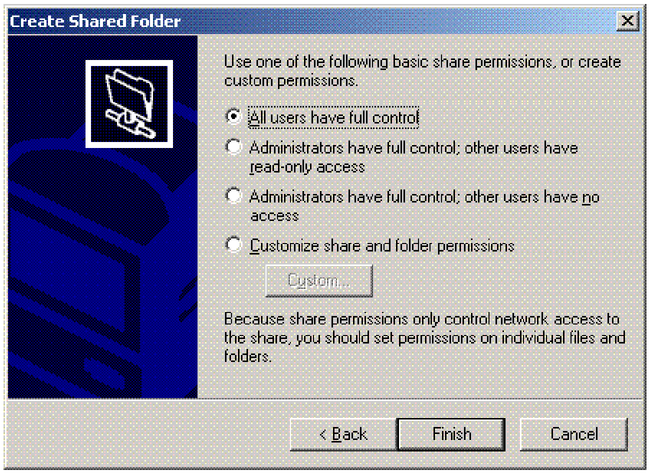
Folder to share: I:\Logs

Share name: Logs

Share description: Log files

Figure 18: Create Shared Folder dialog box

2. Enter the appropriate information for **Folder to share**, browsing for a particular folder if necessary.
3. Enter the share name and a comment to describe the share.
4. Click **Next**. The dialog box illustrated in Figure 19 is displayed.



Use one of the following basic share permissions, or create custom permissions.

● All users have full control

○ Administrators have full control; other users have read-only access

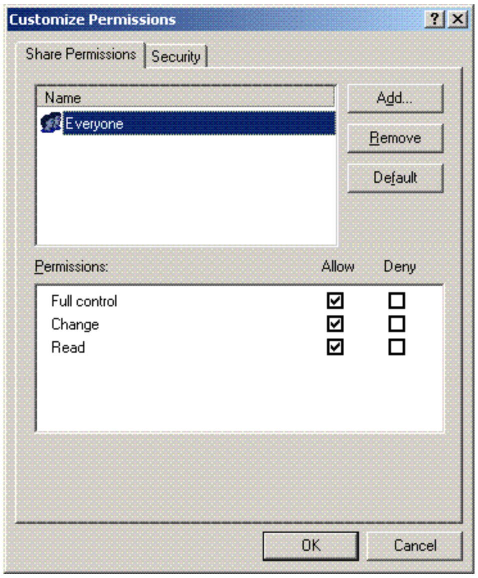
○ Administrators have full control; other users have no access

○ Customize share and folder permissions

Because share permissions only control network access to the share, you should set permissions on individual files and folders.

Figure 19: Create Shared Folder dialog box, customizing

5. Select the appropriate permissions level. If a custom permissions level is needed, select **Customize share and folder permissions**, and then click **Custom**. The **Customize Permissions** dialog box is displayed.



Name
Everyone

Permissions:	Allow	Deny
Full control	☑	☐
Change	☑	☐
Read	☑	☐

Figure 20: Customize Permissions dialog box, Share Permissions tab

The CIFS share permissions dialog box is similar to the dialog box used for managing NTFS file permissions.

There are three permission levels: **Full control, Change**, and **Read**. Each permission level allows connected users specific capabilities with the files located in the share. The following list describes each permission level in detail.

- **Full control** is the default permission applied to any newly created shares. It allows all Read and Change permissions, plus:
  - Changing permissions (NTFS files and folders only)
  - Taking ownership (NTFS files and folders only) (MMC help for the Shared Folders snap-in)
- The **Change** permission level allows all Read permissions, plus:
  - Adding files and subfolders
  - Changing data in files
  - Deleting subfolders and files
- The **Read** permission level allows:
  - Viewing file names and subfolder names
  - Traversing to subfolders
  - Viewing data in files
  - Running program files

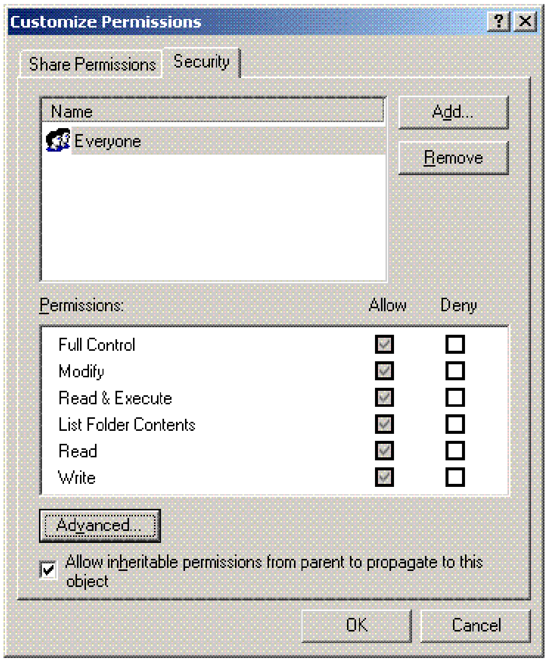
Any of these access permission levels can be applied to shared folders.

6. Choose an appropriate permissions level for each user or group configured to have access to the share.

Note: If a subfolder has a different level of permissions applied to it at the file system level, the most restrictive of the permissions apply. This control allows administrators to build a hierarchical security model into their file sharing strategy.

Note: The dialog box for adding users or groups to the share permissions list is identical to the dialog box for adding users or groups to a directory permissions list.

7. The second tab on the **Customize Permissions** property page deals with share security. The **Security** tab is illustrated in Figure 21.



Name
Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Figure 21: Customize Permissions dialog box, Security tab

The **Security** tab allows for editing the file system security properties that apply to the share folder on the appliance. This information is administered in the same way security settings are administered for files and folders on the NTFS file system. See the previous section, “NTFS File System Security,” for more information.

8. After appropriate permissions and file system security properties have been set for the share, click **OK** to return to the **Create Share Wizard** dialog box. Then, click **Finish**.

Deleting a CIFS Share Using the MMC

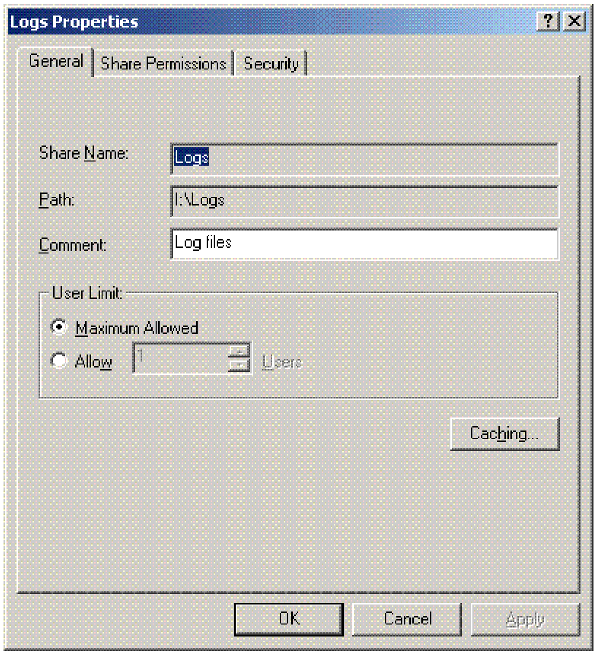
To delete a share using the MMC:

1. From the **MMC**, select **File Sharing**, **Shared Folders**, and **Shares**.
2. Highlight the share to delete.
3. Select **Action** from the toolbar, and then select **Stop Sharing**.

Modifying a CIFS Share Using the MMC

To modify a share using the MMC:

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Shares**.
2. Double-click the share to modify. Figure 22 is an example of the **Share Properties** dialog box that is displayed.



Share Name: Logs

Path: I:\Logs

Comment: Log files

User Limit:

● Maximum Allowed

○ Allow 1 Users

Figure 22: Share Properties dialog box, General tab

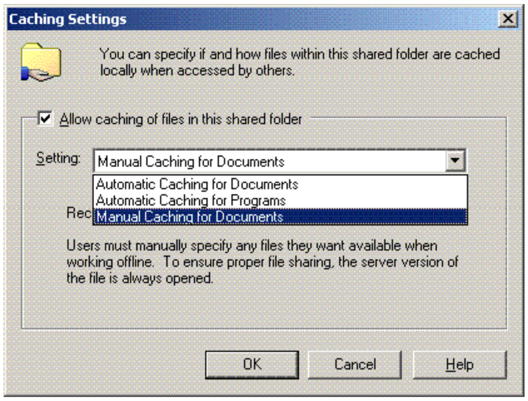
Several tabs in the **Properties** dialog box are used to set customized permissions for the share. They are as follows:

- The **Share Permissions** tab is used to manage permission levels, and is the same tab as documented in the previous section, "Creating a CIFS Share Using the MMC."
- The **Security** tab is used to edit the file system security properties that apply to the share. This tab is documented in the previous section, "Creating a CIFS Share Using the MMC."
- The **General** tab allows the following three properties to be modified: comment, user limit, and caching.
  - To modify the comment, highlight the existing comment, and then enter a new comment that appropriately describes the share.
  - To restrict the number of users who can access the share at any given time, select **Allow**, and then select the desired number of users.

IMPORTANT: The appliance has no license restrictions on the number of users who can access a share at any given time. Restricting users should be done only to accommodate performance implications or infrastructure policies.

- To modify caching settings, select **Caching**. The **Caching Settings** dialog box is displayed.

  The default setting is **Manual Caching for Documents**. Other settings include **Automatic Caching for Documents** and **Automatic Caching for Programs**.



Caching Settings

You can specify if and how files within this shared folder are cached locally when accessed by others.

☑ Allow caching of files in this shared folder

Setting: Manual Caching for Documents

Users must manually specify any files they want available when working offline. To ensure proper file sharing, the server version of the file is always opened.

Automatic Caching for Documents
Automatic Caching for Programs
Manual Caching for Documents
Rec
OK
Cancel
Help

Figure 23: Caching Settings dialog box

Table 5 describes each caching setting.

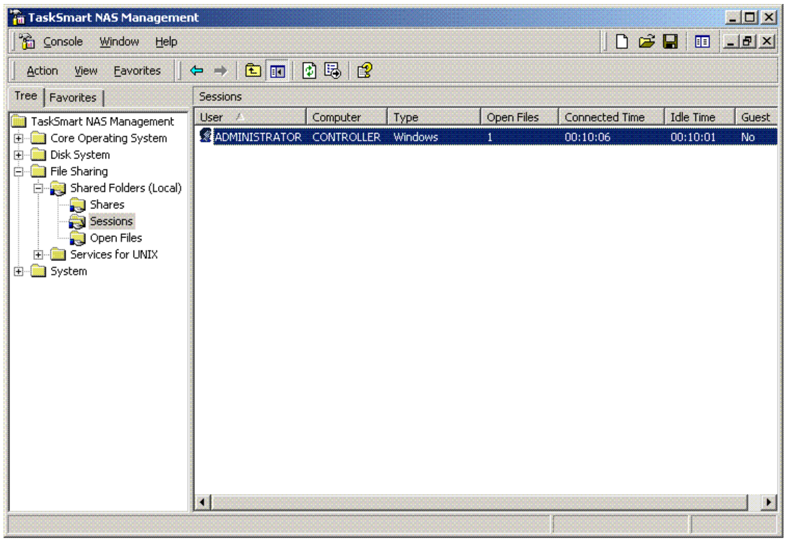
Table 5. Caching Settings

Setting	Description
Manual Caching for Documents	Default setting. Recommended for folders containing user documents. Users must manually specify any files they want available when working offline. To ensure proper file sharing, the server version of the file is always open.
Automatic Caching for Documents	Recommended for folders containing user documents. Open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files. To ensure proper file sharing, the server version of the file is always open.
Automatic Caching for Programs	Recommended for folders with read-only data, or run-from-the-network applications. File sharing is not ensured. Open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files.

3. After the modifications are completed in the **General** tab, click **OK**. The **Share Properties** dialog box is redisplayed.
4. After modifying any additional share properties in the **Share Permissions** tab or the **Security** tab, click **OK** to apply the modifications.

Managing CIFS Sessions Using the MMC

In addition to managing file shares, the **MMC** provides tools for managing CIFS sessions. Figure 24 is an example of the CIFS Shared Folders **Sessions** manager screen.



User	Computer	Type	Open Files	Connected Time	Idle Time	Guest
ADMINISTRATOR	CONTROLLER	Windows	1	00:10:06	00:10:01	No

Figure 24: TaskSmart NAS Management screen (MMC), CIFS Sessions manager

All CIFS sessions that are open on the server are displayed in right pane of the CIFS **Session** manager screen. Information is included about the user and client that initiated the session. For security and maintenance reasons, it is sometimes necessary to forcibly disconnect client sessions.

Terminating a Specific Session

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Sessions**.
2. Highlight the session.
3. Select **Action** from the toolbar, and then click **Close Session**.

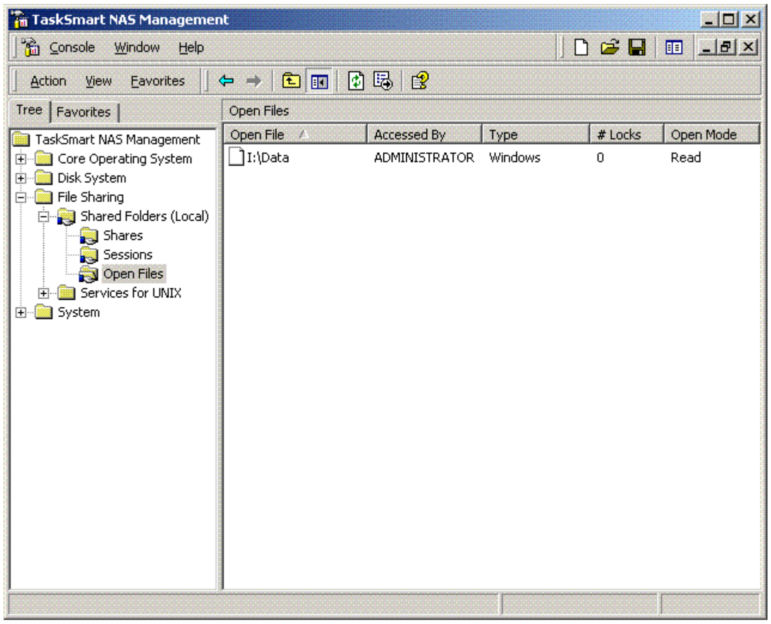
Disconnecting All Sessions

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Sessions**.
2. Deselect all highlighted sessions.
3. Select **Action** from the toolbar, and then click **Disconnect All Sessions**.

CAUTION: Disconnecting a session forces the currently connected user or users to disconnect their CIFS sessions from the server. As a result, it is possible that data loss could occur.

Managing CIFS Open Files Using the MMC

The final tool that the **MMC** provides is CIFS open file management. Figure 25 illustrates the CIFS **Open Files** manager screen. This screen lists all files currently open by CIFS clients, including information about the particular file or folder, the user accessing the client, the number of locks, and the read mode. This tool is a useful management tool, because an administrator can close any open files through this interface.



Open File	Accessed By	Type	# Locks	Open Mode
I:\Data	ADMINISTRATOR	Windows	0	Read

Figure 25: TaskSmart NAS Management screen (MMC), Open Files manager

Closing a Single Open File

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Open Files**.
2. Highlight the file to close.
3. Select **Action** from the toolbar, and then click **Close Open File**.

Closing All Open Files

1. From the MMC, select **File Sharing**, **Shared Folders**, and **Open Files**.
2. Deselect all the files from the list that are to remain open.
3. Select **Action** from the toolbar, and then click **Disconnect All Open Files**.

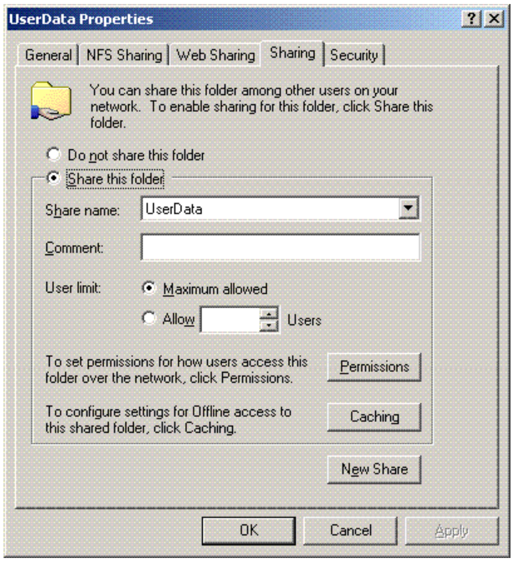
CAUTION: Disconnecting all the open files forcibly closes all files that CIFS users currently have open. Data loss can occur when users are editing affected files.

Share Management Using Windows Explorer

CIFS shares can also be administered through the Windows Explorer interface on the appliance.

Creating a CIFS share using Windows Explorer

1. From Windows Explorer, right-click the folder to share.
2. Select **Properties**. The **Properties** dialog box is displayed.



UserData Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: UserData

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

Figure 26: UserData Properties dialog box

3. Select the **Sharing** tab, and then select **Share this folder**.

Note: The folder name is inserted as the share name by default. If a default is not provided, then a share with the same name as the folder already exists.

4. Select an appropriate user limit.
5. Click **Permissions**, and then assign the appropriate values.
6. Click **Caching** to set up caching settings.

Note: See the section, “Modifying a Share Using the MMC,” earlier in this document, for assistance in the administration of user limits, permissions, or caching.

7. Click **OK** to apply all share properties.

Sharing a Folder With a Different Name

Use the following instructions to add a different name to the existing share:

1. From Windows Explorer, right-click the folder to share.
2. Select **Properties**, and then select the **Sharing** tab.
3. Click **New Share**. The **New Share** dialog box is displayed.

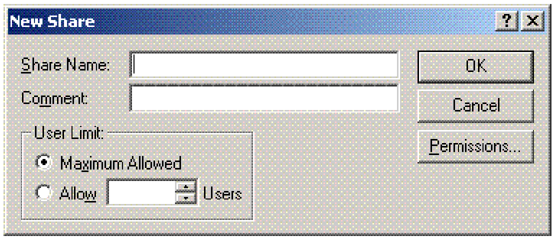


Figure 27: New Share dialog box

4. Enter the new share name, a descriptive comment, and an appropriate user limit.
5. Select **Permissions** to apply different permissions to the new share name.

> **Note:** This feature can be used to ensure compatibility between NFS and CIFS shares with spaces in their names. It can also be shared without the space so that at least one CIFS share name is identical to the NFS export name for the same folder. This feature is also useful for providing a different security model on the same data.

6. Click **OK** to return to the **Share Properties** dialog box.
7. Click **OK** to apply all changes.

Deleting a CIFS Share Using Windows Explorer

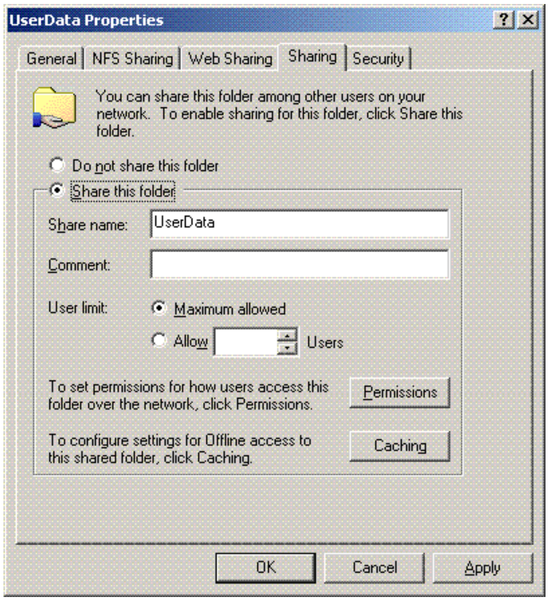
To delete a CIFS share through the Windows Explorer interface:

1. From Windows Explorer, right-click the folder to delete.
2. Select **Properties**, and then select the **Sharing** tab.
3. Select **Do not share this folder**.
4. Click **OK**.

Modifying a CIFS Share Using Windows Explorer

To modify a CIFS share through the Windows Explorer interface:

1. From Windows Explorer, right-click the folder to change.
2. Select **Properties**, and then select the **Sharing** tab.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: UserData

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

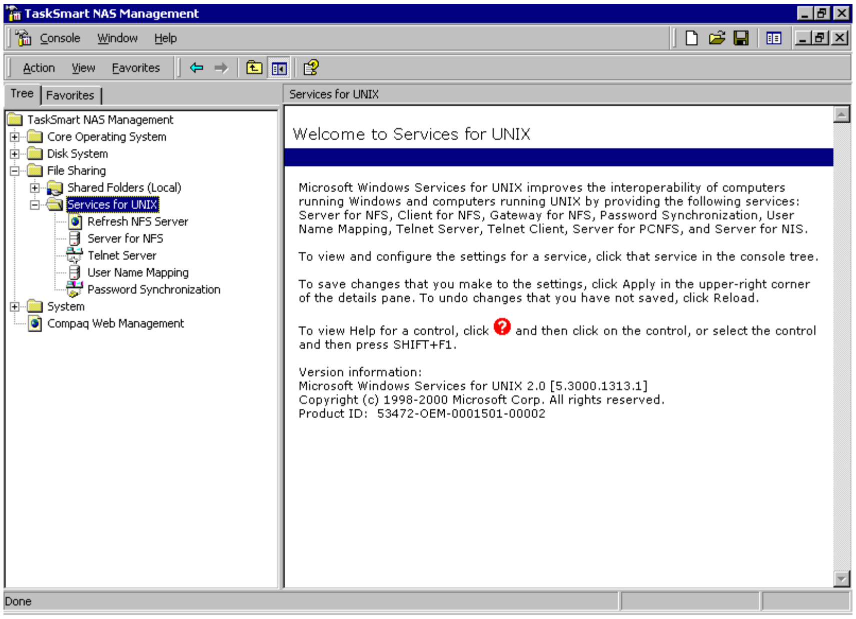
Figure 28: UserData Properties dialog box, Sharing tab

3. If needed, change the user limit.
4. To change the share permissions, select **Permissions**.
5. To change caching settings, select **Caching**.

UNIX Network Integration

Microsoft Services for UNIX (SFU) is a comprehensive software package designed to provide complete UNIX environment integration of an NT file server.

Figure 29 illustrates the Services for UNIX user interface on the TaskSmart N-Series appliance.



Welcome to Services for UNIX

Microsoft Windows Services for UNIX improves the interoperability of computers running Windows and computers running UNIX by providing the following services: Server for NFS, Client for NFS, Gateway for NFS, Password Synchronization, User Name Mapping, Telnet Server, Telnet Client, Server for PCNFS, and Server for NIS.

To view and configure the settings for a service, click that service in the console tree.

To save changes that you make to the settings, click Apply in the upper-right corner of the details pane. To undo changes that you have not saved, click Reload.

To view Help for a control, click ? and then click on the control, or select the control and then press SHIFT+F1.

Version information:
Microsoft Windows Services for UNIX 2.0 [5.3000.1313.1]
Copyright (c) 1998-2000 Microsoft Corp. All rights reserved.
Product ID: 53472-OEM-0001501-00002

Figure 29: Services for UNIX user interface

The following SFU components are described in this section:

- Network File system (NFS)
- Server for NFS
- User Name Mapping
- Mortice Kearn Systems (MKS) Toolkit

Network File System

Network File System (NFS) is a networking protocol for exporting UNIX file systems across a network.

There are three key goals of NFS:

- Allow different UNIX machines to transparently export files across a network.

  This feature works across different versions of UNIX and across different platforms. For example, a LINUX machine can access files on a remote *Tru64*™ UNIX machine. Accessing these files is transparent to both the administrator and the users. The administrator and the user do not notice any difference between accessing local files or files on the remote machine.

- Make administration as easy as possible.

  The remote file system attaches to the local machine in the same manner that the local file system does. The administrator is able to add a remote file system in the same manner as adding another hard drive or external storage.

- Focus exclusively on file system operations.

  The file system is used only for exporting file systems to remote machines. It supports only operations such as read, write, create, delete, and copy.

NFS export permissions are slightly different from Windows NT shares. NFS exporting may specify read only or read/write permissions, and may specify one or more client system names that are granted access to the export. Some exports can be open to all client systems.

NFS Configurations

There are two versions of NFS, version 2 and version 3. Version 3 supports additional file operations that version 2 does not have, such as asynchronous file operations.

NFS has the capacity to operate with the following two different network protocols:

- User Datagram Protocol (UDP)
- Transport Control Protocol (TCP)

Traditionally, NFS operates with UDP for performance purposes, but it can also operate with TCP. This operating ability allows for four possible combinations:

- NFS version 2 operating with UDP
- NFS version 2 operating with TCP
- NFS version 3 operating with UDP
- NFS version 3 operating with TCP

NFS Authentication

NFS export access is granted or denied to clients based on the client name or IP address. The server determines whether or not a specific client machine has access to an NFS export. No user logon to the NFS server takes place when a file system is exported by the NFS server. Permission to read or write to the export is granted to specific client machines. For example, if client machine M1 is granted access to an export but client machine M2 is not, then user “jdoe” can access the export from M1 but not from M2.

The permissions are on a per-export basis. This policy means that each export has its own permissions, independent of other exports on the system. For example, file system “a” can be exported allowing only the Accounting department access, and file system “m” can be exported allowing only the Management department access. If a user in Management needs access to Accounting’s information, the “a” export permissions can be modified to let that one user’s client machine have access. This modification does not affect other client access to the same export, and does not allow the Management user or client access to other exports.

After the client machine has permission to the export, the user logon affects file access. The client machine presents the user ID (UID) and the group ID (GID) of the UNIX user to the server. When accessing a file, the user logon is compared against the typical UNIX permissions of "user", "group", and "other", and typical UNIX access is applied. See the section, "User Name Mapping," later in this document for more information on UID and GID.

Note: User credentials are not questioned or verified by the NFS server. The server assumes that the presented credentials are valid and correct.

If the NFS server does not have a corresponding UID, GID, or if the administrator has set other conditions to filter out the user, a process called "squashing" takes effect. Squashing is when an unknown or filtered user is converted to an "anonymous" user. This user has very restricted permissions on the system. Squashing helps administrators manage access to their exports, by allowing them to restrict access to certain individuals or groups, and squash everyone else down to a user that has restricted (or no) access. Squashing enables the administrator to allow permissions, instead of denying access to all the individuals who are not supposed to have access. See the section "User Name Mapping," later in this document for more details.

Server for NFS

The Services for UNIX NFS server provides native file system support for NFS. Windows NT files can be exported and accessed through NFS.

Until recently, UNIX used only NFS to export files. UNIX was not able to share files with Windows platforms, and Windows platforms were not able to share files with UNIX.

This restriction caused UNIX clients to require UNIX file servers, and Windows clients to require Windows file servers. Windows platforms and UNIX platforms were completely separate environments, causing the duplication of hardware, overhead, and effort.

SFU enables UNIX clients to use Windows-based machines as file servers. The SFU Server for NFS supports NFS v 2 and v 3, and supports them both on the TCP and UDP network protocols.

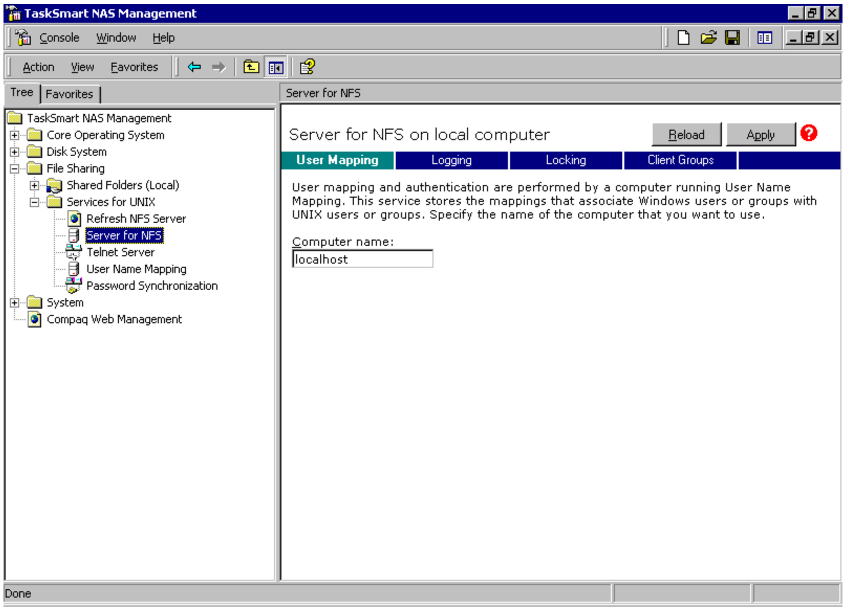
SFU Server for NFS is more fully integrated into the operating system than other third-party NFS server packages. The administrative interface for NFS exports is similar to the CIFS sharing interface used by Windows platforms.

Multiple Domains and Multiple NIS Support

SFU supports user mappings between one or more Windows NT Domains and one or more NIS Domains. The default SFU setup supports multiple NT Domains to a single NIS Domain. For information about setting up SFU to map users in multiple NIS multiple Domains, consult the Compaq "OEM Supplemental Help" section in the SFU online help.

Implementing NFS

1. From the MMC, select **File Sharing**, and then **Services for UNIX**. Then, select **Server for NFS**.



User mapping and authentication are performed by a computer running User Name Mapping. This service stores the mappings that associate Windows users or groups with UNIX users or groups. Specify the name of the computer that you want to use.

Computer name: localhost

Figure 30: Server for NFS user interface, User Mapping pane

2. In the **Computer name** field, enter the name of the computer designated for user mapping and authentication.
3. To run user mapping on the TaskSmart N-Series appliance, enter `localhost`.
4. If a machine other than the localhost is to be used, verify that the user name mapping service is installed and operating on that machine.

Setting the Permissions for NFS Exporting

This section contains the basic procedure to set the permissions for NFS exporting. For more details on NFS exporting, refer to “Services for UNIX Help” in the Readme and Product Information file on the TaskSmart N-Series console.

1. Double-click the **My Computer** icon on the desktop.
2. Create a new folder, or select an existing folder in the Windows Explorer interface.
3. Highlight the selected folder or virtual disk.
4. Right-click the item, select **Sharing**, and then click the **NFS Sharing** tab.
5. Select **Share this folder**, and then set the sharing name.
6. Click **Permissions** to set the export (or share) permissions, client groups, and root access, if desired.

Testing NFS

1. Establish a folder to export, and then export it to NFS clients.
2. From a UNIX or LINUX client, enter **showmount -e** (TaskSmart N-Series name).

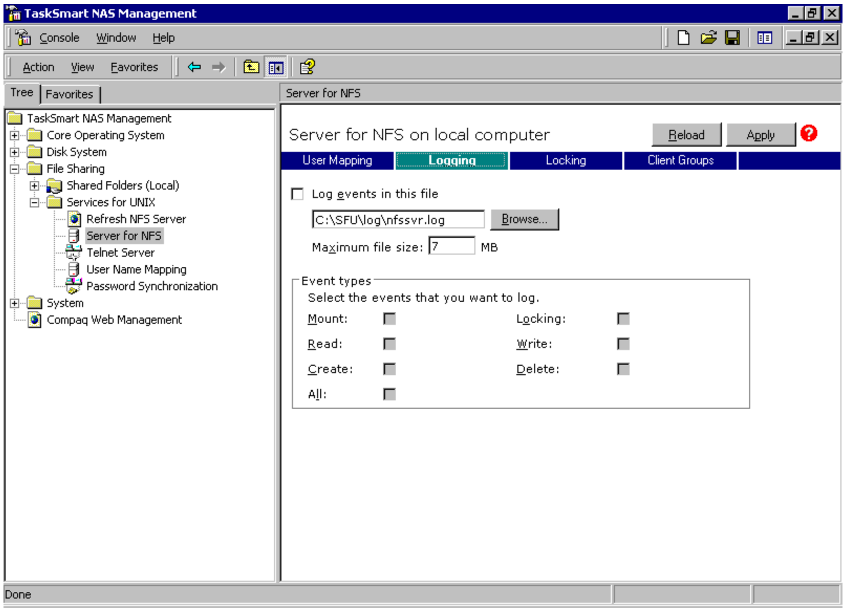
   The **showmount** command works only after the TaskSmart N-Series name is added to the /etc/hosts file of the UNIX client, or if the Domain Name System (DNS) recognizes the TaskSmart N-Series name.
3. Compile a list of exported file systems that the TaskSmart N-Series appliance is exporting to NFS clients.
4. To attach an exported file system to the client directory called **/mount-point**, open the client console screen, and then enter:

   ```
   mount –t nfs servername:/exportname /mount-point
   ```

NFS Event Logging

Various levels of auditing are available in the **Logging** tab of the **Server for NFS** user interface. Auditing sends SFU events to a file for later review and establishes log setting behavior. Some behavior examples include events logged and log file size. For more information, refer to “Services for UNIX Help” in the Readme and Product Information file on the TaskSmart N-Series console.

1. From the **Server for NFS** user interface, select the **Logging** tab.
2. Select **Log events in this file**.
3. Either provide a filename or use the default filename provided (rootdrive\SFU\log\nfssvr.log). Additionally, either provide a maximum file size for the log or use the default log file size (7 MB). The log file is not created initially, but is created when changes are applied.



Server for NFS on local computer

☐ Log events in this file

C:\SFU\log\nfssvr.log

Maximum file size: 7 MB

Event types

Select the events that you want to log.

Mount: ☐ Locking: ☐

Read: ☐ Write: ☐

Create: ☐ Delete: ☐

All: ☐

Figure 31: Server for NFS user interface, Logging pane

NFS File Locking

NFS supports the ability to lock files. File locking helps prevent two or more users from working with the same files at the same time.

For example, Microsoft Office or Star Office places a lock on an open file to prevent other users from editing the file at the same time. NFS supports this action.

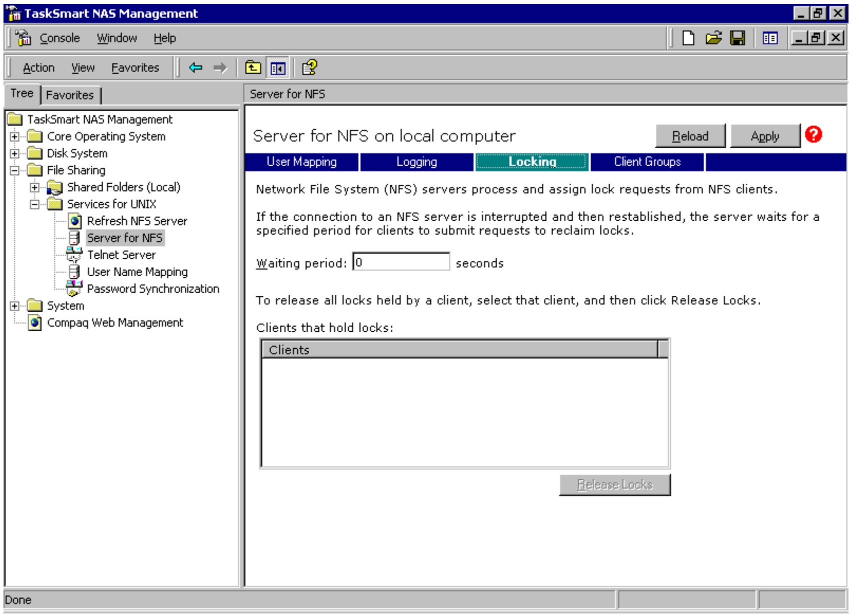
However, NFS locking is advisory. It is not forced on the user. NFS locking depends on the software application components to manage the locks. If an application does not lock a file, or if a second application does not check for locks before writing to the file, there is nothing stopping the users from overwriting files.

File locking is set up in the **Locking** tab of the **Server for NFS** user interface.

From within the **Locking** tab, the **Waiting period** setting determines how long the TaskSmart N-Series appliance allows the locks to be kept open after a client or server crashes. The TaskSmart N-Series appliance keeps the locks open for this time limit 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 open. Otherwise, the TaskSmart N-Series appliance release

s the lock.

The locking user interface also allows the administrator to manually clear locks. Figure 32 illustrates the SFU Server for NFS user interface for file locking.



Server for NFS on local computer

Network File System (NFS) servers process and assign lock requests from NFS clients.

If the connection to an NFS server is interrupted and then restablished, the server waits for a specified period for clients to submit requests to reclaim locks.

Waiting period: 0 seconds

To release all locks held by a client, select that client, and then click Release Locks.

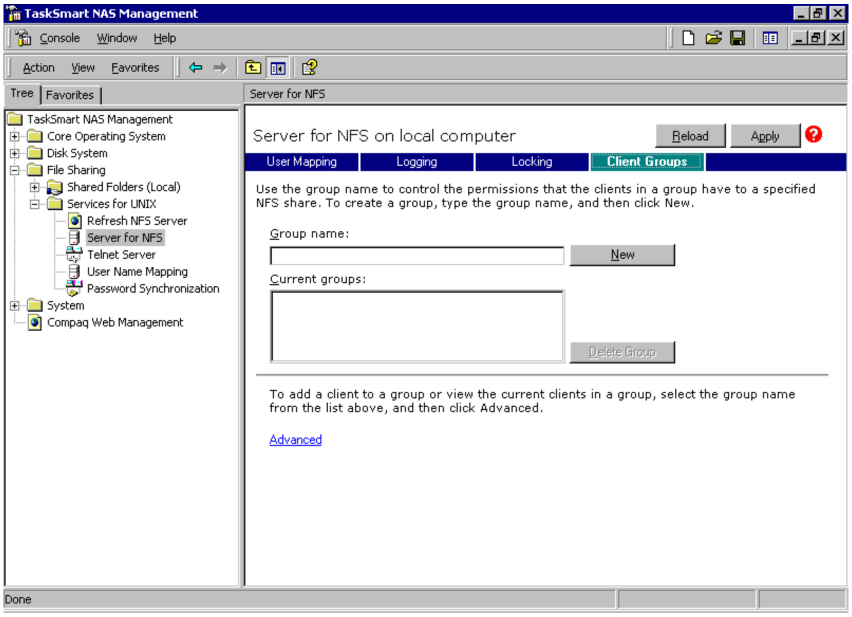
Clients that hold locks:

Figure 32: Server for NFS user interface, file Locking pane

NFS Client Groups

The client groups feature gives administrators a method of assigning access permissions to a set of clients. The administrator creates a client group, gives it a name, and then inserts clients into the group by client name or IP address. After the client group is created, the administrator adds or removes permissions from the entire group, instead of allowing or denying access for each individual client machine.

Groups are administered in the **Client Groups** tab of the **Server for NFS** user interface. Figure 33 illustrates the client groups user interface.



Use the group name to control the permissions that the clients in a group have to a specified NFS share. To create a group, type the group name, and then click New.

To add a client to a group or view the current clients in a group, select the group name from the list above, and then click Advanced.

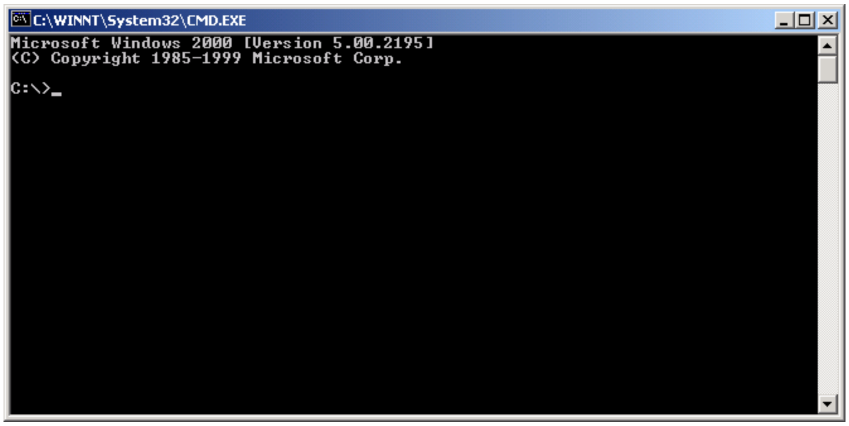
Figure 33: Server for NFS user interface, Client Groups pane

Note: Currently, the client group is allowed to assume the same name as a client. This duplication obscures the client from the view of the server. For example, assume a client d4 exists. If a client group called d4 is created, permissions can no longer be assigned to just the client d4. Any reference to d4 now refers to client group d4.

NFS Command-Line Capabilities

The command-line provides the administrator flexibility to automate setups and other tasks through scripting. All of the SFU file exporting tasks, and other SFU activities, can be accomplished from a command prompt.

Figure 34 and Table 6 illustrate and describe the command-line interface.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>_
```

Figure 34: Command-line user interface

Table 6. Command-Line Interface Command Prompts

Command	Function
nfsexport /?	Learn how to view, rename, create, and delete NFS export drives
nfsstat /?	Learn about viewing statistics by NFS operation type
showmount /?	View the format of the command to display NFS export settings on NFS servers
showmount -a	View users who are connected and what they currently have mounted
showmount -e	View exports from the server and their export permissions
rpcinfo /?	Learn how to display Remote Procedure Call (RPC) settings and statistics
mapadmin /?	View how to add, delete, or change user name mappings
tnadmin /?	View how to change Telnet Server settings
nfsshare /?	Learn how to display, add, and remove exported shares

User Name Mapping

User name mapping is the process of taking user and group identification from one environment, and translating it into user and group identification in another environment. This section defines and describes the purpose and use of user name mapping.

In the context of UNIX and NFS, user and group identification is a combination of a user ID (UID) and group ID (GID). In Windows environments, a user identification is a security ID (SID), or globally unique identifier (GUID) for Windows 2000.

When a fileserver is exporting files within a homogeneous environment, there are no problems with authentication. It is a simple matter of making a direct comparison to determine whether the user should be allowed access to the file, and what level of access to allow.

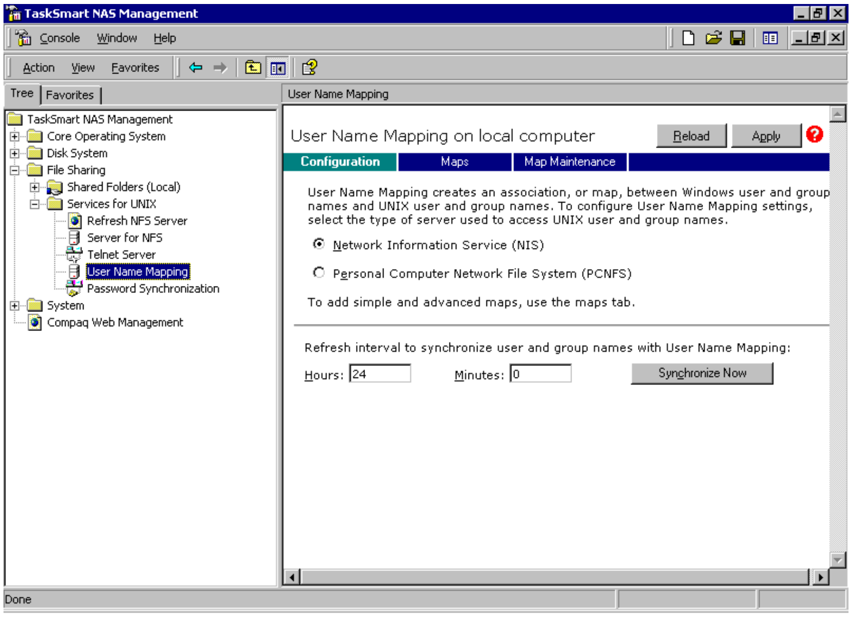
However, when a fileserver is working in a heterogeneous environment, some method of translating user access is required. User name mapping is the process of translating the user security rights from one environment to another.

As described in the previous section, the Server for NFS grants or denies access to the export based on machine name or IP address. However, after the client machine has access to the export, user-level permissions are used to grant or deny access to user files and directories.

The TaskSmart N-Series appliance is capable of operating in a heterogeneous environment, meaning it is able to work with both UNIX and Windows clients. Because the files are stored in the native Windows NT file system, the server has to map the UNIX users to Windows users to determine the user access level of the files.

Note: User name mapping is not designed to address existing user database problems in the existing environment. All UIDs and GIDs must be unique across all UNIX Domains and all SIDs, and GUIDs must be unique across all Windows NT Domains. See the section, “Creating Simple User Name Maps,” later in this document for additional information on NIS.

Figure 35 illustrates the SFU User Name Mapping user interface.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

● Network Information Service (NIS)

○ Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 35: User Name Mapping user interface

Implementing User Name Mapping

User name mappings are most easily done in the Microsoft Management Console. Additionally, there is a command-line interface for the mapping server. However, the GUI interface makes it very easy to map users.

The mapping server makes a distinction between two different modes of mapping:

- Simple
- Advanced

In simple mode, user and group names that exactly match across Windows and UNIX are automatically equated by user name. This comparison is done automatically by the user name mapping server. It is possible for the administrator to disable this feature.

Note: If this feature is turned off, the administrator must use advanced mode and manually map each user.

In advanced mode, the administrator can manually map any users and groups to any other users and groups. Advanced maps override simple maps, giving administrators the capability of using simple mapping for most users, and then using advanced mappings to make changes to simple mappings. This combination makes the administrator's job much easier.

SFU currently supports squashing. The default user is "ANONYMOUS LOGON", but can be changed. For more details on how to change the default squashing user, refer to the Compaq "OEM Supplemental Help" chapter of the online SFU help, found on the TaskSmart N-Series console.

Figure 36 is a diagram showing an example of how the mapping server works for an "ls-al" command.

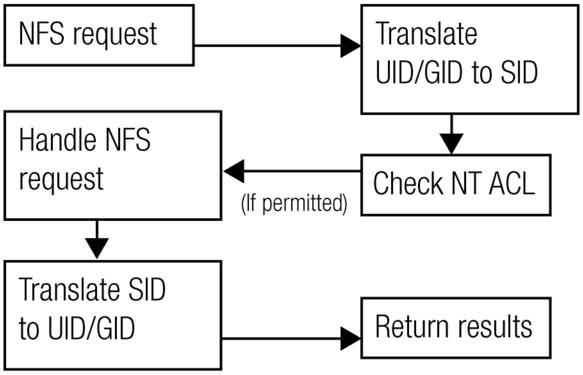


Figure 36: Mapping server ls-al command example

A double translation, as illustrated above, is sometimes necessary because some commands return user ID information. For example, if the NFS request issued was an "ls-al" command, the return listing of files contains user information (the user and group that own the file). Because this information is contained in an NT Access Control List (ACL), this information is not UNIX ready. The ACL information must be converted back to UNIX UIDs and GIDs, for the UNIX systems to understand and display the user information.

This second translation is not done for commands that do not return user information. For example, if the NFS request was just to read data from or write data to a file, the second translation would not be performed because there is no returning user information.

Requirement

The Server for NFS Authentication software must be installed on all Primary Domain Controllers (PDCs) and Backup Domain Controllers (BDCs) that have NT users mapped to UNIX users. See the following section, “Installing User Name Mapping for NFS Authentication,” for details.

Limitation

User name mapping is system-wide, as opposed to export-by-export. In SFU, whomever the user is mapped to applies to all file systems. Any changes to the default squashing user are also system-wide.

Installing User Name Mapping for NFS Authentication

1. Locate the *SFUCUSTOM.MSI* file in the SFU directory.
2. On the Domain controller where the service is being installed, use Windows Explorer to open the shared directory containing *SFUCUSTOM.MSI*.
3. Double-click the file to open it. Windows Installer is launched automatically.

   If the Domain controller used does not have Windows Installer installed, locate the file *InstMSI.exe* in the SFU directory and run it. After this installation, the Windows Installer program starts when opening *SFUCUSTOM.MSI.*
4. Click **Next** when the **Welcome to Windows Services for UNIX** screen is displayed.
5. Enter the name of the user and the organization, and then click **Next**.
6. Accept the license agreement, and then click **Next**.
7. Select the default option if using only Authentication Tools for NFS, or select **Will be installed on local hard drive** for **Password Synchronization** to have NFS Authentication and Password Synchronization installed.
8. Select the directory where Server for NFS Authentication is to be installed, and then click **Next**.
9. Click **Finish** when installation is complete.

IMPORTANT: The installation of the user name mapping service is required on all primary Domain controllers and backup Domain controllers for Domains that have Windows users mapped to UNIX users.

Mapping Procedures

The TaskSmart N-Series appliance stores the data in an NTFS file system. The user name mapping server must translate the UNIX users into Windows users, so that the appliance can determine user access rights to the data.

The administrator designates the source of mapping information for both CIFS and NFS client users.

- UNIX: Local files or NIS
- CIFS: Local or Windows NT Domain

Using User Name Mapping across one or more Windows Domains requires the installation of Server for NFS Authentication on all PDCs and BDCs that have Windows users mapped to UNIX users.

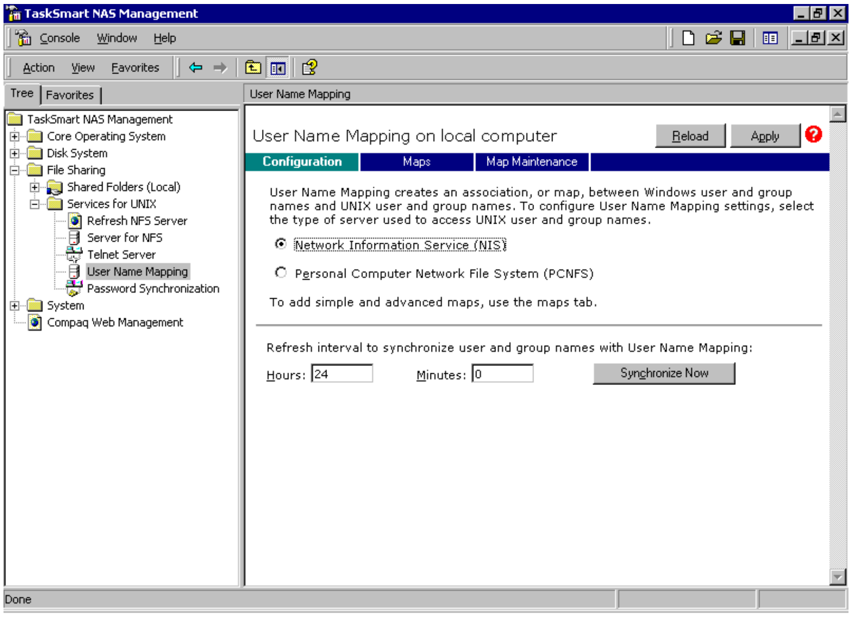
Creating Simple User Name Maps

Two levels of mapping, simple and advanced, allow for user name matching. The administrator must determine the appropriate level of mapping.

Simple, or implicit, is the first level of user name mapping. Simple user name mapping automatically equates Windows NT logons and UNIX logons with matching spellings, whether they are actually the same users or not. The user name mapping service allows the administrator to enable or disable simple mapping.

The administrator can map one or more Windows NT Domains to one Network Information Service (NIS) Domain.

Figure 37 illustrates the **User Name Mapping** user interface.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

● Network Information Service (NIS)

○ Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 37: User Name Mapping user interface, NIS Configuration pane

Basic Guidelines for Creating Simple User Name Maps

1. From the MMC, select **File Sharing**, **Services for UNIX**, and then **User Name Mapping**. Then, select the **Configuration** tab.
2. Click either **Network Information Systems (NIS)**, or **Personal Computer Network File System (PCNFS)**.

   For NIS configurations, the refresh fields determine how often the mapping server connects to the NIS Domains to update the UNIX user list.

   For PCNFS configurations, the refresh fields determine how often the files are refreshed from disk.

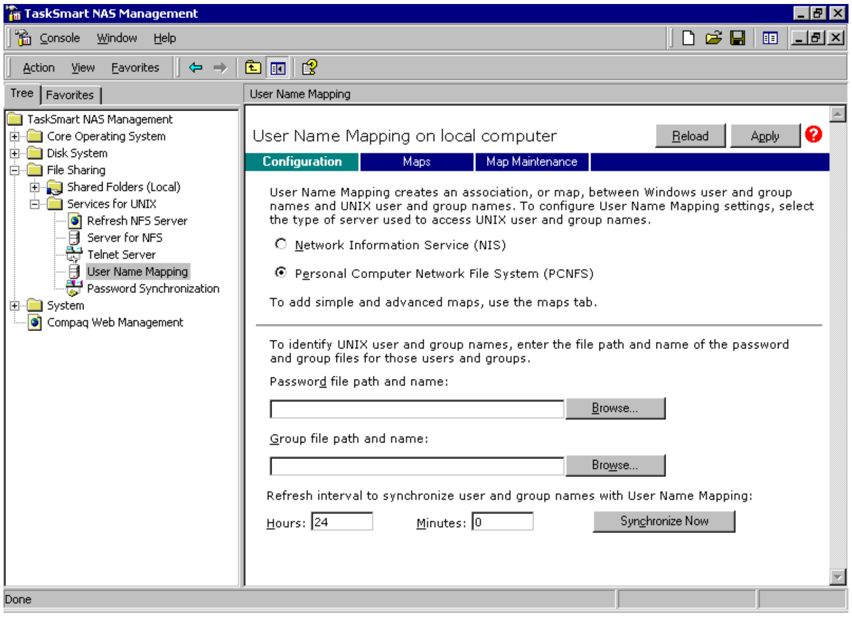
   If the administrator is not using NIS, the following files from the UNIX machine must be obtained and copied to the TaskSmart N-Series appliance:

   -/etc/password

   -/etc/group
3. Select the **Maps** tab, and then enter the mapping settings. These settings include specifying whether a map is simple or advanced, and indicating the mapping match.

Creating Simple User Name Maps using PCNFS

1. From the MMC, select **File Sharing**, **Services for UNIX**, and **User Name Mapping**. Then, select the **Configuration** tab.
2. Click **Personal Computer Network File system (PCNFS)**.
3. The **Password** and the **Group** fields are displayed. In the appropriate box, enter the path and name of the local password and group files, or click **Browse** to locate the files. Figure 38 illustrates the PCNFS Configuration screen.



User Name Mapping on local computer

User Name Mapping creates an association, or map, between Windows user and group names and UNIX user and group names. To configure User Name Mapping settings, select the type of server used to access UNIX user and group names.

○ Network Information Service (NIS)

● Personal Computer Network File System (PCNFS)

To add simple and advanced maps, use the maps tab.

To identify UNIX user and group names, enter the file path and name of the password and group files for those users and groups.

Password file path and name:

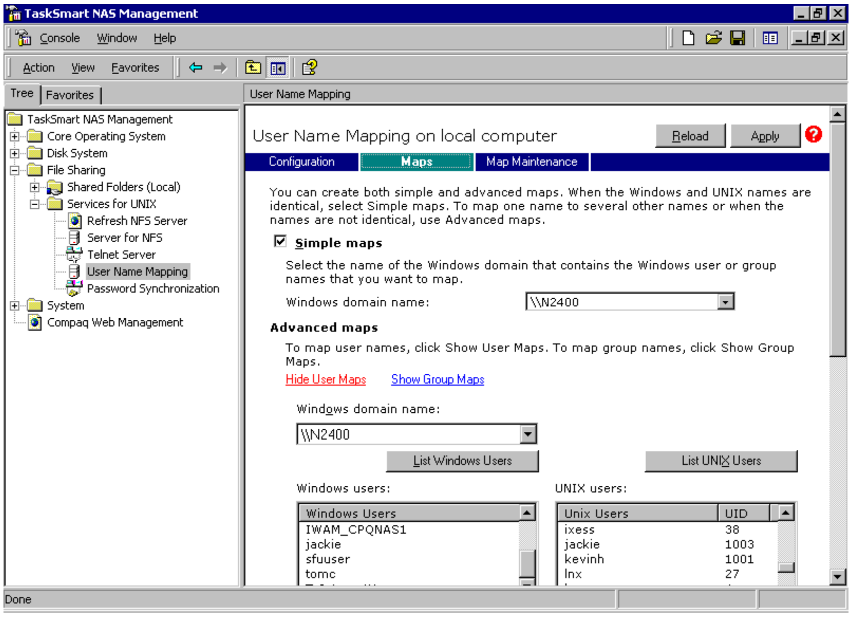
Group file path and name:

Refresh interval to synchronize user and group names with User Name Mapping:

Hours: 24 Minutes: 0

Figure 38: User Name Mapping user interface, PCNFS Configuration pane

4. Select the **Maps** tab. Figure 39 is an example of the PCNFS simple mapping screen.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☑ Simple maps

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

Windows users:

Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc

UNIX users:

Unix Users	UID
ixess	38
jackie	1003
kevinh	1001
lnx	27

Figure 39: Simple maps for PCNFS, Maps pane (top portion)

5. Select **Simple Maps**.

6. In the **Windows domain name** drop-down box, select the domain name to map.

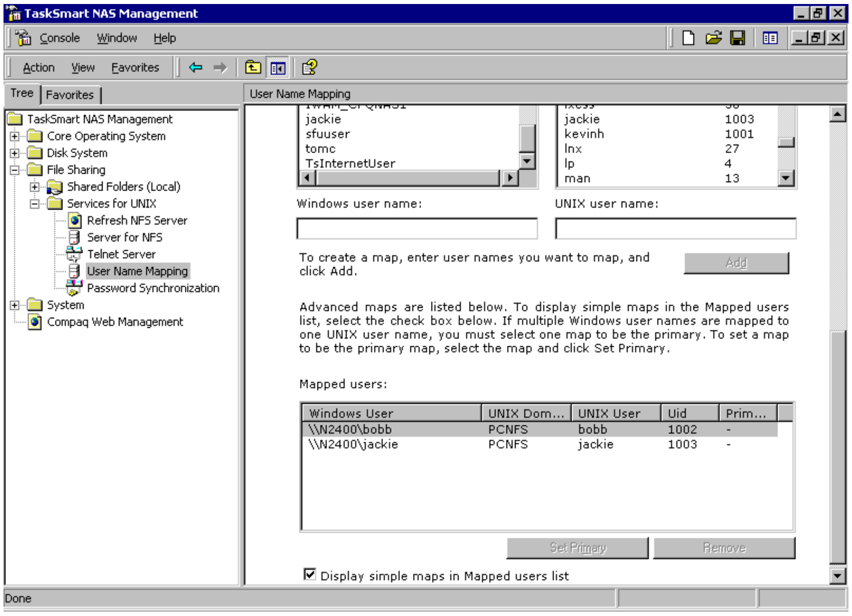
IMPORTANT: Only one domain can have simple mappings. For information about how to set up simple maps for multiple domains, refer to the Compaq "OEM Supplemental Help" chapter of the online SFU help found on the TaskSmart N-Series console.

7. Click **Apply** at the top of the screen to save these changes.

8. Click **Show Users Maps**, or **Show Groups Maps**, depending on the type of map list needed. This link is found in the **Advanced Maps** section at the bottom of half of the screen. See Figure 39 for an example of this screen display.

   When mapping multiple Windows domains, choose the Windows domain from the **Windows domain name** drop-down box. Multiple domains will be listed only if domain trusts have been established.

9. Select **Display simple maps in Mapped users list** at the bottom of the screen. If simple maps are enabled, the display lists the maps that match in spelling for Windows and UNIX. Figure 40 is an example of the bottom part of the PCNFS simple mapping pane.



jackie
sfuuser
tomc
TsInternetUser

jackie	1003
kevinh	1001
lnx	27
lp	4
man	13

Windows user name:

UNIX user name:

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\bobb	PCNFS	bobb	1002	-
\\N2400\jackie	PCNFS	jackie	1003	-

☑ Display simple maps in Mapped users list

Figure 40: Simple maps for PCNFS, Maps pane (bottom portion)

Figure 40 lists simple user maps. The procedures for creating user maps and group maps are the same. To look at the simple group maps, select **Show Group Maps** and select **Display simple maps in Mapped groups list**. The group maps will be displayed in the **Mapped groups box** near the bottom of the screen.

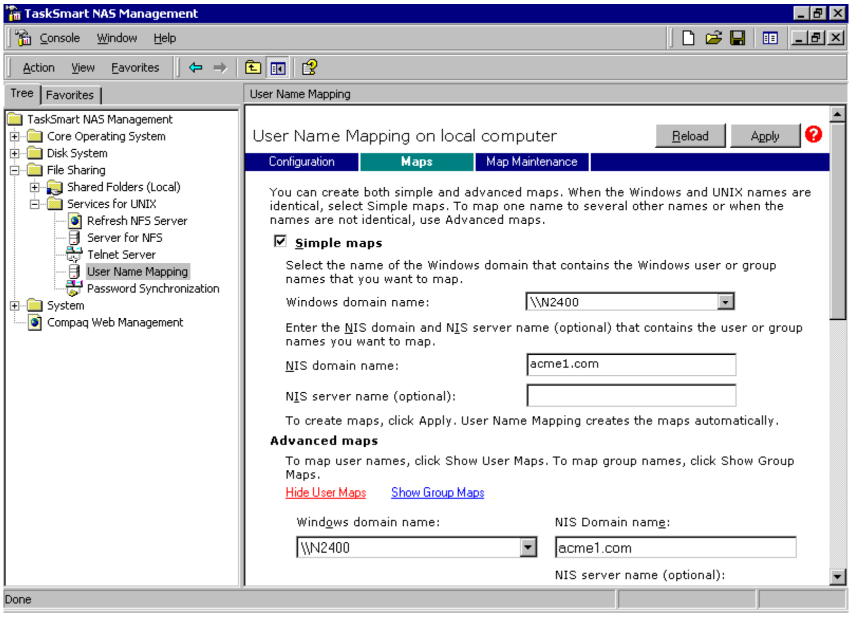
Creating Simple User Name Maps Using NIS

1. From the MMC, select **File Sharing**, **Services for UNIX**, and then **User Name Mapping**. Then, select the **Configuration** tab.
2. Select **Network Information Service (NIS)**.
3. Click the **Maps** tab.
4. Select **Simple Maps**.
5. Select the Windows domain name to map.

   Only one domain can have simple mappings. For information about how to set up simple maps for multiple domains, refer to the Compaq “OEM Supplemental Help” chapter of the online SFU help found on the TaskSmart N-Series console.
6. Enter the domain name of the NIS server. The NIS server name is optional.
7. Click **Apply** at the top of the screen to save these changes.

8. In the Advanced Maps section, click **Show Users Maps** or **Show Groups Maps** depending on what type of map list is needed.

   When mapping multiple Windows domains, choose the Windows domain from the **Windows domain name** drop-down box. Multiple domains will be listed only if domain trusts have been established.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☑ **Simple maps**

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Enter the NIS domain and NIS server name (optional) that contains the user or group names you want to map.

NIS domain name: acme1.com

NIS server name (optional):

To create maps, click Apply. User Name Mapping creates the maps automatically.

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Hide User Maps Show Group Maps

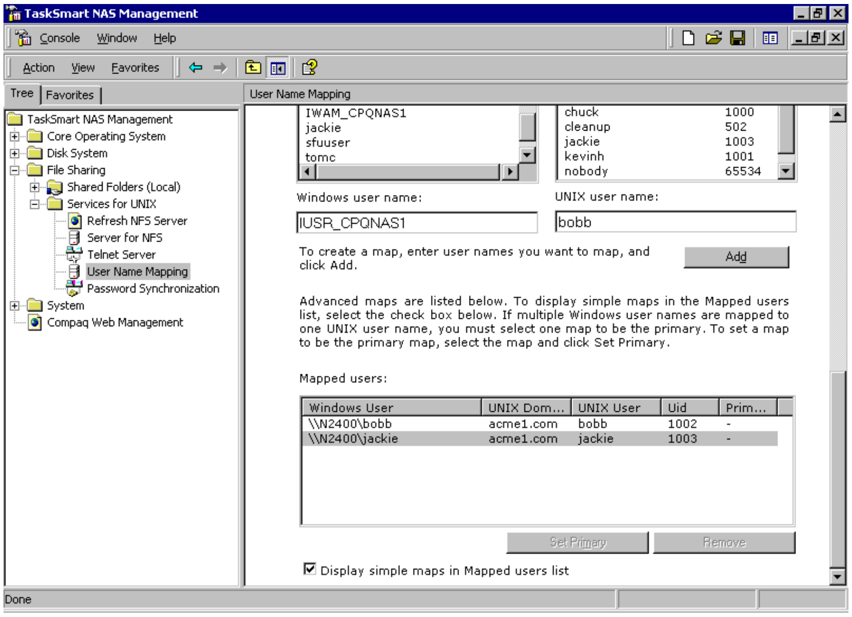
Windows domain name: \\N2400

NIS Domain name: acme1.com

NIS server name (optional):

Figure 41: Simple maps for NIS, Maps pane (top portion)

9. Select **Display simple maps in Mapped users list** at the bottom of the screen. A list of maps that match in spelling for Windows and UNIX is displayed in the **Mapped users** box. Figure 42 is an example of this screen display.



IWAM_CPQNAS1
jackie
sfuuser
tomc

chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534

Windows user name: IUSR_CPQNAS1

UNIX user name: bobb

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\bobb	acme1.com	bobb	1002	-
\\N2400\jackie	acme1.com	jackie	1003	-

☑ Display simple maps in Mapped users list

Figure 42: Simple maps for NIS, Maps pane (bottom portion)

Figure 42 lists simple user maps. The procedures for creating user maps and group maps are the same. To look at the simple group maps, select **Show Group Maps** and select **Display simple maps in Mapped groups list**. The group maps will be listed in the **Mapped groups** box.

Advanced User Name Maps

Advanced, or explicit, is the second level of user name mapping. Advanced user name mapping allows the administrator to specifically decide how matching is accomplished. The administrator manually lines up the Windows NT and UNIX user and group names.

Advanced mapping requires a primary user to be mapped when mapping multiple Windows users to a single UNIX user. If primary mapping is not indicated for a mapping, the map created first will become the primary map. The primary map is not indicated in the map listing.

Basic Guidelines for Creating Advanced User Name Maps

1. From the MMC, select **File Sharing**, **Services for UNIX**, and then **User Name Mapping**. Click the **Configuration** tab.
2. Select either **Network Information Systems (NIS)**, or **Personal Computer Network File System (PCNFS)**.

   For NIS configurations, the refresh fields determine how often the mapping server connects to the NIS Domains to update the UNIX user list.

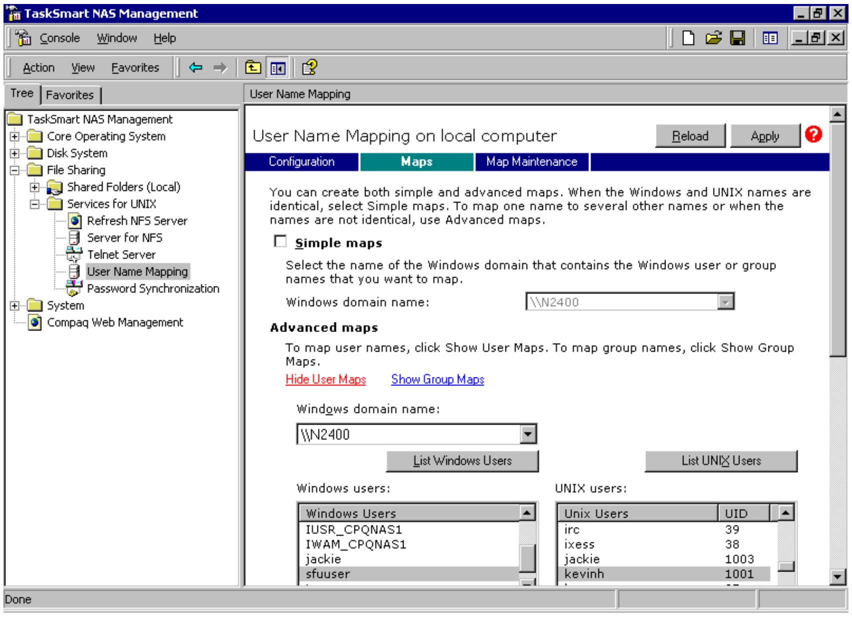
   For PCNFS configurations, the refresh fields determine how often the files are refreshed from disk.

   If the administrator is not using NIS, the following files from the UNIX machine must be obtained and copied to the TaskSmart N-Series appliance:

   ```
   -/etc/password
   -/etc/group
   ```
3. Select the **Maps** tab. Enter the appropriate mapping settings. These settings include specifying whether a map is simple or advanced, and indicating the mapping match.

Creating Advanced User Name Maps Using PCNFS

1. From the MMC, select **File Sharing**, **Services for UNIX**, and then **User Name Mapping**. Then, select the **Configuration** tab.
2. Select **Personal Computer Network File system (PCNFS)**.
3. Boxes for the path and name of the password and group files are displayed. Fill in these boxes accordingly, or click **Browse** to locate the files.
4. Select the **Maps** tab. Figure 43 is an example of the PCNFS mapping screen.
5. Click **Show Users** or **Show Groups** depending on what type of map needs to be created. This option is found in the Advanced Maps section of the screen.



User Name Mapping on local computer

You can create both simple and advanced maps. When the Windows and UNIX names are identical, select Simple maps. To map one name to several other names or when the names are not identical, use Advanced maps.

☐ **Simple maps**

Select the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: \\N2400

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

Windows users:

Windows Users
IUSR_CPQNAS1
IWAM_CPQNAS1
jackie
sfuuser

UNIX users:

Unix Users	UID
irc	39
ixess	38
jackie	1003
kevinh	1001

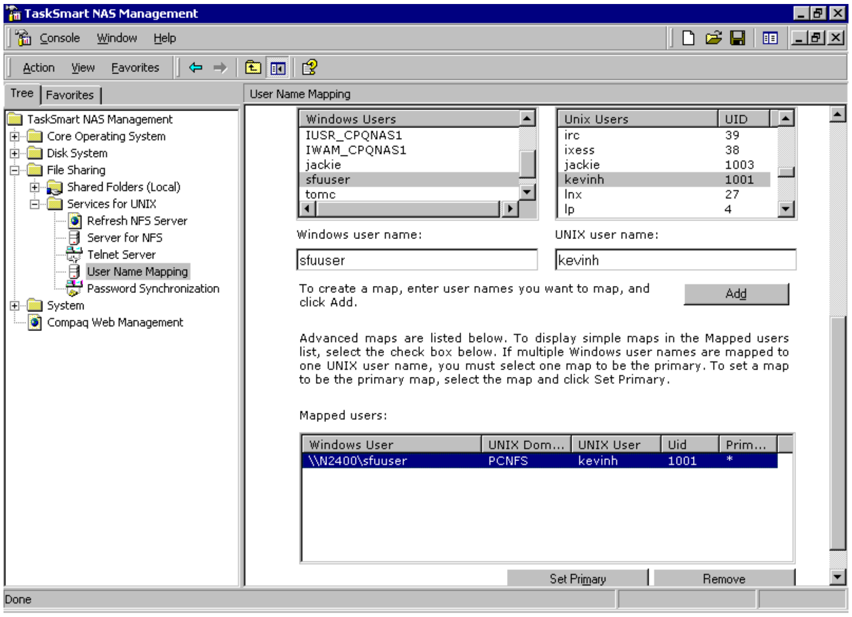
Figure 43: Advanced maps for PCNFS, Maps pane (top portion)

6. Click **List Windows Users** to display the Windows users.

   When mapping multiple Windows domains, choose the Windows domain from the **Windows domain name** drop-down box. Multiple domains will be listed only if domain trusts have been established.

7. Click **List UNIX Users** to display the UNIX users that are found in the password file that was previously supplied in the **Configuration** tab screen.

8. Highlight the **Windows user** and the **UNIX user** to map, and then click **Add**.



Windows Users
IUSR_CPQNAS1
IWAM_CPQNAS1
jackie
sfuuser
tomc

Unix Users	UID
irc	39
ixess	38
jackie	1003
kevinh	1001
lnx	27
lp	4

Windows user name: sfuuser

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\sfuuser	PCNFS	kevinh	1001	*

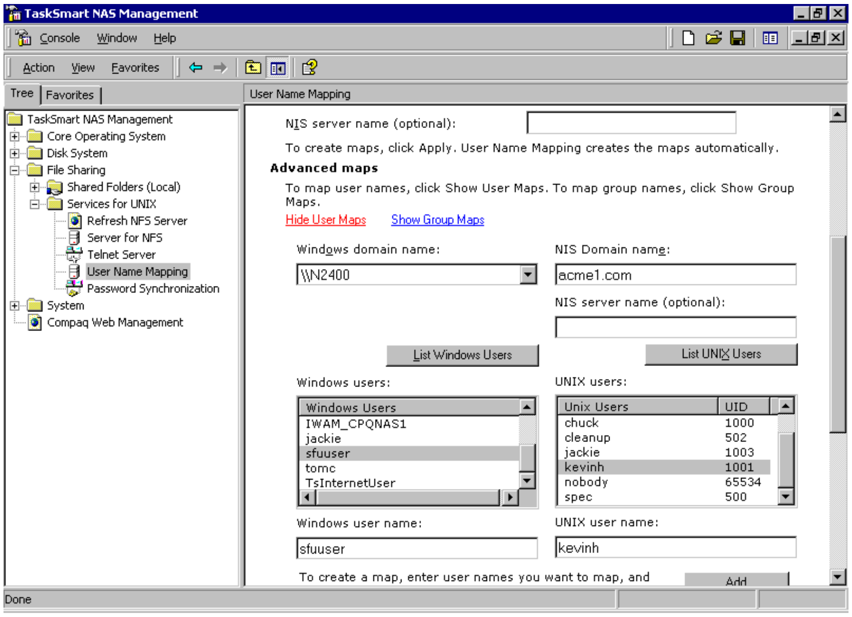
Figure 44: Advanced maps for PCNFS, Maps pane (bottom portion)

9. Repeat step 8 until all of the desired users are mapped.
10. Click **Apply** at the top of the screen to save these changes.

Figure 44 lists advanced user maps. The procedures for creating user maps and group maps are the same. To view the group maps, click **Show Group Maps** in the **Advanced maps** section of the screen.

Creating Advanced User Name Maps using NIS

1. From the **MMC**, select **File Sharing**, **Services for UNIX**, and **User Name Mapping**. Then select the **Configuration** tab. Click **Network Information Service (NIS)**.
2. Select the **Maps** tab.
3. Enter the domain name of the NIS server. The NIS server name is optional.
4. Click **Show Users** or **Show Groups** depending on what type of map is to be created. This link is found in the **Advanced maps** section of the screen.



NIS server name (optional):

To create maps, click Apply. User Name Mapping creates the maps automatically.

Advanced maps

To map user names, click Show User Maps. To map group names, click Show Group Maps.

Windows domain name: \\N2400

NIS Domain name: acme1.com

NIS server name (optional):

Windows users:

Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc
TsInternetUser

UNIX users:

Unix Users	UID
chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534
spec	500

Windows user name: sfuuser

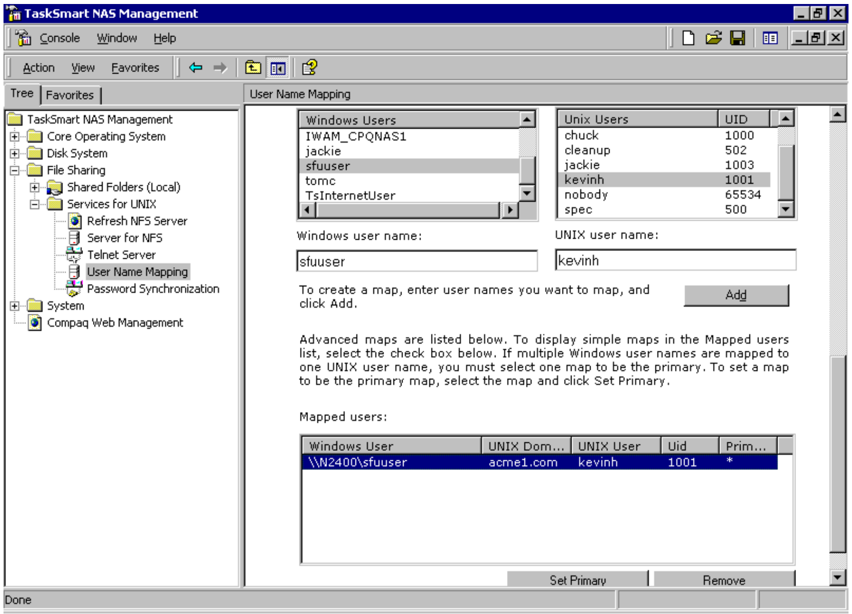
UNIX user name: kevinh

To create a map, enter user names you want to map, and

Figure 45: Advanced maps for NIS, Maps pane (top portion)

5. Click **List Windows Users** to display the Windows users.

   When mapping multiple Windows domains, choose the Windows domain from the **Windows domain name** drop-down box. Multiple domains will be listed only if domain trusts have been established.
6. Enter the NIS domain name. The NIS server name is optional.
7. Click **List UNIX Users** to display the UNIX users in the NIS domain.
8. Highlight the **Windows user** and the **UNIX user** to map, and then click **Add**.



Windows Users
IWAM_CPQNAS1
jackie
sfuuser
tomc
TsInternetUser

Unix Users	UID
chuck	1000
cleanup	502
jackie	1003
kevinh	1001
nobody	65534
spec	500

Windows user name: sfuuser

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\sfuuser	acme1.com	kevinh	1001	*

Figure 46: Advanced maps for NIS, Maps pane (bottom portion)

9. Repeat step 8 until all of the users are mapped.
10. Click **Apply** at the top of the screen to save these changes.

Figure 46 lists advanced user maps. The procedures for creating user maps and group maps are the same. To view the group maps, click **Show Group Maps** in the **Advanced maps** section of the screen.

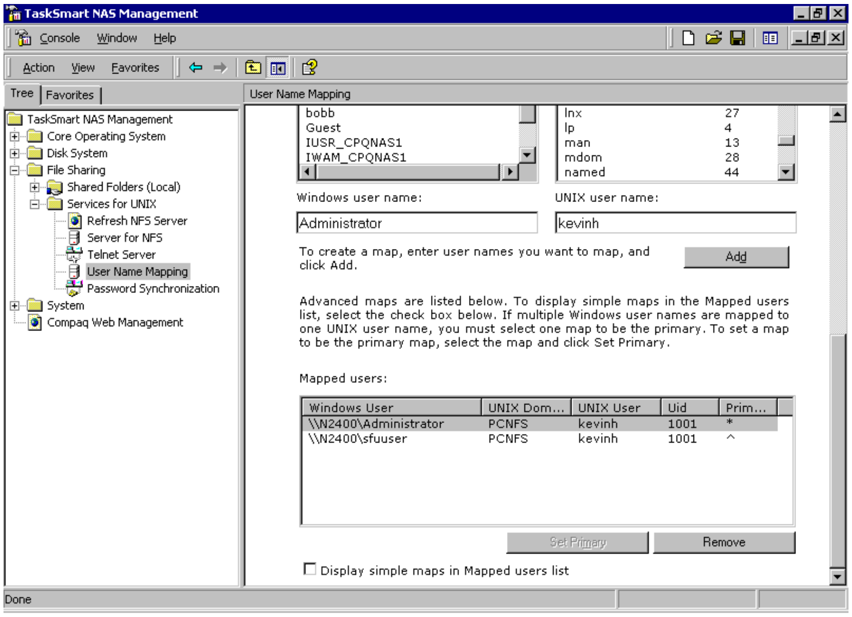
Creating Primary Mapping

When an initial mapping is created for a user or group, it is marked as primary by default. If multiple maps are created for one UNIX user or group to multiple Windows users or groups, a dialog box will be displayed, asking for which mapping to set as primary.

Note: The administrator must make sure to assign primary user mappings for any UNIX user that has more than one NT user mapped to them.

To create a primary map:

1. Select the Windows and UNIX user or group pair to be the primary mapping.
2. Click **Set Primary**. An asterisk in the **Primary Mapping** column in the **Mapped Users** section indicates that the primary mapping has been set for that user.
3. If a primary map already exists for the UNIX user, a dialog box is displayed, prompting for confirmation to set the selected mapping as the primary map.
4. Click **Apply** at the top of the screen to save these changes. Figure 47 illustrates the **User Name Mapping** screen after **Set Primary** is clicked.



Windows user name: Administrator

UNIX user name: kevinh

To create a map, enter user names you want to map, and click Add.

Advanced maps are listed below. To display simple maps in the Mapped users list, select the check box below. If multiple Windows user names are mapped to one UNIX user name, you must select one map to be the primary. To set a map to be the primary map, select the map and click Set Primary.

Mapped users:

Windows User	UNIX Dom...	UNIX User	Uid	Prim...
\\N2400\Administrator	PCNFS	kevinh	1001	*
\\N2400\sfuuser	PCNFS	kevinh	1001	^

☐ Display simple maps in Mapped users list

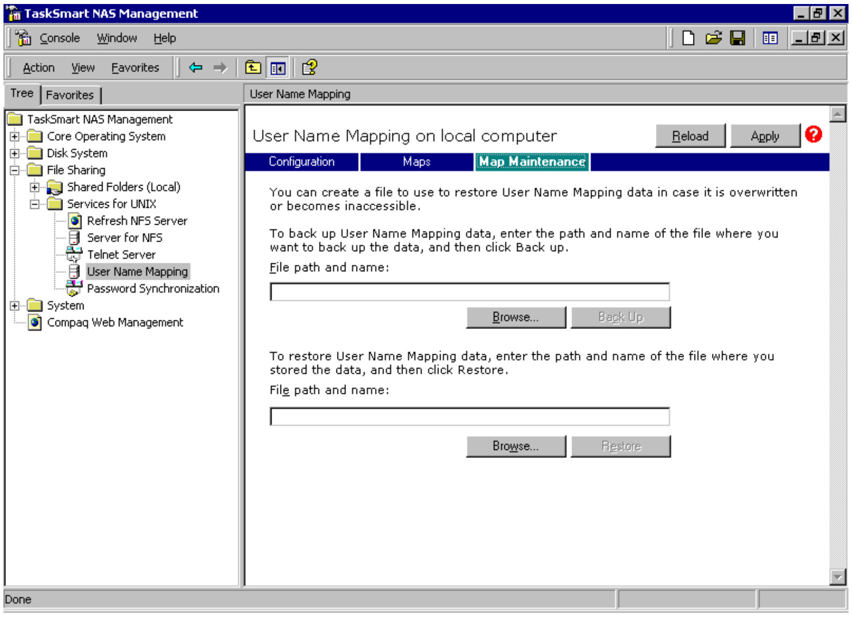
Figure 47: Primary User Mapping applied

These same procedures are used to either create or change primary group mappings.

Backup and Restoration of Mappings

User Name Mapping has the capability to save and retrieve mappings from files. This feature is useful for backing up mapping settings prior to making changes, and for exporting the mapping file from one server to another that is using the same mapping information.

The User Name Mapping server can save already-created mappings to a file, or can load them from a file and populate the mapping server. This feature is found in the **Map Maintenance** tab of the **User Name Mapping** screen, as shown in Figure 48.



You can create a file to use to restore User Name Mapping data in case it is overwritten or becomes inaccessible.

To back up User Name Mapping data, enter the path and name of the file where you want to back up the data, and then click Back Up.

File path and name:

To restore User Name Mapping data, enter the path and name of the file where you stored the data, and then click Restore.

File path and name:

Figure 48: User Name Mapping user interface, Map Maintenance pane

Backing up Map Settings

1. From the MMC, select **File Sharing**, **Services for UNIX**, and **User Name Mapping**. Select the **Map Maintenance** tab.
2. Enter the path and the name of the file to back up in the **File path and name** box, or click **Browse** to locate the file. Double-click the file to select it.
3. If the file is being created for the first time, follow these additional steps:
    a. Browse to the target directory.
    b. Right-click inside the file listing pane, and select **New**, **Text Document**. Then, enter a name for the file, and press **Enter**.
    c. Double-click the new file to select it.
4. Click **Backup**.

Restoring Map Settings

This feature is particularly useful in restoring user mappings to address server failures. The administrator can implement redundant mapping servers for fault tolerance by pointing the NFS server to a mapping service on another TaskSmart N-Series appliance. All user name mappings must be the same for this feature to work properly.

1. From the MMC, select **File Sharing**, **Services for UNIX**, and **User Name Mapping**. Select the **Map Maintenance** tab.
2. Enter the path and the name of the file to restore from in the **File path and name** box, or click **Browse** to locate the file.
3. Click **Restore**.

If mapping services are deployed in different departments, the user name mappings may be different.

Mortice Kern Systems Toolkit

The Mortice Kern Systems (MKS) toolkit is a collection of UNIX utilities ported to the Windows NT 32-bit command console. Details about the how to install and run these utilities are available in the online help documentation.

Novell Network Integration

When integrating a TaskSmart N-Series appliance into an existing Novell and Microsoft network, it can join that network using either the Domain or the Workgroup model.

To join a network environment with Novell servers, Microsoft's File and Print Services for NetWare (FPNW) program must be installed onto the TaskSmart N-Series appliance. This program allows the TaskSmart N-Series appliance to emulate a Novell server, thus making its integration into the network seamless.

For additional information on File and Print Services for NetWare, go to the following Microsoft website:

www.microsoft.com/WINDOWS2000/guide/server/solutions/

For additional information on Novell products, go to the following Novell website:

www.novell.com/

Domain or Workgroup Environment

A TaskSmart N-Series appliance can be deployed in a Workgroup or in a Domain environment. When a TaskSmart N-Series appliance is deployed in a Workgroup environment, all user and group account access permissions are stored locally on the TaskSmart N-Series 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 TaskSmart N-Series appliance integrates with the Domain controller infrastructure.

File and Print Services for NetWare

IMPORTANT: IPX\SPX protocol is required on the Novell servers. The printing capabilities of File and Print Services for NetWare are not supported on the TaskSmart N-Series appliance.

File and Print Services for NetWare (FPNW) is one part of the Microsoft's Services for NetWare. The most common use of the NetWare network operating system is as a file and print server.

FPNW eases the addition of a TaskSmart N-Series appliance into a mixed infrastructure by providing a NetWare user interface (UI) to a Windows 2000-based server. Administrators and users see the same familiar NetWare UI. In addition, the same single logon for clients is maintained without a need for any client configuration changes.

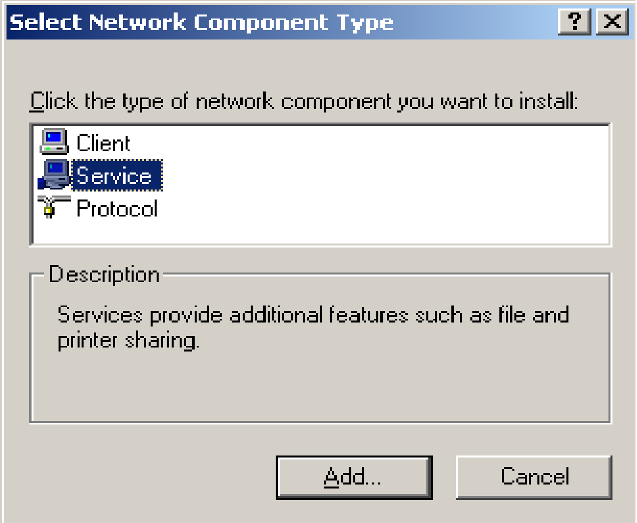
The installation of FPNW on the TaskSmart N-Series appliance allows for a smooth integration with existing Novell servers. The TaskSmart N-Series appliance will emulate a Novell server, allowing authentication from Novell clients, the use of Novell logon scripts, the creation of Novell volumes (actually CIFS shares), the use of Novell file attributes, and many other Novell features.

Installing File and Print Services for NetWare

IMPORTANT: The printing capabilities of FPNW are not supported on the TaskSmart N-Series appliance.

To install File and Print Services for NetWare:

1. From the TaskSmart N-Series appliance console, click **Start**, and then select **Settings-Network and Dial-up Connections**.
2. Click **Local Area Connection**, and then click **Properties**.
3. Click **Install**. The **Select Network Component Type** dialog box is displayed.
4. Select **Service**, and then click **Add**.



Click the type of network component you want to install:

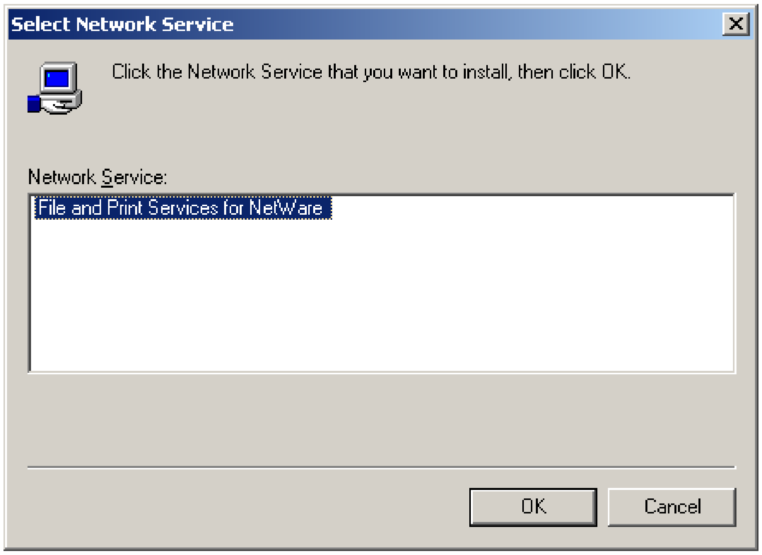
Description

Services provide additional features such as file and printer sharing.

Figure 49: Select Network Component Type dialog box

5. Click the **Have Disk** icon, and then navigate to the location of Services for NetWare. Services for NetWare is located in the path: c:\compaq\SFN.

6. Select the FPNW folder, and then click **OK**. The **Select Network Service** dialog box is displayed. File and Print Services for NetWare should be displayed as an option to install.



Select Network Service
Click the Network Service that you want to install, then click OK.
Network Service:
File and Print Services for NetWare
OK
Cancel

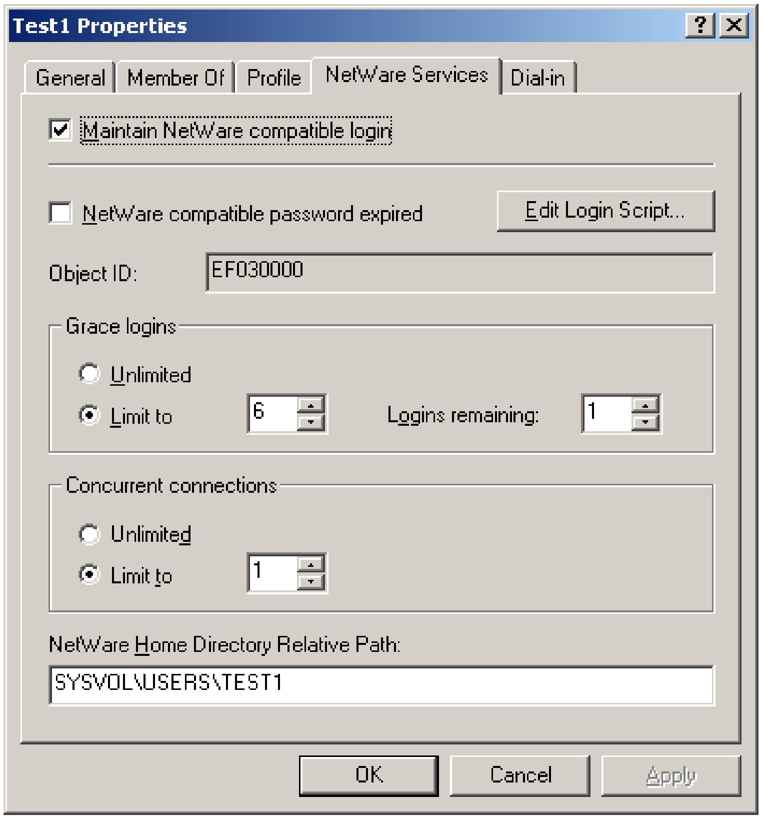
Figure 50: Select Network Service dialog box

7. Select **File and Print Services for NetWare**, and then click **OK**. FPNW is now installed on the appliance.

Creating and Managing NetWare-Enabled Accounts

1. From the TaskSmart N-Series Console, click **Microsoft Management Console**, **Core Operating System**, and then **Local Users and Groups**.
2. Right-click **Users**, and then click **New User**.
3. Complete the **New User** dialog boxes.
4. Click **Users**, and in the details pane, right-click the user account, and then click **Properties**. The **User Properties** dialog box is displayed. See Figure 51 for an example of this screen.
5. Select the **NetWare Services** tab.

   The **NetWare Services** tab is where login scripts are created and edited, grace logins and concurrent connections are limited, and a NetWare home directory path is specified. The installation of FPNW also creates a supervisor account, which is used to manage FPNW. The supervisor account is required if the TaskSmart N-Series appliance is added as a bindery object into NDS.



☑ Maintain NetWare compatible login

□ NetWare compatible password expired

Object ID: EF030000

Grace logins

○ Unlimited

● Limit to 6 Logins remaining: 1

Concurrent connections

○ Unlimited

● Limit to 1

NetWare Home Directory Relative Path: SYSVOL\USERS\TEST1

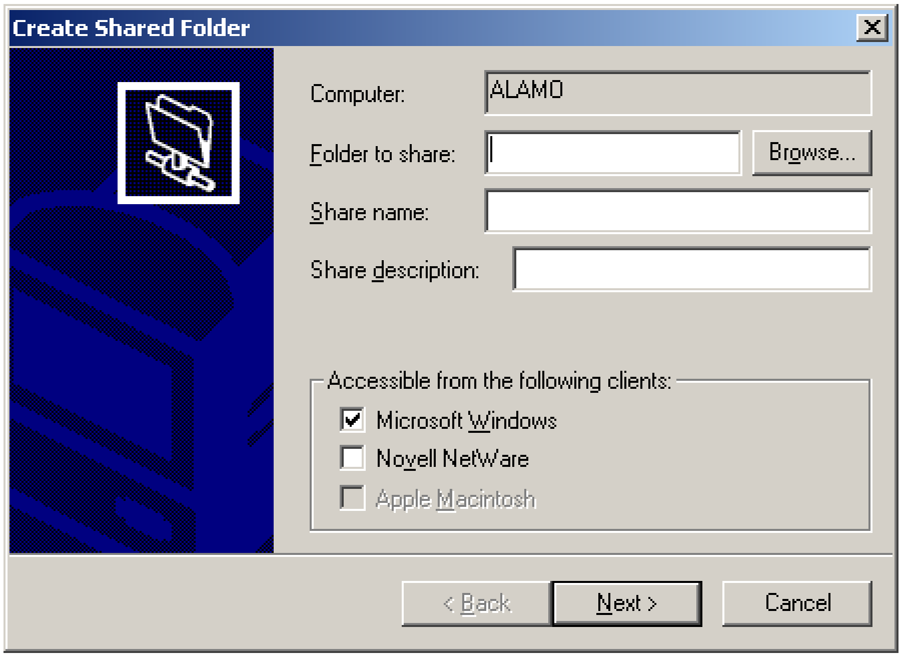
Figure 51: User Properties dialog box, NetWare Services tab

6. Click **Maintain NetWare compatible login**.
7. Set the other NetWare options for the user, and then click **OK**.
8. Enter the user account password in both the **Password** and **Confirm Password** fields, and then click **OK**.

Creating Volumes

Before creating a volume (share), verify that the pool and the virtual disks that will contain the data have been created.

1. From the TaskSmart N-Series Console, click **Microsoft Management Console**, **File Sharing**, **Shared Folders**, and **Shares**.
2. Right-click **Shares**, and then click **New File Share**. The **Create Shared Folder** dialog box is displayed.



Create Shared Folder

Computer: ALAMO

Folder to share:

Share name:

Share description:

Accessible from the following clients:

☑ Microsoft Windows

☐ Novell NetWare

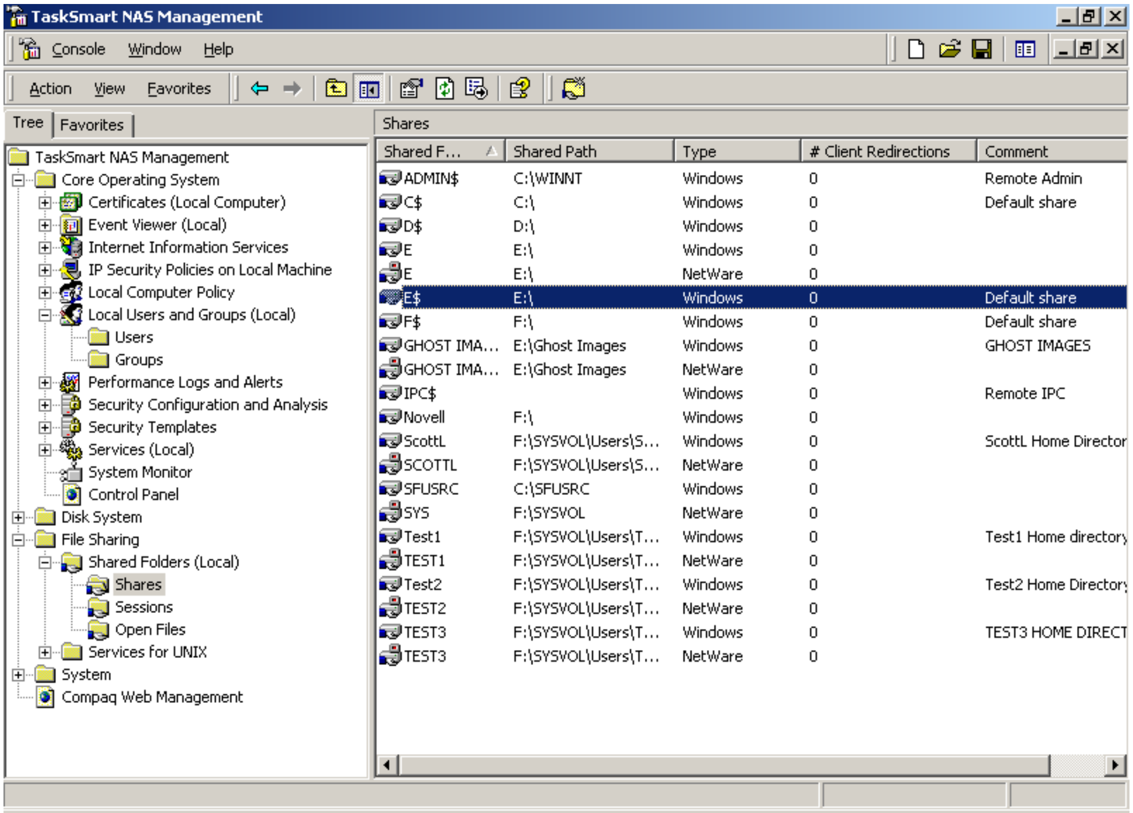
☐ Apple Macintosh

Figure 52: Create Shared Folder dialog box

3. Enter the path of the directory to share or click **Browse** to choose from a list.
4. Enter the name of the share. The users will see this name.
5. Enter a description for the share.
6. Select **Microsoft Windows**, **Novell NetWare**, or both, depending on which type of clients can access this share. Then, click **Next**.
7. Choose standard permissions or customize the share permissions by clicking **Customize share and folder permissions**, and then **Custom**.
8. After entering the permissions, click **Finish**. Then click either **Yes** to create another shared folder or **No** to exit.

Managing Volumes

1. From the TaskSmart N-Series Console, click **Microsoft Management Console**, **File Sharing**, **Shared Folders**, and **Shares**. Figure 53 is an illustration of the **MMC Shares** screen.



- TaskSmart NAS Management
  - Core Operating System
    - Certificates (Local Computer)
    - Event Viewer (Local)
    - Internet Information Services
    - IP Security Policies on Local Machine
    - Local Computer Policy
    - Local Users and Groups (Local)
      - Users
      - Groups
    - Performance Logs and Alerts
    - Security Configuration and Analysis
    - Security Templates
    - Services (Local)
    - System Monitor
    - Control Panel
  - Disk System
  - File Sharing
    - Shared Folders (Local)
      - Shares
      - Sessions
      - Open Files
    - Services for UNIX
  - System
  - Compaq Web Management

Shared F...	Shared Path	Type	# Client Redirections	Comment
ADMIN$	C:\WINNT	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D$	D:\	Windows	0	
E	E:\	Windows	0	
E	E:\	NetWare	0	
E$	E:\	Windows	0	Default share
F$	F:\	Windows	0	Default share
GHOST IMA...	E:\Ghost Images	Windows	0	GHOST IMAGES
GHOST IMA...	E:\Ghost Images	NetWare	0	
IPC$		Windows	0	Remote IPC
Novell	F:\	Windows	0	
ScottL	F:\SYSVOL\Users\S...	Windows	0	ScottL Home Director
SCOTTL	F:\SYSVOL\Users\S...	NetWare	0	
SFUSRC	C:\SFUSRC	Windows	0	
SYS	F:\SYSVOL	NetWare	0	
Test1	F:\SYSVOL\Users\T...	Windows	0	Test1 Home directory
TEST1	F:\SYSVOL\Users\T...	NetWare	0	
Test2	F:\SYSVOL\Users\T...	Windows	0	Test2 Home Director
TEST2	F:\SYSVOL\Users\T...	NetWare	0	
TEST3	F:\SYSVOL\Users\T...	Windows	0	TEST3 HOME DIRECT
TEST3	F:\SYSVOL\Users\T...	NetWare	0	

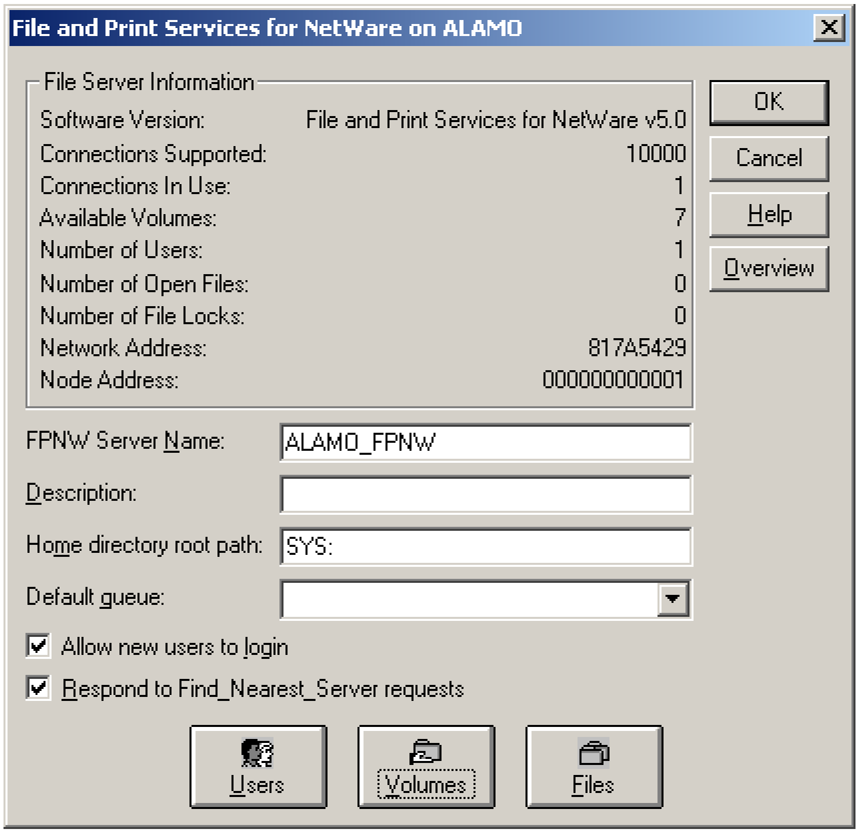
Figure 53: MMC Shares screen

2. In the right-hand pane of the screen, right-click the volume, and then click **Properties**.
3. Select the **Share Permissions** tab.
4. To add additional permissions, change permissions, or remove permissions for a user or group, do one of the following:
   - To grant permissions to an additional user or group, select the user or group, and then click **Add**. After the additional users or groups are added, click **OK**.
   - To change the permissions granted to a user or group, select the user or group, click **Permissions**, and then select **Allow** or **Deny** for each item.
   - To remove permissions for a group or user, select the user or group, and then click **Remove**.

   Permissions can be set on a shared volume regardless of its type of file system. Volume permissions are effective only when the volume is accessed over the network. The group of volume permissions set for the volume applies equally to all files and subdirectories in the volume. Volume permissions on an NTFS volume operate in addition to NTFS permissions set on the directory itself. Volume permissions specify the maximum access allowed.

Managing File and Print Services for NetWare

1. To open FPNW, click **Start**, then select **Settings**, and then click **Control Panel**.
2. Double-click **FPNW**. The **File and Print Services for NetWare** dialog box is displayed.



File and Print Services for NetWare on ALAMO

File Server Information

Software Version: File and Print Services for NetWare v5.0

Connections Supported: 10000

Connections In Use: 1

Available Volumes: 7

Number of Users: 1

Number of Open Files: 0

Number of File Locks: 0

Network Address: 817A5429

Node Address: 000000000001

FPNW Server Name: ALAMO_FPNW

Description:

Home directory root path: SYS:

Default queue:

☑ Allow new users to login

☑ Respond to Find_Nearest_Server requests

Figure 54: File and Print Services for NetWare dialog box

3. Enter a name for the FPNW server. The FPNW server name must be different than the server name used by Windows or LAN Manager–based clients to refer to the server. If changing an existing name, the new name will not be effective until File and Print Services for NetWare is stopped and restarted. For example, in Figure 54, the Windows server name is Alamo and the FPNW server name is Alamo_FPNW.
4. Enter the home directory root path in the **Home directory root path** field. This path is relative to where the Sysvol volume is installed. This is the root location for the user's individual home directories. If the directory specified does not already exist, it must first be created.
5. To manage users, volumes, and files, do one of the following:
   - To see connected users, disconnect users, send broadcast messages to all users connected to the server, and to send a message to a specific user, click **Users**.
   - To see users connected to a specific volume, and to disconnect users from a specific volume, click **Volumes**.
   - To see open files and to close files, click **Files**.

Remote Administration

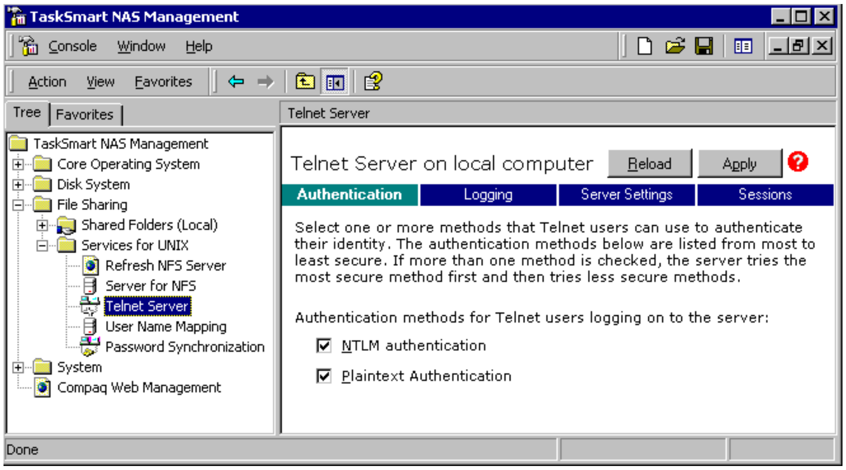
The Compaq TaskSmart N-Series appliance is capable of remote administration by each of the following methods:

- Telnet Server
- Remote shell daemon
- Microsoft Terminal Services
- Remote Insight Lights-Out Edition board
- Web-based user interface
- *Compaq Insight Manager*™

Telnet Server

Telnet Server is a UNIX command-line utility that allows users to connect to machines, log on, and obtain a command prompt remotely. To allow users Telnet Server access, Telnet Server must be installed. Telnet Server is preinstalled on the TaskSmart N-Series appliance.

Figure 55 illustrates the Telnet Server interface.



Telnet Server on local computer

Select one or more methods that Telnet users can use to authenticate their identity. The authentication methods below are listed from most to least secure. If more than one method is checked, the server tries the most secure method first and then tries less secure methods.

Authentication methods for Telnet users logging on to the server:

☑ NTLM authentication

☑ Plaintext Authentication

Figure 55: Telnet Server user interface screen

The utility enables remote administration and user access from other machines. For more information regarding Telnet Server, refer to the UNIX man pages available on the system.

Authentication

Use the **Authentication** tab to select user authentication methods allowed by the Telnet Server. The administrator determines what method of authentication is appropriate, based on the work environment.

Auditing

Telnet Server can log various events. The **Logging** tab allows the administrator to enable logging and select the events that should be logged. Note that errors and significant events are always logged to the Windows NT Event List.

Server Settings

Use the **Server Settings** tab to change Telnet Server parameters. These parameters determine how the TaskSmart N-Series Telnet Server operates. For example, one parameter controls the number of simultaneous Telnet Server connections the server allows.

Sessions

The **Sessions** tab provides the ability to terminate sessions.

Remote Shell Daemon

The remote shell, commonly referred to as "rsh" in UNIX, is a method for allowing users to access a command prompt or run a command on another machine. It can be used in a fashion similar to Telnet Server, or can be used to directly invoke a remote command.

For example:

```
Rsh <server name>  ls -al
```

The remote shell runs the "ls -al" command on <server name>, and returns the results to the screen.

Note: A *.RHOSTS* file must be created to allow client access to the server. Refer the SFU help topic "Rshsvc" on how to create the *.RHOSTS* file.

Currently, SFU implements only the remote command functionality of rsh. If a command line is needed, use Telnet Server.

For more information regarding the setup and use of Remote Shell or the remote shell service, refer to the online help documentation.

Microsoft Terminal Services

One of the useful features of the TaskSmart N-Series appliances is the inclusion of utility programs that an administrator may want to use. One of these included programs is the Terminal Services program by Microsoft. Terminal Services provides a high-performance remote management mechanism that allows the user to connect to the desktop of the TaskSmart N-Series appliance from a remote Windows client.

Terminal Services gives the administrator a remote point of presence that has capabilities identical to physically being present on the local logon console.

Instructions that detail the installation and use of Terminal Services is available in the *Using Microsoft Terminal Services to Manage TaskSmart N-Series Appliances* document at the following website:

www.compaq.com/TaskSmart/n2400/

Remote Insight Lights-Out Edition Board

The following information provides an overview of the Remote Insight Lights-Out Edition board capabilities. Refer to the *Compaq Remote Insight Lights-Out Edition Installation and Users Guide* on the Compaq Documentation CD for further information.

The Remote Insight Lights-Out Edition board is a PCI-based, single-board computer that uses a Web interface to provide remote management of the server from a remote console. Complete keyboard, mouse, and video capability for the server is available, regardless of the state of the host operating system or the host CPU. A built-in processor, combined with a standard external power supply, makes the Remote Insight Lights-Out Edition board independent of the host server and its operating system. The Remote Insight Lights-Out Edition board provides remote access, sends alerts, and performs other management functions, even if the host server operating system is not responding or the server has lost power.

IMPORTANT: The remote client console must have a direct browser connection to the Remote Insight Lights-Out Edition board without passing through a proxy server or firewall.

The Remote Insight Lights-Out Edition board provides the following features:

- Hardware-based graphical remote console access
- Remote restart
- Server failure alerting
- Integration with Compaq Insight Manager
- LAN access through onboard NIC
- Browser support for Internet Explorer 4.01 or newer
- Reset and failure sequence replay
- Remote Insight Lights-Out Edition board User Administration Security
- External power
- Auto configuration of IP address via Domain Name Server (DNS) or Dynamic Host Control Protocol (DHCP)
- Virtual power button
- User Management—allows the user with supervisory access to add or delete users, or modify an existing user's configuration. This feature also allows the user to modify the following:
  - User name
  - Logon name
  - Password/confirm password
  - Supervisor access
  - Logon access
  - Remote console access
  - Remote server reset access

- Alert management—allows the user to send test alerts, to clear pending alerts, and to specify which type of alert messages to receive. This feature includes the ability to do the following:
  - Select alert types received
  - Generate a global test alert
  - Generate an individual test alert
  - Clear pending alerts
  - Enable alerts
- Virtual diskette drive – allows the administrator to upload a raw diskette image to the Remote Insight Lights-Out Edition board. This image can then be used to boot from, for example, so that a *ROMPaq*™ can be applied remotely.

Refer to the *Compaq Remote Insight Lights-Out Edition Board User Guide* for more information about the features and functionality of the Remote Insight Lights-Out Edition board. For more detailed information, go to the following Compaq website:

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

Configuring the Remote Insight Lights-Out Edition Board

By default, the TaskSmart N-Series appliance comes from the factory with full remote manageability. The Remote Insight Lights-Out Edition board on the TaskSmart N-Series appliance is initially configured through the TaskSmart Configuration Utility. SNMP is already enabled, the Compaq Insight Management Agents are preinstalled, and the Remote Insight Lights-Out Edition board is fully functional.

The Remote Insight Lights-Out Edition board comes with factory default settings, which the administrator can change. Administrators may want to add users, change SNMP trap destinations, or change networking settings. Refer to the *Compaq Remote Insight Lights-Out Edition Installation and Users Guide* for more information about changing these settings.

The Remote Insight Lights-Out Edition board is preconfigured by the TaskSmart Configuration Utility CD with a default user name, password, DNS name, and IP address. These defaults are as follows:

- USERNAME: Administrator
- PASSWORD: (last four digits of the serial number)
- DNS NAME: RIBXXXXXXXXXXXX (The 12 Xs represent the MAC address of the Remote Insight Lights-Out Edition board.)
- IP ADDRESS:

There are several methods for performing Remote Insight Lights-Out Edition board configuration changes. These methods include the following:

- Web interface access
- Remote Insight Lights-Out Edition board configuration utility access by pressing the **F8** key during a system restart

- System Utilities access by pressing the **F10** key during a system restart

  To access the System Utilities screen, do the following:

  1. Select **Configure Hardware**.
  2. Select **PCI Resources**.
  3. Select **Remote Insight Lights-Out Edition board**.
  4. Change the server name, network settings, or users.
  5. Save changes before exiting.

- Remote Insight Lights-Out Edition board Configuration Service

  The Compaq TaskSmart N-Series appliance comes equipped with a Remote Insight Lights-Out Edition board Configuration Service. This service is a Compaq supplied Windows NT service that configures the network setting for the Remote Insight Lights-Out Edition board.

  Initially, the Remote Insight Lights-Out Edition board is configured by the TaskSmart Configuration Utility. The Remote Insight Lights-Out Edition board configuration service is designed to periodically locate the TaskSmart Configuration diskette, and then check for the existence of a *CQNASRIB.CFG* file. This file was originally created by the TaskSmart Configuration Utility.

  The service uses the read-only attribute of the configuration file to determine if the configuration should be applied. On each poll cycle, the service checks the read-only attribute of the configuration file. The poll ranges between 1 and 5 minutes. If the poll range is not set, the service configures the Remote Insight Lights-Out Edition board and sets a read-only attribute on the configuration file.

  To re-enable the TaskSmart Configuration diskette for Remote Insight Lights-Out Edition board configuration, the read-only attribute of the *CQNASRIB.CFG* file must be reset.

  For the configuration to occur, the read-only attribute requires the TaskSmart Configuration diskette not be write protected.

  It is recommended that the TaskSmart Configuration Utility be used to enable the TaskSmart Configuration diskette. The Remote Insight Lights-Out Edition board uses the TaskSmart Configuration Utility before changing the read-only attribute on the *CQNASRIB* file.

Accessing the Server Using the Remote Insight Lights-Out Edition Board

Using the Web interface of a client machine is the recommended procedure for remotely accessing a server.

1. Enter the actual Internet Protocol (IP) address of the Remote Insight Lights-Out Edition board as the address on a client browser program, such as Internet Explorer.
2. Supply the “Administrator” user name and password.

Web-Based User Interface

The TaskSmart N-Series appliance includes a Web-based user interface for the administrator to remotely manage the machine. The Web-based user interface provides user and group management, share management, SANworks Virtual Replicator (SWVR) management, and a subset of Microsoft Windows 2000 operations. In addition, the Web-based user interface includes wizards to guide the administrator through repetitive tasks such as creating a share. To access the Web-Based user interface, launch a Web browser and enter the following in the address field:

<the TaskSmart machine name or IP address>:3201/

Online help for the Web interface is available.

Compaq Insight Manager

The TaskSmart N-Series appliance is equipped with the latest Compaq Insight Management Agents for Servers, allowing easy manageability of the server through Compaq Insight Manager, Hewlett Packard OpenView, and Tivoli NetView.

Compaq Insight Manager version 4.70 or higher is needed to successfully manage the TaskSmart N-Series appliance. Compaq Insight Manager is a comprehensive management tool that monitors and controls the operation of Compaq servers and clients. Compaq Insight Manager consists of two components:

- Windows-based console application
- Server-based or client-based management data collection agents

  Management agents monitor over 1,000 management parameters. Key subsystems are instrumented to make health, configuration, and performance data available to the agent software. The agents act upon that data by initiating alarms in the event of faults. The agents also provide updated management information, such as network interface or storage subsystem performance statistics.

For more information about Compaq Insight Manager, refer to the Compaq Management CD.

Installing Compaq Insight Manager for Hewlett Packard OpenView

The TaskSmart N-Series appliance can be managed using Hewlett Packard (HP) OpenView by following these steps:

1. Install Compaq Insight Manager for HP OpenView, v2.0 or higher onto the client machine.
   a. Insert the Compaq Management CD version 4.70 or higher into the CD-ROM drive of the management console of the client machine.
   b. From the Compaq Management CD window, click **Compaq Insight Manager**.
   c. Select **Compaq Insight Manager**, and then follow the installation directions.

   For detailed instructions on downloading and installing Compaq Insight Manager for Hewlett Packard OpenView (Windows NT operating system), visit the following website:

   www.compaq.com/products/servers/management/nt-ov-dl.html

   For detailed instructions on downloading and installing Compaq Insight Manager for Hewlett Packard OpenView (HPUX), visit the management area website:

   www.compaq.com/products/servers/management

2. Depending on the version of Compaq Insight Manager for HP OpenView that is being used, an addition to the *CPQCONFIG.DAT* may be needed to manage the TaskSmart N-Series appliance from HP OpenView. Because HP OpenView works with different platforms, the location of the *CPQCONFIG.DAT* file varies. Do a search for the file. After the file has been located, add the following line to the file and save it:

   ```
   Server : ntsrvr : 1.3.6.1.4.1.232.11.2.7.2.1.4.0 string "TaskSmart N-Series"
   ```

   This command string allows HP OpenView to identify the TaskSmart N-Series appliance.

Compaq Insight Manager for HP OpenView integrates Compaq hardware management and event notification into the HP OpenView Network Node Manager (NNM) network management console.

Compaq Insight Manager for HP OpenView introduces a browser launch from the NNM console to the home page of the Web-enabled Compaq Management Agents, as shown in Figure 56. This interface is used to collect in-depth information about installed Compaq hardware.

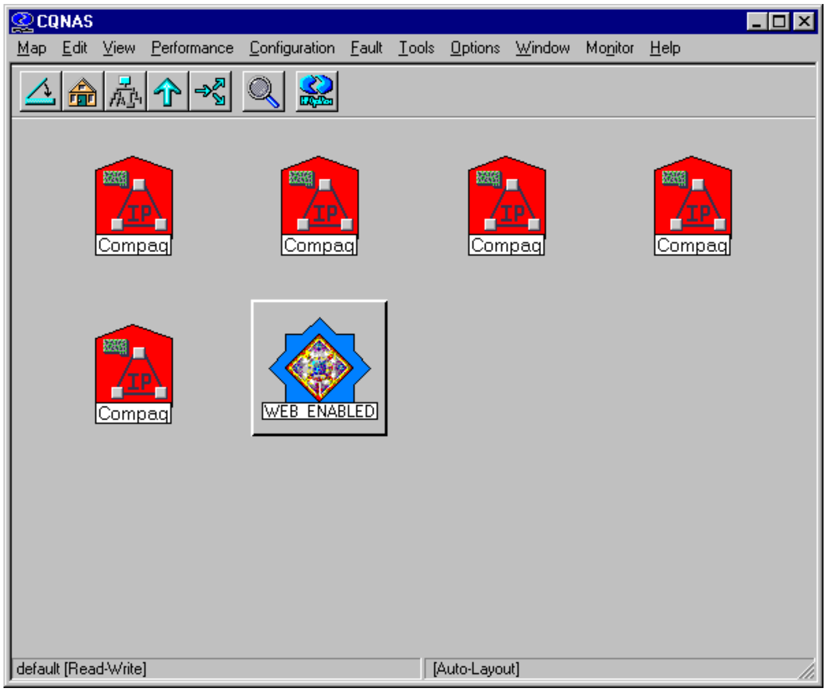

CQNAS
Map Edit View Performance Configuration Fault Tools Options Window Monitor Help
Compaq
Compaq
Compaq
Compaq
Compaq
WEB_ENABLED
default [Read-Write]
[Auto-Layout]

Figure 56: Web Enabled user interface

The collected information includes system status, system health, pre-failure monitors, performance and environmental data, event alarms and Windows NT statistics.

Installing Compaq Insight Manager for Tivoli NetView (AIX), v2.0

Compaq Insight Manager for Tivoli NetView integrates Compaq hardware management and event notification into the Tivoli NetView network management console.

This release introduces an integrated browser launch from the NetView console to the home page of the Web-enabled Compaq Management Agents, used to collect in-depth information about Compaq hardware. The information collected includes system status, system health, prefailure monitors, performance and environmental data, event alarms and Windows NT statistics.

Compaq Insight Manager for Tivoli NetView can be obtained from the following Compaq website:

www.compaq.com/products/servers/management/

The TaskSmart N-Series appliance can be managed using Tivoli NetView (AIX). The following steps are required to manage the TaskSmart N-Series appliance through Tivoli NetView.

1. Install Compaq Insight Manager for Tivoli NetView, v2.0 or higher onto the client machine.
   a. Insert the Compaq Management CD version 4.70 or higher into the CD-ROM drive of the management console of the client machine.
   b. From the Compaq Management CD window, click **Compaq Insight Manager**.
   c. Select **Compaq Insight Manager**, and then follow the installation directions.
2. Modify *CPQCONFIG.DAT* in Tivoli NetView.

   Depending on the version of Compaq Insight Manager for Tivoli NetView that is being used, an addition to the *CPQCONFIG.DAT* may be needed in order to manage the TaskSmart 2400 appliance from Tivoli NetView. Often the location of the *CPQCONFIG.DAT* file varies. Do a search for the file. After the file has been located, add the following line to the file and save it.

```
Server : ntsrvr : 1.3.6.1.4.1.232.11.2.7.2.1.4.0 string "TaskSmart N-Series";
```

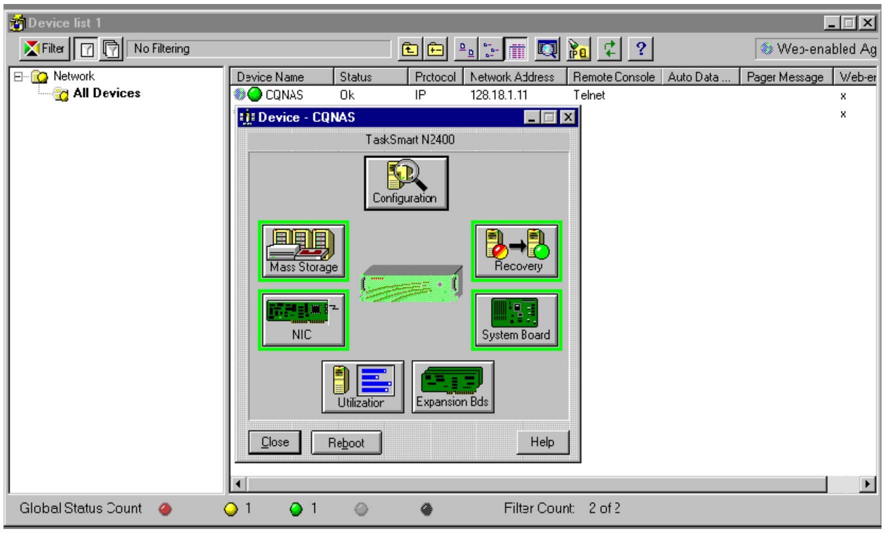
This command string allows Tivoli NetView to identify the TaskSmart N-Series appliance.

Managing Compaq Insight Manager

System monitoring applications such as Compaq Insight Manager allow the administrator to accomplish normal administrative tasks from any remote location with a Web browser.

To manage the TaskSmart N-Series appliance using the Compaq Insight Manager console:

1. Select **Discover IP devices** from the Compaq Insight Manager setup menu.
2. Click **New**.
3. Enter the IP address range of the device, and then click **Add**.
4. Click **Close** when finished.
5. Click **Find Devices**, and then select the device to view.
6. Click **Add/Update All Devices**.
7. Double-click the server to display a device information window. The window displays management data collected by the Compaq agents. Figure 57 illustrates the device information window.



Device Name	Status	Protocol	Network Address	Remote Console	Auto Data ...	Pager Message	Web-en
CQNAS	Ok	IP	128.18.1.11	Telnet			x
							x

Figure 57: Compaq Insight Manager, Device information window

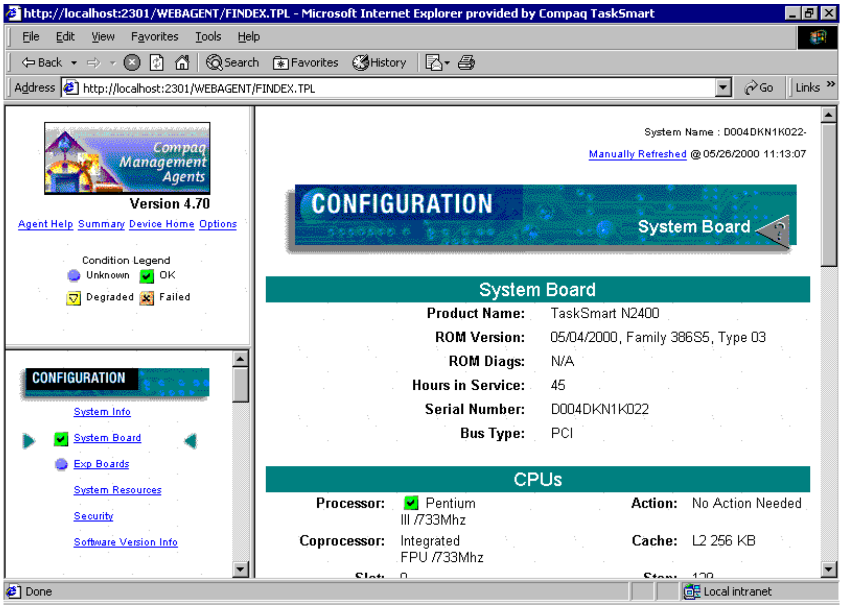
Accessing the Compaq Insight Manager Agent Web Interface

There are two methods for accessing the Compaq Insight Manager Agent Web user interface:

- From the Compaq Insight Manager console, right-click the device name and select **View Web Data**. The Agent Web interface of the server launches in a browser within Compaq Insight Manager.
- Open a Web browser and enter the server IP address using port 2301.

  An example IP address is http://122.18.1.14:2301.

  The default logon account is "Anonymous." Click the account name to log on as an "Administrator.. The default name and password are both "administrator" (in lower case). After the user is logged on as an administrator, the user can change the password.



System Name : D004DKN1K022-

Manually Refreshed @ 05/26/2000 11:13:07

System Board

Product Name:	TaskSmart N2400
ROM Version:	05/04/2000, Family 386S5, Type 03
ROM Diags:	N/A
Hours in Service:	45
Serial Number:	D004DKN1K022
Bus Type:	PCI

CPUs

Processor:	✓ Pentium III /733Mhz	**Action:**	No Action Needed
Coprocessor:	Integrated FPU /733Mhz	**Cache:**	L2 256 KB
Slot:	0	**Step:**	120

Figure 58: Compaq Insight Manager Agent Web user interface

Ethernet Teams

Compaq Network Teaming and Configuration Utility

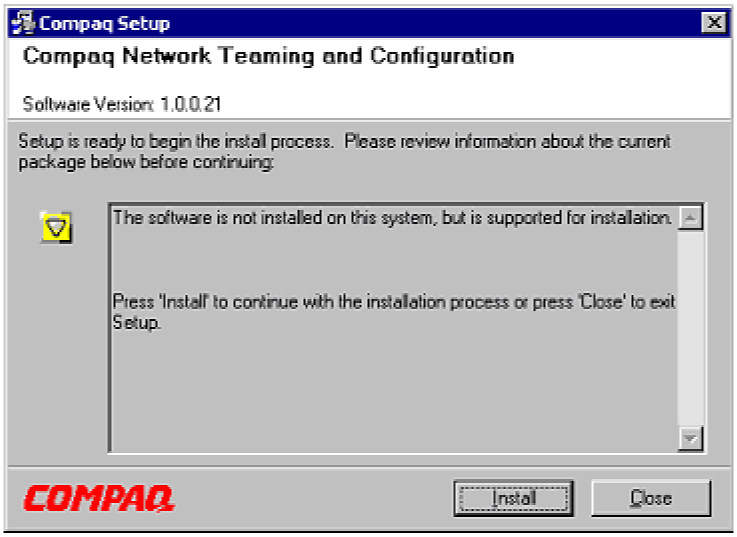
The TaskSmart N-Series appliance is equipped with the Compaq Network Teaming and Configuration (CPQTEAM) Utility. The CPQTEAM Utility allows users to configure and monitor Compaq Network Interface Controllers (NICs) operating under Windows 2000, and provides several options for increasing fault tolerance and throughput.

- **Fault Tolerance**—provides automatic redundancy. If the primary NIC fails, the secondary NIC takes over.
- **Load Balancing**—provides the ability to balance transmissions across NICs. This process improves server throughput.

Installing the CPQTEAM Utility

Before using the CPQTEAM Utility, it must first be installed. To install the CPQTEAM Utility, perform the following steps:

1. Double-click the **CPQTEAM Setup** icon on the desktop.
2. When the following message box is displayed, click **Install**.



Compaq Network Teaming and Configuration

Software Version: 1.0.0.21

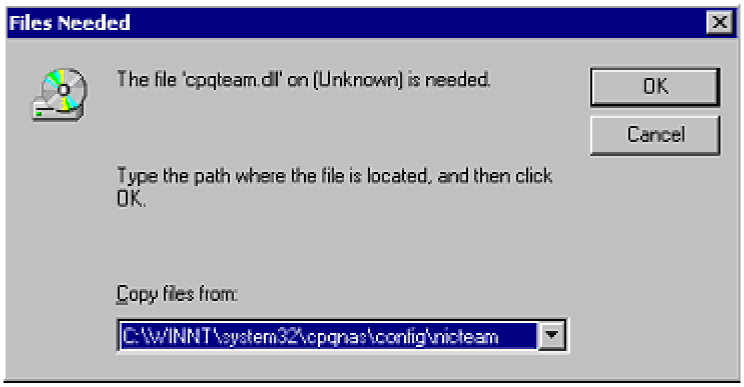
Setup is ready to begin the install process. Please review information about the current package below before continuing.

The software is not installed on this system, but is supported for installation.

Press 'Install' to continue with the installation process or press 'Close' to exit Setup.

Figure 59: Installing CPQTEAM

3. Click **OK** when prompted with the following message (the system will provide the path):



Files Needed

The file 'cpqteam.dll' on (Unknown) is needed.

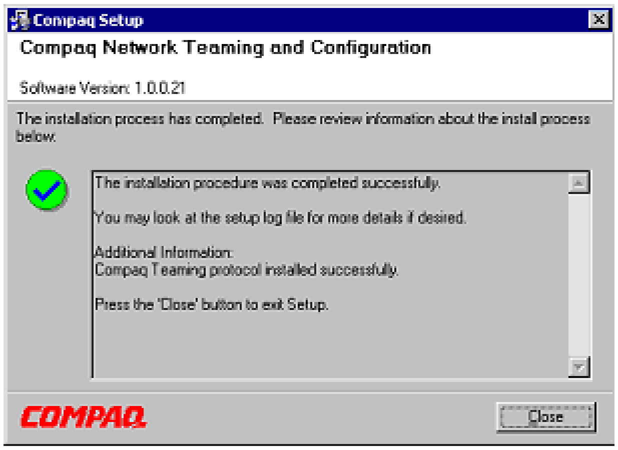
Type the path where the file is located, and then click OK.

Copy files from:

C:\WINNT\system32\cpqnas\config\nicteam

Figure 60: Selecting the CPQTEAM file path

4. The CPQTEAM Utility is now installed on the TaskSmart N-Series appliance. When installation is complete, the following screen is displayed. Click **Close**. The appliance is now ready to use the CPQTEAM Utility.



Compaq Setup

Compaq Network Teaming and Configuration

Software Version: 1.0.0.21

The installation process has completed. Please review information about the install process below.

The installation procedure was completed successfully.

You may look at the setup log file for more details if desired.

Additional Information:
Compaq Teaming protocol installed successfully.

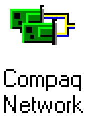
Press the 'Close' button to exit Setup.

Figure 61: CPQTEAM installation complete screen

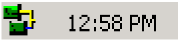
Opening the CPQTEAM Utility

There are two methods to access the CPQTEAM utility:

- From the Windows **Control Panel**, double-click the **Compaq Network** icon.



- Double-click the **Tray** icon in the **Windows toolbar** at the bottom of the Windows 2000 screen.



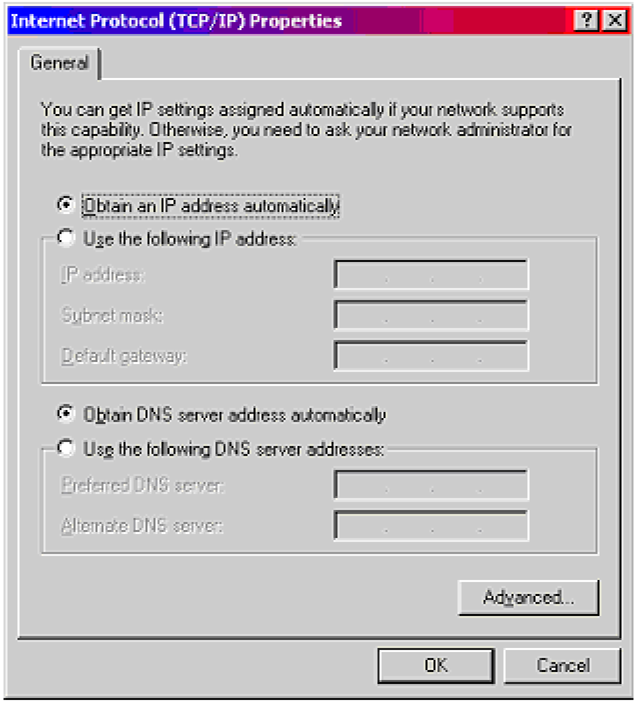
Adding a NIC to a Team

Before a NIC is teamed, verify the following system conditions:

- The NICs must be on the same network.
- The NICs must be DHCP-enabled and the Domain Name System (DNS) server address fields must be left blank.

> **IMPORTANT:** The Teaming utility becomes unstable if static IPs, Subnets, and DNS addresses are set before teaming.

- The Internet Protocol (TCP/IP) Properties for each NIC must match the dialog box displayed in Figure 62.
- The duplex and speed settings of the NIC must be set to the default values as displayed in Figure 63.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

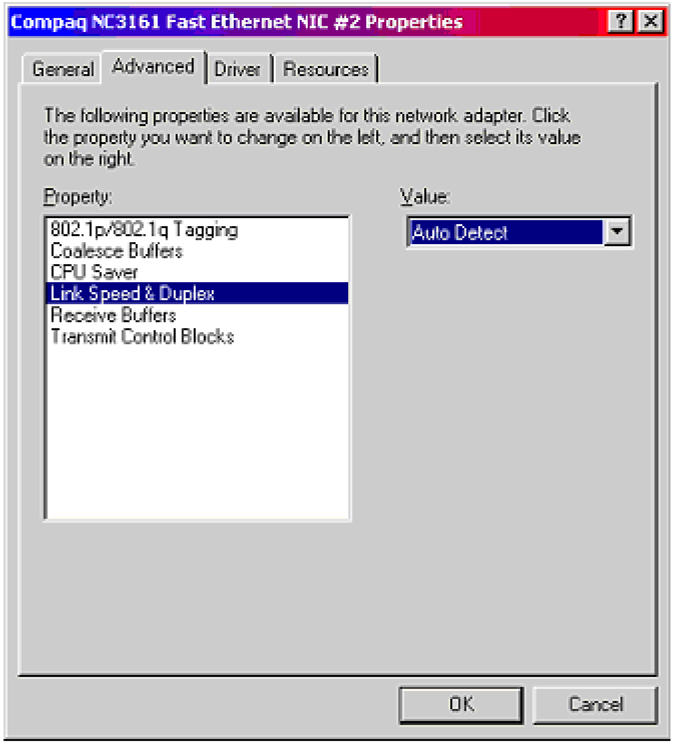
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 62: Internet Protocol (TCP/IP) Properties dialog box


Compaq NC3161 Fast Ethernet NIC #2 Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

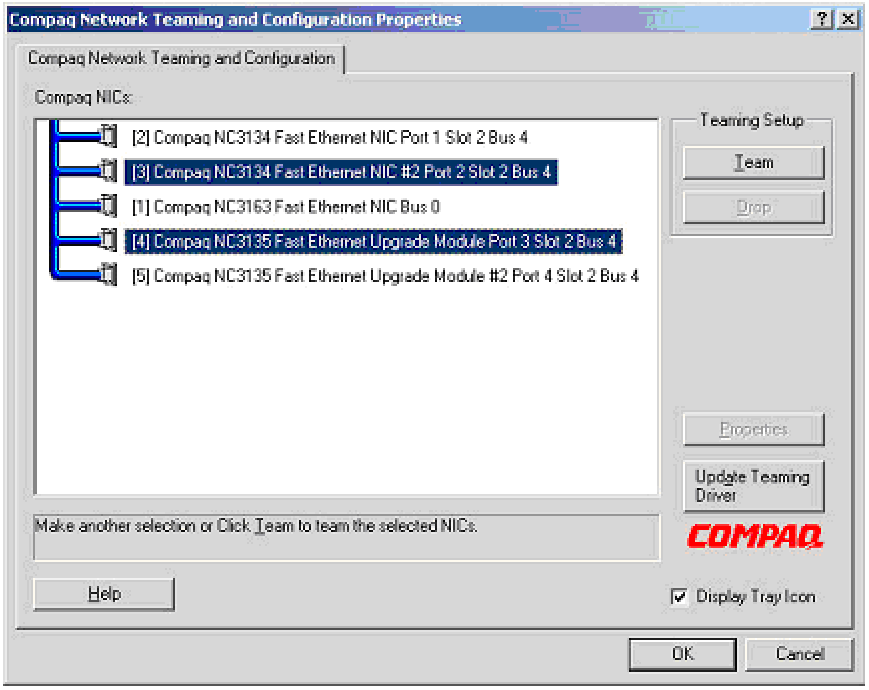
Property:
- 802.1p/802.1q Tagging
- Coalesce Buffers
- CPU Saver
- Link Speed & Duplex
- Receive Buffers
- Transmit Control Blocks

Value: Auto Detect

Figure 63: NIC Properties dialog box

NIC Teaming Setup Procedures

1. Open the CPQTEAM utility.
2. Highlight the NICs to team, and then click **Team**.


Compaq Network Teaming and Configuration Properties

Compaq NICs:
- [2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4
- [3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4
- [1] Compaq NC3163 Fast Ethernet NIC Bus 0
- [4] Compaq NC3135 Fast Ethernet Upgrade Module Port 3 Slot 2 Bus 4
- [5] Compaq NC3135 Fast Ethernet Upgrade Module #2 Port 4 Slot 2 Bus 4

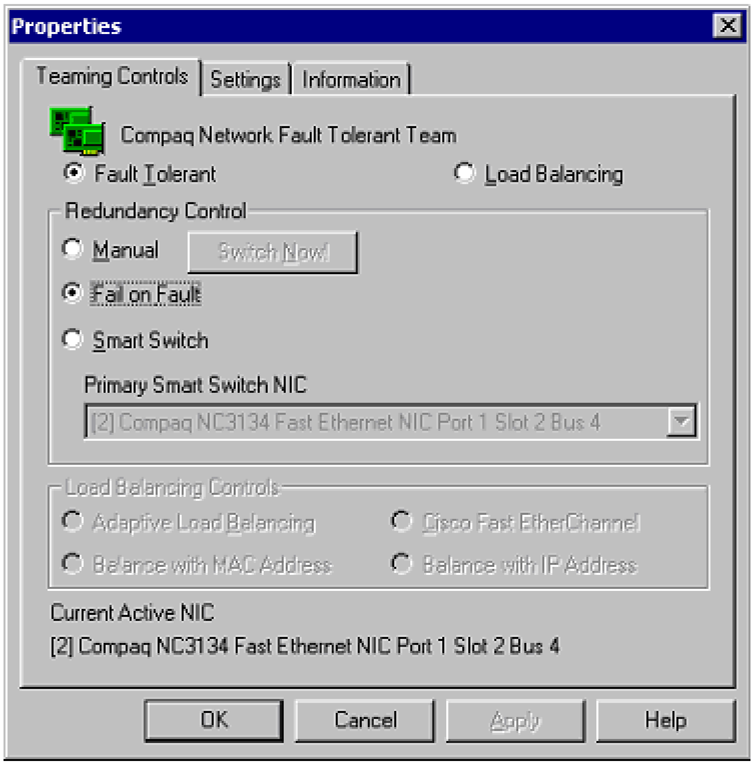
Make another selection or Click Team to team the selected NICs.

Figure 64: Compaq Network Teaming and Configuration Properties dialog box

3. Configure the team as needed by selecting either **Fault Tolerant** or **Load Balancing** in the subsequent dialog boxes. Fault tolerance and load balancing are discussed in the following sections.
4. Complete the CPQTEAM setup by responding to several additional warning screens. These warning screens are discussed in the "NIC Teaming Setup Completion" section.

Fault Tolerance

The **Fault Tolerant** teaming option provides three redundancy control options: **Manual**, **Fail on Fault**, and **Smart Switch**. These options are displayed in Figure 65.



Compaq Network Fault Tolerant Team

● Fault Tolerant ○ Load Balancing

Redundancy Control

○ Manual

● Fail on Fault

○ Smart Switch

Primary Smart Switch NIC

[2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4

Load Balancing Controls

○ Adaptive Load Balancing ○ Cisco Fast EtherChannel

○ Balance with MAC Address ○ Balance with IP Address

Current Active NIC

[2] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4

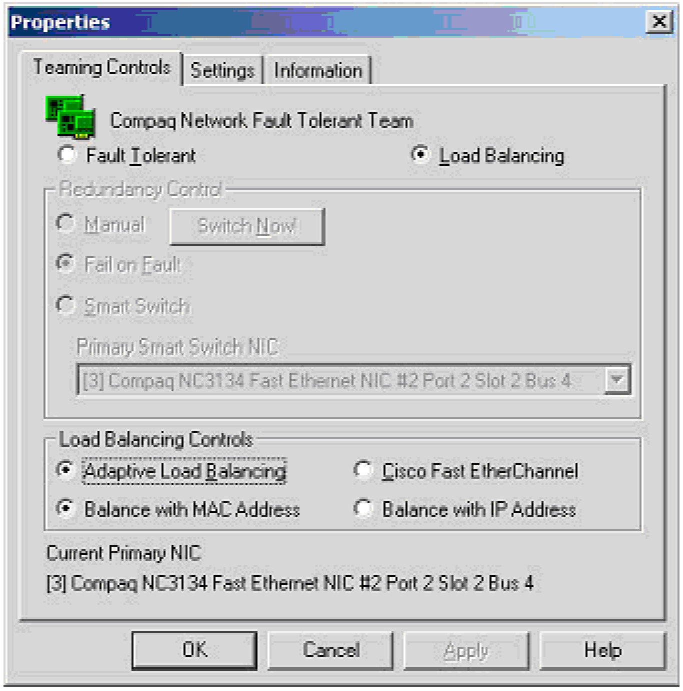
Figure 65: Teaming Controls dialog box, Fault Tolerant options

- **Manual**—This setting lets the user change from a Primary NIC to a Secondary NIC only when the user clicks **Switch Now!** The **Switch Now!** option is disabled until the user selects **Manual**, and then clicks **Apply**.
- **Fail on Fault**—This setting automatically switches from a Primary NIC to a Secondary NIC when the Primary NIC fails.
- **Smart Switch—**This setting allows for a member of a team to be selected as the preferred Primary Smart Switch NIC. As long as this NIC is operational, it is always the active NIC. When this NIC fails and is restored or replaced, it automatically resumes its status as the active NIC. Because of its functionality, **Smart Switch** is the recommended choice for **Fault Tolerance**.

Detailed information about configuring teams for fault tolerance can be found in the "Compaq Network Teaming and Configuration" section of the CPQTEAM Utility online help.

Load Balancing

The **Load Balancing** teaming option provides four load balancing control options: **Adaptive Load Balancing**, **Cisco Fast EtherChannel**, **Balance with MAC Address**, and **Balance with IP Address**. These options are shown in the screen illustrated in Figure 66.



Compaq Network Fault Tolerant Team

○ Fault Tolerant ● Load Balancing

○ Manual

● Fail on Fault

○ Smart Switch

Primary Smart Switch NIC: [3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4

● Adaptive Load Balancing ○ Cisco Fast EtherChannel

● Balance with MAC Address ○ Balance with IP Address

Current Primary NIC

[3] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4

Figure 66: Teaming Controls dialog box, Load Balancing options

- **Adaptive Load Balancing (ALB)—**Creates a team of NICs to increase server transmission throughput. This option works with any 100Base-TX or Gigabit switch. With ALB, NICs can be grouped into teams to provide a single, virtual NIC with increased transmission bandwidth. To use ALB, at least two teamed Compaq NICs must be linked in the server to the same network switch.
- **Cisco Fast EtherChannel (FEC)—**This feature creates a team of NICs to increase transmission and reception throughput. Unlike ALB, Cisco FEC can be configured to increase both transmission and reception channels between the server and switch. For example, a Cisco FEC team containing four Compaq Fast Ethernet NICs configured for full-duplex operation provides an aggregate maximum transmit rate of 400 megabits per second (Mbps) and an aggregate maximum receive rate of 400 Mbps resulting in a total bandwidth of 800 Mbps.
- **Balance with MAC Address—**This feature allows load balancing of IP packets among the teamed NICs using the last four bits of the MAC (Medium Access Control layer) address.
- **Balance with IP Address—**This feature allows load balancing of IP (Internet Protocol) packets among the teamed NICs using the last four bits of the IP address.

Load Balancing with MAC or IP Address

The CPQTEAM Utility load balances IP packets among the teamed NICs installed in a server. The primary NIC in the team receives all incoming packets. The choice is available to load balance with the source MAC address (the address transmitted from the workstation) or the source IP address.

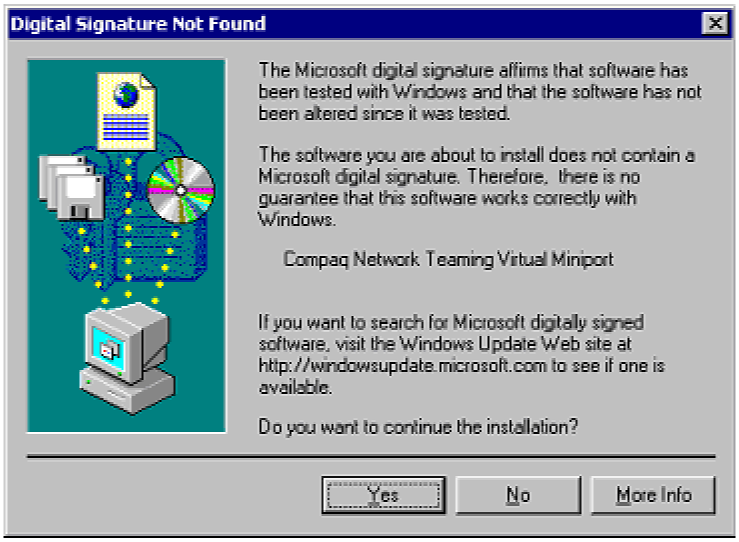
Using the last four bits of either source address, the teaming driver algorithm then assigns this source address to the port of one of the NICs in the team. This port is then used to transmit all packets destined for that source address. If there are four NICs in the team, the packets are received by the primary NIC on the team. The packets are retransmitted through one of the four ports.

Detailed information about these four load-balancing teaming options can be found in the "Compaq Network Teaming and Configuration" section of the online help in the CPQTEAM Utility.

NIC Teaming Setup Completion

After completing the NIC teaming procedure, several warning screens are displayed.

1. When prompted to continue, click **Yes**.



The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

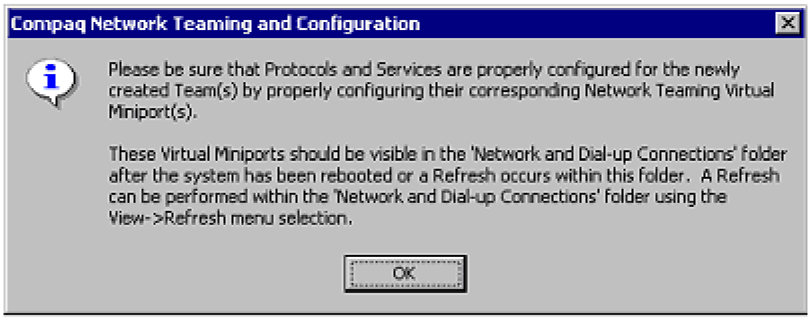
Compaq Network Teaming Virtual Miniport

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

Figure 67: License Warning dialog box

2. Click **OK**.

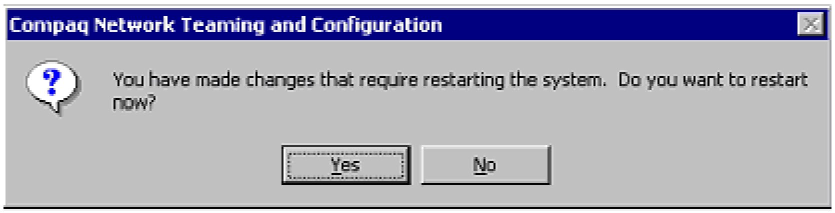


Please be sure that Protocols and Services are properly configured for the newly created Team(s) by properly configuring their corresponding Network Teaming Virtual Miniport(s).

These Virtual Miniports should be visible in the 'Network and Dial-up Connections' folder after the system has been rebooted or a Refresh occurs within this folder. A Refresh can be performed within the 'Network and Dial-up Connections' folder using the View->Refresh menu selection.

Figure 68: Compaq Network Teaming and Configuration dialog box

3. After all screens have been completed, a final dialog box is displayed, prompting to restart the system. At this time, close all other open applications, and then click **Yes** to restart the system.



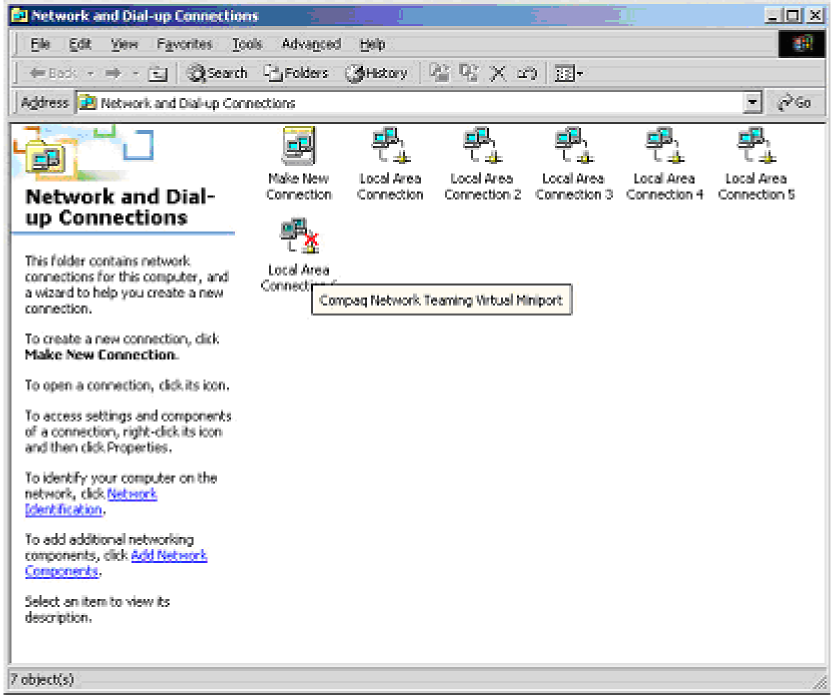
You have made changes that require restarting the system. Do you want to restart now?

Figure 69: Compaq Network Teaming and Configuration Restart dialog box

Configuring the TCP/IP Protocol on the New Team

After the NIC teaming procedure has been completed, a new virtual network adapter must be created in the **Networking Properties** screen. To access the networking properties, use the following steps:

1. Right-click the **My Network Places** icon in the TaskSmart N-Series desktop, and then select **Properties** to display the **Network and Dial-up Connections** dialog box. The TaskSmart N-Series appliance must be restarted after adding a NIC to a team and before the virtual network adapter is created and accessible in the networking properties.



Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

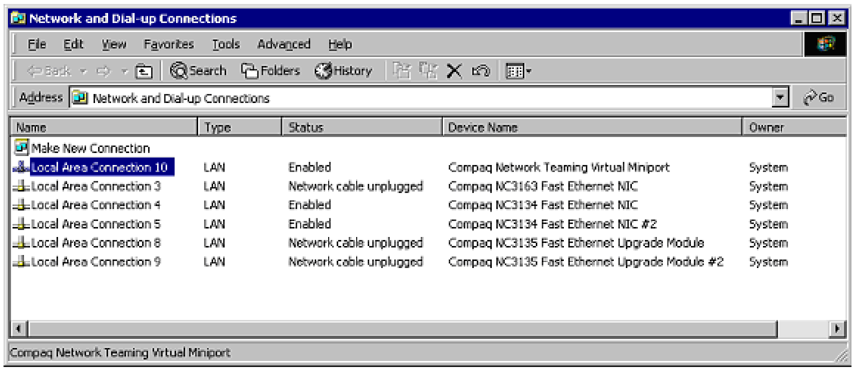
To identify your computer on the network, click Network Identification.

To add additional networking components, click Add Network Components.

Select an item to view its description.

Figure 70: Network and Dial-up Connections screen

2. Select **View** from the toolbar, and then click **Details**.

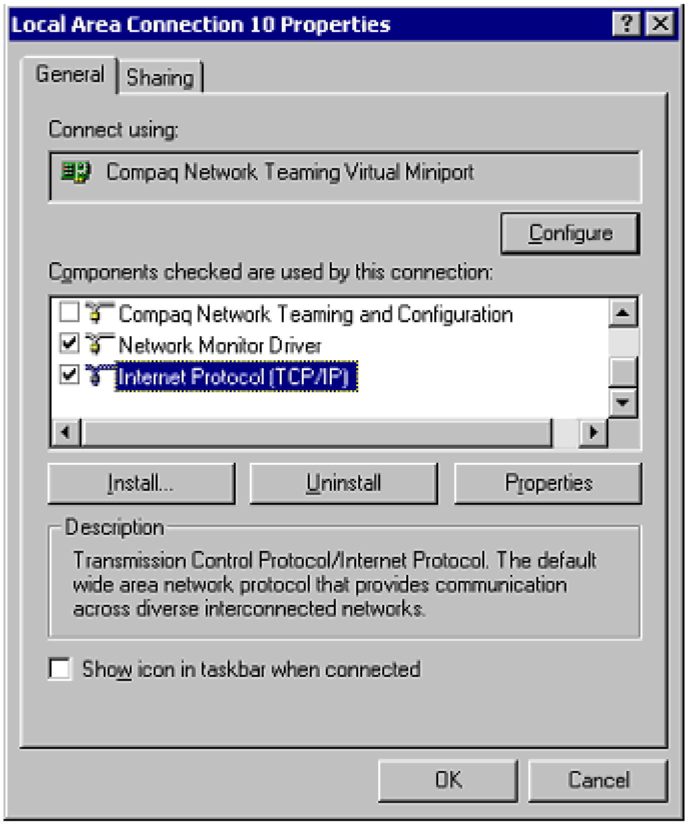

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go

Name	Type	Status	Device Name	Owner
Make New Connection				
Local Area Connection 10	LAN	Enabled	Compaq Network Teaming Virtual Miniport	System
Local Area Connection 3	LAN	Network cable unplugged	Compaq NC3163 Fast Ethernet NIC	System
Local Area Connection 4	LAN	Enabled	Compaq NC3134 Fast Ethernet NIC	System
Local Area Connection 5	LAN	Enabled	Compaq NC3134 Fast Ethernet NIC #2	System
Local Area Connection 8	LAN	Network cable unplugged	Compaq NC3135 Fast Ethernet Upgrade Module	System
Local Area Connection 9	LAN	Network cable unplugged	Compaq NC3135 Fast Ethernet Upgrade Module #2	System

Compaq Network Teaming Virtual Miniport

Figure 71: Network and Dial-up Connections dialog box

3. Right-click **Compaq Network Teaming Virtual Miniport**, and then click **Properties**. A dialog box similar to the example in Figure 72 is displayed.



Connect using:

Compaq Network Teaming Virtual Miniport

Components checked are used by this connection:

- □ Compaq Network Teaming and Configuration
- ☑ Network Monitor Driver
- ☑ Internet Protocol (TCP/IP)

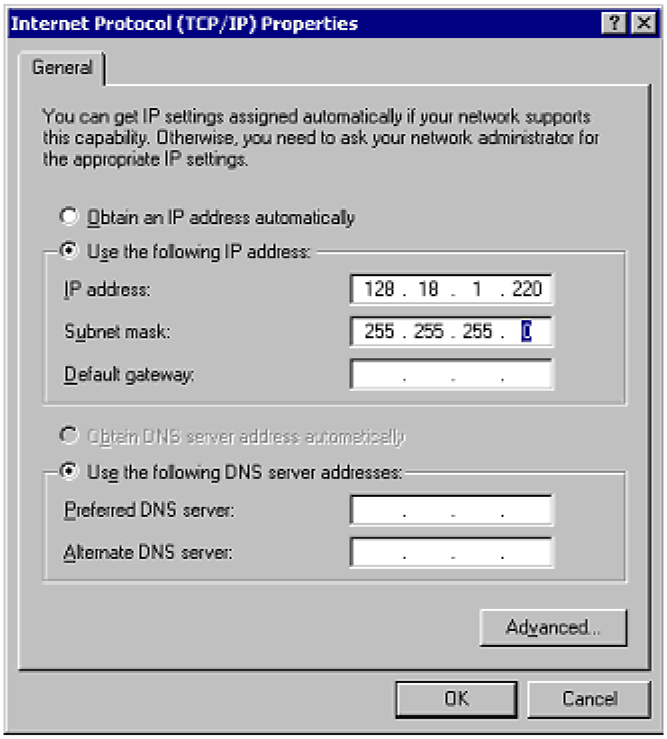
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in taskbar when connected

Figure 72: Local Area Connection Properties dialog box

4. Click **Properties** to configure the **IP address**, **Subnet Mask**, and **DNS address** of the team. The **Internet Protocol Properties** dialog box is displayed.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 128 . 18 . 1 . 220

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

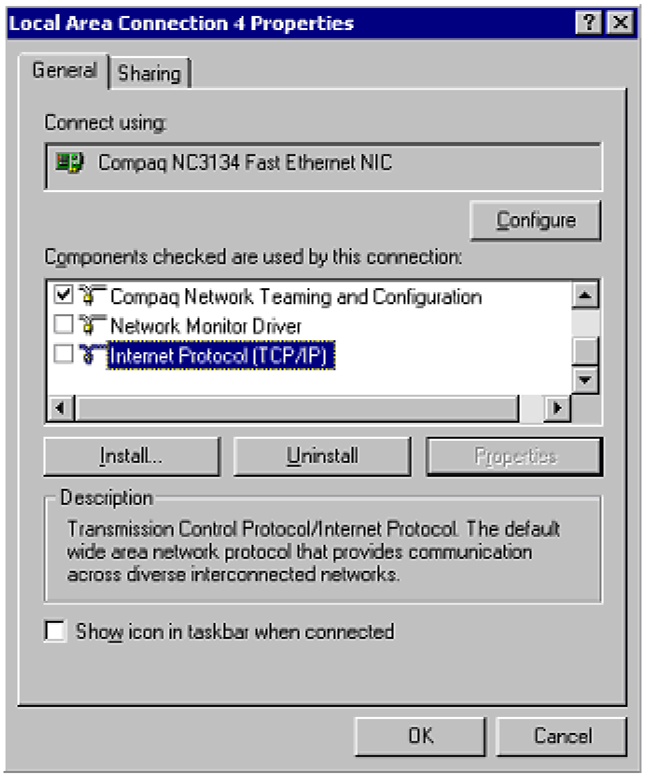
Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 73: Local Area Connection Internet Protocol Properties dialog box

IMPORTANT: When this process is complete, do not modify the TCP/IP Protocols for the individual Ethernet ports that are teamed.

5. After configuring the TCP/IP settings, click **OK**. The **Local Area Connection Properties** dialog box is redisplayed. Click **OK** again.



Connect using:

Compaq NC3134 Fast Ethernet NIC

Components checked are used by this connection:

☑ Compaq Network Teaming and Configuration
☐ Network Monitor Driver
☐ Internet Protocol (TCP/IP)

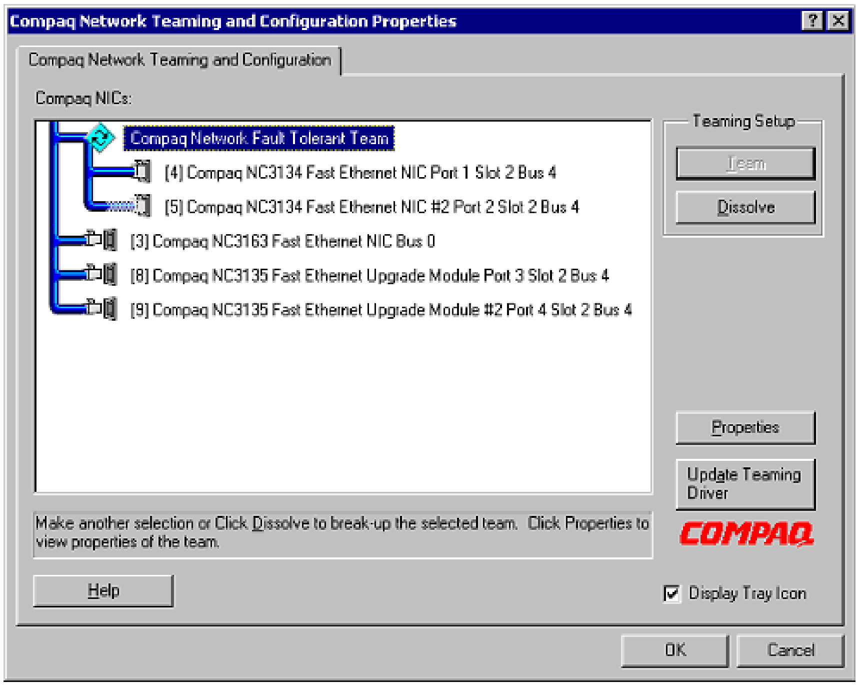
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

Figure 74: Local Area Connection Properties dialog box

6. To view the status of the Ethernet team, open the CPQTEAM Utility. A properties screen is displayed, showing the teamed NICs.


Compaq Network Teaming and Configuration Properties
Compaq Network Teaming and Configuration
Teaming Setup
Team
Dissolve
Properties
Update Teaming Driver
COMPAQ
Help
OK
Cancel

Compaq NICs:

Compaq Network Fault Tolerant Team
[4] Compaq NC3134 Fast Ethernet NIC Port 1 Slot 2 Bus 4
[5] Compaq NC3134 Fast Ethernet NIC #2 Port 2 Slot 2 Bus 4
[3] Compaq NC3163 Fast Ethernet NIC Bus 0
[8] Compaq NC3135 Fast Ethernet Upgrade Module Port 3 Slot 2 Bus 4
[9] Compaq NC3135 Fast Ethernet Upgrade Module #2 Port 4 Slot 2 Bus 4

Make another selection or Click Dissolve to break-up the selected team. Click Properties to view properties of the team.

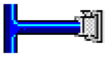
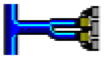
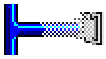
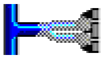
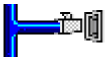
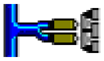
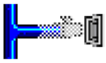
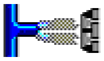
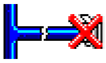
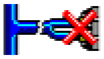
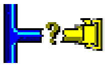
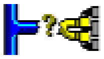
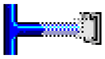
☑ Display Tray Icon

Figure 75: Compaq Network Teaming and Configuration Properties dialog box

NIC Teaming Troubleshooting

Problems with the NIC Teaming feature are diagnosed by the connection icons displayed in the **Compaq Network Teaming and Configuration** dialog box. The following table lists the error icons for RJ-45 and Gigabit Fibre NICs.

Table 7. NIC Teaming Troubleshooting

RJ-45	Gigabit Fibre	Description
		**Active OK**—The NIC is operating properly. The driver is installed in the registry and is loaded. If the NIC is a member of a team, the NIC is active.
		**Installed inactive**—The NIC is installed and is OK, but is not active.
		**Cable fault**—The driver is installed in the registry and is loaded. The broken cable indicator means that the cable is unplugged, loose, broken, or the switch or hub is not operating properly. If this icon is displayed, check all network connections and make sure the hub/switch is working properly. When the connection is restored, this icon will change.
		**Inactive cable fault**—A cable fault has occurred while the NIC was inactive.
		**Hardware failure**—The driver is installed in the registry and is loaded. The driver is reporting a hardware problem with the NIC. This problem may be serious. Contact an authorized Compaq service provider.
		**Unknown**—The appliance is unable to communicate with the driver for the installed NIC. The NIC is installed in the registry, but the driver is not. This error occurs when the NIC has been installed but the appliance has not been restarted. If this problem persists after the appliance has been restarted, the driver has not been loaded or the Advanced Network Control Utility is unable to communicate with the driver. **Note**: Only NICs assigned as members of a team are displayed as Unknown. If a teamed NIC is turned off, it displays as Unknown.
		**Disabled**—The NIC has been disabled through the Device Manager or NCPA.

For more advanced problems with NIC Teaming, refer to the “Compaq Network Teaming and Configuration” section of the CPQTEAM Utility online help.

Compaq Professional Service Offerings

Compaq Services offers complete services for the implementation, management and support of user environments, including the following:

- Warranty upgrades
- Installation and configuration
- Priority Service Plan
- Performance and Capacity Planning
- System Management and Monitoring

For more information, visit the Compaq website at

http://www.compaq.com